Member States Confronted with EU-Based Rules in the Field of Cybersecurity, The Effectiveness of Directive (EU) 2016/1148

Theodoros Karathanasis

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ GRENOBLE ALPES

École doctorale : EDSJ - École Doctorale Sciences Juridiques
Spécialité : Droit Européen
Unité de recherche : Centre d'Études sur la Sécurité Internationale et les Coopérations Européennes

Les Etats-Membres de l'Union Européenne Face aux Règles Européennes en Matière de Cybersécurité : L'effectivité de la Directive (UE) 2016/1148

Member States Confronted with EU-Based Rules in the Field of Cybersecurity, The Effectiveness of Directive (EU) 2016/1148

Présentée par :

Theodoros KARATHANASIS

Direction de thèse :

Monsieur Fabien TERPAN — Directeur de thèse
MAITRE DE CONFERENCES HDR, Sciences Po Grenoble

Rapporteurs :

Monsieur Paul James CARDWELL
PROFESSEUR, King's College London

Monsieur Juan Santos VARA
PROFESSEUR, University of Salamanca

Thèse soutenue publiquement le **10 Novembre 2022**, devant le jury composé de :

Madame Karinne BANNELIER-CHRISTAKIS MAITRE DE CONFERENCES HDR, Université Grenoble Alpes	Examinatrice
Monsieur Paul James CARDWELL PROFESSEUR, King's College London	Rapporteur
Madame Gaëlle, MARTI PROFESSEUR DES UNIVERSITES, Université Jean Moulin - Lyon 3	Présidente
Monsieur Fabien TERPAN MAITRE DE CONFERENCES HDR, Sciences Po Grenoble	Directeur de thèse
Monsieur Juan Santos VARA PROFESSEUR, University of Salamanca	Rapporteur

- Under the direction of Fabien TERPAN -

Member States Confronted with EU-Based Rules in the Field of Cybersecurity

The Effectiveness of Directive (EU) 2016/1148

Theodoros KARATHANASIS

European Law

Résumé

La directive 2016/1148 (connue sous le nom de directive SRI) est la première directive de l'Union européenne invitant les États membres à relever collectivement et globalement, les défis de sécurité des réseaux numériques dans un certain nombre de domaines clés (à savoir l'énergie, les transports, la banque, les bourses, les fournisseurs de services numériques…), tout en soulignant la nécessité d'une politique internationale cohérente de l'UE dans le domaine cyber. La directive SRI est entrée en vigueur en août 2016. Les États membres disposaient de 21 mois, jusqu'au 9 mai, pour transposer la directive en droit national et disposaient de 6 mois supplémentaires pour identifier les opérateurs de services essentiels. Malgré les progrès réalisés par les États membres de l'UE dans l'adoption de leur stratégie nationale sur la sécurité des réseaux et des systèmes d'information, la transposition de la directive SRI à travers l'UE n'est pas uniforme. La présente thèse tente, à partir d'une étude de cas – la directive SRI – d'offrir une réflexion sur l'effectivité des directives européennes et leur capacité à harmoniser les règles européennes. Ainsi, contrairement à la littérature existante, la valeur ajoutée de cette thèse consiste à analyser et comparer la transposition de la Directive SRI dans six Etats Membre de l'UE – la Finlande, la France, la Grèce, l'Irelande, le Luxembourg et la Pologne – afin d'identifier des points de divergence ou de convergence. L'objectif de cette étude spécifique est d'apporter d'avantage d'éclaircissements sur les raisons pour lesquelles les Etats-Membres de l'Union Européenne ne transpose pas de manière uniforme les directives européennes. Afin d'étudier l'état d'avancement de la sécurité des systèmes de réseau et d'information dans chacun des six États membres de l'UE étudiés, un cadre a été établi avec des critères spécifiques sur la base duquel l'évaluation est réalisée. Pour évaluer l'utilisation discrétionnaire de la marge de manœuvre accordée par la Directive par la Finlande, la France, la Grèce, l'Irlande, le Luxembourg et la Pologne, trois hypothèses ont été testées concernant le degré d'inadéquation politique, d'inadéquation institutionnelle et d'efficacité administrative. De cette évaluation, il en ressort que plus les directives européennes offriront une marge de manœuvre réglementaire aux Etats-Membres de l'UE pour la transposition de leur contenu, plus la préservation des intérêts nationaux par les États membres de l'UE affectera la mise en application uniforme des directives à travers l'UE. Car, si la transposition de la Directive SRI par les Etats-Membres, ici étudiés, a été légalement conforme à court terme. La mise en application des loi nationaux de transposition risque de mettre en évidence, sur le long terme, l'étendu des divergences réglementaires sur la protection des systèmes de réseau et d'information à travers l'UE.

Abstract

Directive 2016/1148 (known as the NIS Directive) is the first European Union law calling on Member States to address the digital network security challenges collectively and globally in several key areas (namely energy, transport, banking, stock exchanges, and digital services providers, public administrations etc.), while underlining the need for a coherent EU cyber-friendly international policy. The NIS Directive came into force in August 2016. Member States had 21 months, until 9th of May, to transpose the Directive into national law and had an additional 6 months to identify the operator's basic services. Despite progress made by EU Members states in adopting their national strategy on the security of network and information systems, the transposition of the NIS directive across the EU offers a fragmented landscape. Thie present thesis attempts, from a case study – the NIS directive – to offer a reflection on the effectiveness of European directives and their capacity of harmonizing the European rules. The added value of this thesis lies in the analysis and comparison of six national regulatory frameworks, those of Finalnd, France, Greece, Ireland, Luxembourg, and Poland in order to identify points of divergence or convergence. The objective of this specific study is to shed more light on the reasons why the Member States transpose directives in many different ways. To study the state of play on the network and information systems security in each of the six Member States of the EU studied in this thesis , a framework was established with specific criteria on the basis of which the evaluation is carried out. For assessing the discretionary use of the regulatory leeway by Finland, France, Greece, Ireland, Luxembourg and Poland three hypothesis have been tested regarding the degree of policy misfit, of institutional misfit and the administrative effectiveness. From this assessment, it emerged that the more the Directives offer a regulatory leeway to EU Member States for the transposition of their content, the more the preservation of national interests by EU Member States affects the uniform application of directives across the EU. Because, if the transposition of the NIS Directive by the Member States, studied here, was legally compliant in the short term. The application and the enforcement of the national laws of transposition risk highlighting, in the long term, the extent of regulatory divergences on the protection of network and information systems across the EU.

ACKNOWLEDGEMENT

I would like to thank everyone who has given me their support and encouragement during all these years of work.

First, I would like to thank my thesis supervisor, Mr. Fabien Terpan, for the continuous support, interest, and patience they have shown throughout my doctoral studies at the University of Grenoble Alpes. His advice, as well as his important comments, remarks, and suggestions, have constantly encouraged me in my academic research. I also thank the Grenoble Cybersecurity Institute for the funding it offered me throughout my research (as part of the IDEX Research-CDP2 and CESICE project - ANR-15-IDEX-02).

I would like to thank several people who have supported me since the first time I have been involved in cybersecurity: members of the Grenoble Doctoral School, members of the Grenoble Cybersecurity Institute and in particular, Mr. Philippe Elbaz-Vincent and Mrs Karine Bannelier Christakis, as well as the members of CESICE.

Finally, I am grateful for the love, kindness, and patience my family and friends have shown. Without their support and encouragement, I would not have even begun my doctoral studies.

REMERCIEMENTS

Je tiens à remercier toutes les personnes qui m'ont apporté leur soutien et encouragements pendant toutes ces années de travail.

Tout d'abord, je voudrais remercier mon directeur de thèse Monsieur Fabien Terpan pour le soutien continu, l'intérêt et la patience dont ils ont fait preuve tout au long de mes études doctorales à l'Université de Grenoble Alpes. Ses conseils, ainsi que ses commentaires, remarques et suggestions importants, m'ont constamment encouragé dans mes recherches académiques. Je remercie aussi l'Institut de Cybersécurité de Grenoble pour le financement qu'il m'a offert tout au long de ma recherche (dans le cadre du projet de IDEX Recherche- CDP2 et le CESICE - ANR-15-IDEX-02).

Je tiens à remercier un certain nombre de personnes qui m'ont soutenu depuis la première fois que j'ai été impliqué dans la cybersécurité: les membres de l'Ecole doctorale de Grenoble, les membres de l'institut de Cybersécurité de Grenoble et notamment, Monsieur Philippe Elbaz-Vincent et Madame Karine Bannelier Christakis, ainsi que les membres du CESICE.

Enfin, je suis reconnaissant envers ma famille et mes amis pour l'amour, la gentillesse et la patience dont ils ont fait preuve. Sans leur soutien et leurs encouragements, je n'aurais même pas commencé mes études doctorales.

A mes parents / To my parents.

"Μὴ φεύγειν τοὺς πόνους ἢ μηδὲ τὰς τιμὰς διώκειν."

Thycidides,

Histories B', 2.63.1

Summary

List of Abbreviations

A-

AFET: *Committee on Foreign Affairs*

AFSJ: *Area of Freedom, Security and Justice*

AG: *Advocate General*

ALDE: *Alliance of Liberals and Democrats for Europe*

ANSSI: *National Information Systems Security Agency*

ARCEP: *Regulatory Authority for Electronic Communications, Posts and Press Distribution (ARCEP)*

B-

BERC: *Body of European Regulators for Electronic Communications*

C-

C3: *Luxembourg Cybersecurity Skills Centre*

CEE: *Central and Eastern Europe*

CASES: *Cyberworld Awareness & Security Enhancement Services*

CDPC: *European Committee on Crime Problems*

CEPOL: *European Union Agency for Law Enforcement Training*

CERT: *Computer Emergency Response Teams*

CFSP: *Common Foreign and Security Policy*

CG: *Cooperation Group*

CICREST: *Interministerial Commission for the Coordination of Networks and Electronic Communications Services for Defense and Public Security*

CIIP: *Critical Information Infrastructure Protection*

CIRCL: *Computer Incident Response Centre Luxembourg*

CJEU: *Court of Justice of the European Union*

CLS: *Council Legal Service*

CME: *Coordinated Market Economies*

CNIL: *National Commission for Informatics and Liberties*

CNPD: *Luxembourg Commission for Data Protection*

COREPER: *Comité des Représentants Permanents*

CSDP: *Common Security and Defence Policy*

CSIRT: *Computer Security Incident Response Teams*

CSSF: *Financial Sector Supervisory Commission*

CTIE: *Luxembourg Information Technologies Centre*

CUN: *Charter of the United Nations*

D-

DECC: *Department of Communications, Climate Action and Environment*

DG CONNECT: *Directorate General for Communications Networks, Content and Technology*

DG INFSO: *Directorate-General for the Information Society*

DG HOME: *Directorate-General for Migration and Home Affairs*

DG GROW: *Directorate-General for the Internal Market, Industry, Entrepreneurship and SMEs*

DG MOVE: *Directorate-General for Mobility and Transport*

DG FISMA: *Directorate-General for Financial Stability, Financial Services and Capital Markets Union*

DME: *Dependent Market Economies*

DPC: *Data Protection Commission*

DPO: *Data Protection Officer*

DSM: *Digital Single Market*

DSP: *Digital Service Provider (DSP)*

E-

EC3: *European Cybercrime Centre*

ECB: *European Central Bank*

ECEJ: *European Commission for the Efficiency of Justice*

ECR: *European Conservatives and Reformists*

ECTC: *European Counter Terrorism Centre*

ECTEC: *European Cybercrime Training and Education Group*

EDA: *European Defence Agency*

EDPB: *European Data Protection Board*

EEAS: *European External Action Service*

EEC: *European Economic Community*

EETT: *Hellenic Telecommunications and Post Commission*

EFD: *Europe of Freedom and Direct Democracy*

EKA: *Hellenic Security Regulation*

EMSC: *European Migrant Smuggling Centre*

ENF: *Europe of Nations and Freedoms*

ENISA: *European Union Agency for Cybersecurity*

EPCIP: *European Programme for Critical Infrastructure Protection*

EPP: *European People's Party*

EPPO: *European Public Prosecutor's Office*

ESOCC: *European Serious Organized Crime Centre*

EU: *European Union*

EU-CSS: *European Union Cyber Security Strategy*

EUGS: *European Union Global Strategy*

EUISS: *European Union Institute for Security Studies*

EUROJUST: *European Union Agency for Criminal Justice Cooperation*

EUROPOL: *European Union Agency for Law Enforcement Cooperation*

F-

FAP-GC: *First Additional Protocol to the Geneva Conventions of 1949*

FICORA: *Finnish Communications Regulatory Authority*

FR7: *Seventh Framework Programme for Research and Technological Development*

G-

GCS: *Government Centre for Security*

GDPR: *General Data Protection Regulation*

GNCCB: *Garda National Cyber Crime Bureau*

GUE / NGL: *European United Left / Nordic Green Left*

H-

HCPN: *High Commission for National Protection*

HPDPA: *Hellenic Personal Data Protection Authority*

HR/VP: *High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission*

I-

ICJ: *International Court of Justice*

ICT: *Information and communications technology*

ICTY: *International Criminal Tribunal for the former Yugoslavia*

IHL: *International Humanitarian Law*

ILR: *Luxembourg Regulatory Institute*

IMCO: *Committee on the Internal Market and Consumer Protection*

INTRE: *Committee on Industry, Research and Energy*

IoT: *Internet of Things*

ISA: *Poland's Internal Security Agency*

ISS: *Information Systems Security*

J-

JHA: *Justice and Home Affairs*

JRC: *Joint Research Centre*

JURI: *Committee on Legal Affairs*

K-

KEMEA: *Hellenic Centre for Security Studies*

L-

LED: *Law Enforcement Directive*

LIBE: *Committee on Civil Liberties, Justice and Home Affairs*

LME: *Liberal Market Economies*

LSA: *Lead Supervisory Authority*

M-

MEP: *Member of the European Parliament*

MP: *Member of the Parliament*

MDSD: *Most Different Systems Design*

MSSD: *Most Similar Systems Design*

N-

NATO: *North Atlantic Treaty Organization*

NCA: *National Competent Authority*

NCSC: *National Cyber Security Centre*

NCSS: *National Cyber Security Strategy*

NESA: *National Emergency Management Agency*

NIS: *Network and information systems*

NGO: *Non-Governmental Organisation*

O-

OCLCTIC: *Central Office for the Fight against Crime related to Information and Communication Technologies*

OECD: *Organisation for Economic Co-operation and Development*

OES: *Operators providing Essential Services*

OLAF: *European Anti-Fraud Office*

P-

PESCO: *Permanent Structured Cooperation Framework*

PPPs: *Public-Private Partnerships*

Q-

QMV: *Qualified Majority Voting*

S-

S&D: *Progressive Alliance of Socialists and Democrats in the European Parliament*

SERIMA: *Security Risk Management*

SPOC: *Single Point of Contact*

T-

TEU: *Treaty on European Union*

TFEU: *Treaty on the Functioning of the European Union*

TRAFICOM: *Finnish Transport and Communications Agency*

TSG: *Threat Sharing Group*

U-

UKE: *Office of Electronic Communications*

UN-GGE: *United Nations Group of Governmental Experts*

UNSC: *United Nation Security Council*

US: *Unite States*

V-

VAHTI: *Government Information Security Management Board*

VoF: *Varieties of Capitalism*

W-

WP-TELE: *Working Party on Telecommunications and Information Society*

List of Appendix

List of Tables and Figures

“ La directive intrigue, dérange, divise, sa singularité en est la cause[1] ”.

Robert Kovar, 1987

[1] R. Kovar, ‘Observations sur l’intensité normative des directives’, in P. Pescatore (ed), *Liber amicorum*, (Nomos Verlag, 1987), 359

Introduction

Threats upon national infrastructures are constantly on the increase around the world. Technological development, innovation and interconnectivity with anyone or anything from almost anywhere has radically changed the way we communicate, as well as the way societies function. The risks on the so-called Internet of Things (IoT), which refers to a network that connects uniquely identifiable things[1] to the internet, have indeed increased. The disadvantage of today's interconnection is that it creates vulnerability to cyber-attacks, which are designed to access sensitive corporate and personal data or interrupt services. As connected society and IoT continue to challenge the *status quo* of states and citizens' behaviour on information security practices, the evolution of technology and innovations veils added risks.

On April 29th, 2007, the Estonian public and private institutions' servers were suddenly submerged by millions of requests. Sent massively, these floods of requests quickly saturated the relevant sites, making them inaccessible. On May 10th, the country's leading bank, *Hansapank*, was forced to close its online services for several hours. On May 15-16th, the second biggest establishment in Estonia, *SEB Eesti Uhispank*, was also hit. A real nuisance, when it is known that 99% of banking transactions in the small Baltic republic are realized via the Internet. In December 2012, the first confirmed cyberattack against a German power utility took place[2]. During this cyberattack one of the four most powerful companies in the world suffered from this incident[3].

A wide net of ransomware cyberattacks targeted a large number of European companies and institutions in June 2017. Banks, the national electricity supplier, Kiev airport, administrations and the metro were affected. In the United Kingdom, the advertising group WPP also acknowledged that its IT systems had been targeted. The ransomware also affected the working operations of the National society of French railroads (Société Nationale des Chemins de fer Français – SNCF) outside of Saint-Gobain. The Danish shipping company Maersk was also reporting problems, notably on its terminals in the Belgium port of Zeebrugge.

This reveals not only the immense importance of the cyberspace for political, economic, and social transactions within the European Union (hereafter the Union or EU) but also in its relations with other international actors. In response to this widespread phenomenon, the Cooperative Cyber Defence Centre of Excellence (hereafter CCDCE) in Tallinn (Estonia) hosted a multi-year process designed to provide the views of a high-level experts group on the application of international law to cyber activities.

---

[1] Available at https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (accessed on March 14th, 2018)

[2] Available at https://www.euractiv.com/section/energy/news/european-renewable-power-grid-rocked-by-cyber-attack/ (accessed on March 14th, 2018)

[3] *Ibid*

Two years after the publication of the United States (hereafter US) International Strategy for Cyberspace,[1] the High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the Commission (hereafter HR/VP), Federica Mogherini, and the European Commission (hereafter Commission) presented in February 2013, the first European Union Cyber Security Strategy (EU-CSS).[2] In this document, the European Commission defines cybersecurity as

> "*the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein*".[3]

Compared to the United States' conception, the Union's approach on cybersecurity issues tends to bring a more effective response to cyber threats and attacks by promoting the protection of human rights and freedoms through an open and free cyberspace. The EU-CSS outlines the EU's vision to strengthen the level of EU's cybersecurity and its capabilities by enhancing *inter alia* cooperation between Member States.[4] Moreover, it defines strategic priorities and actions, and asks Governments "*to safeguard access and openness, to respect and protect fundamental rights online, to maintain the reliability and interoperability of the Internet*". Among these priorities we can find the Cyber resilience, which objectively recognizes "*the insufficient effectiveness of preventive security measures, be they political, organisational, managerial, legal or technical*"[5], and draws on an analysis of what happens when a digitally networked system is being attacked. Following this, the European Commission has developed – through a communication followed by a Directive – a policy on network and information systems (hereafter NIS) to enhance cyber resilience.

Cybersecurity incidents[6] may threaten the functionality and effectiveness of critical infrastructures that provide services essential to the proper functioning of our societies, such as finance, health, energy or transport. These infrastructure systems are based on the integrity and security of NIS. Since the beginning of the 21st century, network and information systems have been perceived across the EU as a key factor to economic and

[1] Available at https://www.justsecurity.org/17729/time-u-s-international-strategy-cyberspace/ (accessed on December 20th, 2018)

[2] European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013, JOIN(2013) 1; which the Council of the EU (Council) welcomed on 25 May 2013

[3] *Ibid*

[4] See G. Ramunno, 'EU Cyberdefence Strategy,' (2014) *European Union Military Committee* 6

[5] See S. Ghernaouti and C. Aghroum, 'Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cybersécurité', (2012) 4 *Sécurité et stratégie* 11

[6] Intentional or accidental

societal development[1]. This led the Commission to define NIS security as "*the ability of a network or an information system to resist accidental events or malicious actions at a given level of confidence*"[2] that could "*compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted data as well as related services offered via these networks and systems*"[3].

Disruptions to the EU internal market, rising number, frequency, and complexity of NIS incidents, as well as the incomplete view of their frequency and gravity, undermined consumer confidence in the internal market since the beginning of the 21st century. The European Programme for Critical Infrastructure Protection (hereafter EPCIP)[4] and the Strategy for a Secure Information Society,[5] which were adopted by the Commission, urged the Member States to increase their NIS infrastructures and to cooperate in resolving cross border NIS issues. The Council of the European Union, the European Parliament and the European Commission agreed therefore that a change was needed in the way the Union addresses the network and information security issues.

The Directive 2016/1148 of 6 July 2016 on measures for a high common level of security of network and information systems across the Union (hereafter NIS Directive), is then the first European directive adopted by the Parliament and the Council in line with its commitment[6] for building a digital environment where economic and social potential may be expressed. Following the adoption of Directive 2002/21/EC[7] on a common regulatory framework for electronic communications networks and services (also known as Framework Directive) reformed by Directive 2009/140/EC[8], the implementation of the EPCIP and the adoption of the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (also known as GDPR)[9], the NIS Directive is the cornerstone of the EU's efforts to strengthen its global cybersecurity.

---

[1] European Commission, Communication on 'Network and Information Security: Proposal for A European Policy Approach', COM(2001)298.

[2] Malicious actions are software's, such as viruses, which can disable computers, delete or modify data.

[3] European Commission, Communication on '*Network and Information Security: Proposal for A European Policy Approach*' COM(2001)298.

[4] European Commission, Communication on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final ; Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM(2009) 149 final ; Communication on Critical Information Infrastructure Protection – 'Achievements and next steps: towards global cyber-security', COM(2011) 163 final ; Council of the European Union, Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[5] European Commission, Communication on a 'Strategy for a Secure Information Society' (COM(2006)251), from which the main elements of this strategy were endorsed in a Council Resolution 2007/068/01.

[6] European Commission, Communication on 'Digital Agenda for Europe', COM(2010) 245 ; on "Stockholm Programme/Action Plan" COM(2010) 171 ; on 'EU Internal Security Strategy in action' COM(2010) 673.

[7] OJ L 108, 24.4.2002, p. 33–50

[8] OJ L 337, 18.12.2009, p. 37–69

[9] OJ L 119, 4.5.2016, p. 1–88

The NIS Directive intends of building resilience throughout cybersecurity capabilities development, better cooperation between the Member States and undertakings in major key areas[1], while underlining the need for a coherent EU cyber-friendly international policy. It focuses primarily on the regulation of Operators providing Essential Services (hereafter OES) for the maintenance of economic and societal activities, e.g., energy, transport, financial market infrastructure or health sector; and the regulation of the Digital Service Providers (hereafter DSPs) in the domains of cloud services, online marketplaces and search engines. The NIS Directive sets two primary obligations for these stakeholders[2]: to establish a security management system against threats to NIS; and to advise the authorities "*without undue delay*" of any consequent security breach. In achieving its objectives, the NIS Directive combines maximum and minimum harmonization requirements. The Directive also imposes several obligations to EU Members States, which are mostly obligations of result as Member States must take the proper measures in its national legal order in giving full effect to the Directive[3].

The NIS Directive came into force in August 2016. Member States had 21 months, until May 9th, 2018, to meet with their obligation to transpose the Directive into national law and had another 6 months to identify the OES. Although EU Member States progressed in adopting their national strategy on the security of NIS, there were still important delays on NIS Directive transposition across the Union. Hence there are a number of reasons why this directive should not be fully effective. As regards the EU, the cross-cutting nature of cybersecurity may affect its legal framing on the matter as cybersecurity may relate to policies were the EU does not have full competence. The nature of the *instrumentum* used and the type of obligation contained within it, may also be relevant.

At national level, the impact of domestic factors may also affect the transposition's outcome. The extent to which EU Member States may have recourse to the discretionary room left by NIS Directive's obligation should be taken in consideration. It is important to precise here that NIS Directive transposition has resulted in important delays across the Union[4]. The Policy and institutional misfit, as well as the administrative effectiveness may also have an important impact on NIS Directive transposition. Drawing on this, and in order to have a clearer view of EU cybersecurity in law and in practice, the present PhD thesis is assesing the effectiveness of the NIS directive by distinguishing between the nature of the EU's norms and their transposition throughout European directives.

---

[1] Companies, with the exception of telecommunication operators ('undertakings providing public communications networks or publicly available electronic communications services') and public administrations are not subject to NIS requirements and are not required to report security incidents.

[2] NIS Directive, recitals 47 and 49

[3] Article 288 of the Treaty on the Functioning of the European Union (TFEU) : *a directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and method*

[4] Austria, Bulgaria, Belgium, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, and Romania, still had not fully transposed the NIS Directive on September 19th, 2018, although they had adopted a series of measures.

The concept of the effectiveness of law became one of the cardinal concepts of the legal theory in the middle of the 20th century. *Michel Virally* makes extensive references to it in his work on legal thought published in 1960[1]. Defended in 1962, the thesis of *Paul Amselek* marks important developments on legal thought by affirming that "*the study of the effectiveness ruled by legal norms, questions the very nature of a legal norm, while the analysis of the effectiveness of legal norms concerns the question of their implementation*"[2]. Naturally, the ineffectiveness of the law will refer to the idea that it is not applied by the authorities responsible for its implementation and / or by the competent judge to sanction the violations to which it is the subject. The effectiveness of a norm therefore depends either on the conformity of the behaviour followed by its recipients or by the authorities responsible for its implementation (compliance), or on the sanction against those who do not follow the rule (infringement).[3] The effectiveness of EU law is a question explored since the beginning of European integration but still always left open to interpretation.

Since its origin, various European scholars have constructed a traditional narrative on the effectiveness of Union law over conflicting national law. According to this narrative, Union law must prevail and deploy full effect over national law in all circumstances, including constitutional law. However, various authors intended to deviate from the classical meaning of equating effectiveness with the application of the legal norm.[4] The present thesis holds the view of *François Ost* and *Michel van de Kerchove*. According to them, effectiveness is an extremely complex notion which they define, at first glance, as "*the ability of the rule to orient the behaviour of its recipients in the direction desired by the legislator*".[5] They start from the idea that the legal norm is a benchmark for actions. Therefore, if the subjects of law are guided, in part, according to legal norms, it is not necessarily for applying them.

Indeed, in this context, what counts is not that the rule of law is respected and applied, but it is the circumstance that it can be used, mobilized by the subjects of law or the State authorities of application. As far as the EU is concerned, those circumstances are defined for the most by domestic factors. In his work on domestic politics, *Falkner et al.* argues that "*policy makers primarily implement directives in a correct and*

[1] M. Virally, *La pensée juridique* (Panthéon Assas (Eds), 1960), 137

[2] P. Amselek, *Perspectives critiques d'une réflexion épistémologique sur la théorie du droit* (LGDJ, 1964), 340

[3] J. Carbonnier, *Flexible droit. Pour une sociologie du droit sans rigueur* (Paris: LGDJ, 1998); P. Lascoumes, 'Effectivité', in A.-J. Arnaud (eds), *Dictionnaire encyclopédique de théorie et de sociologie du droit* (LGDJ, 1993); H. Kelsen, *Théorie générale des normes* (Paris : PUF, 1996) ; P. Malinvaud, *Introduction à l'étude du droit. Cadre juridique des relations économiques* (Paris : Litec, 1992); J.-L. Aubert, *Introduction au droit et thèmes fondamentaux du droit civil*, (Paris : Armand Colin, 1984)

[4] O. Bloch and W. von Wartburg, *Dictionnaire étymologique de la langue française* (Paris : PUF, 2004); F. Ost and M. van de Kerchove, *De la pyramide au réseau. Pour une théorie dialectique du droit* (Brussels: Publications des Facultés universitaires Saint-Louis, 2002); C. Mincke, 'Effets, effectivité, efficience et efficacité du droit : le pôle réaliste de la validité', (1998) *Revue interdisciplinaire d'études juridiques*, 40

[5] F. Ost and M. van de Kerchove, *De la pyramide au réseau. Pour une théorie dialectique du droit* (Brussels: Publications des Facultés universitaires Saint-Louis, 2002), 329.

prompt manner if EU provisions do not clash with domestic politics and interests"[1]. Consequently, the present Phd thesis will furthermore aim to highlight the need for legal studies to include domestic politics when studying European integration and more specifically, compliance to EU law. In so doing, it seeks to create a bridge between law and politics.

Seen from the angle of legal effect and legal application made by the rule of law, effectiveness is thus a concept which is inviting us to relate the nature of the legal rule (legal framing) to the behaviours it induces (implementation).

Studying Effectiveness

Effectiveness and legal framing

Framing is considered as a sort of strategy fort framers, like EU institutions or interest groups, which seek to "*shape the debate surrounding a policy issue with the aim of influencing policy outcomes towards their preferred direction*"[2]. Throughout legal framing, or framing through law, policy actors can play a crucial role in public policy debates and impact on their outcomes.[3] Yet, while framing studies have distinguished "*between legal, technical, economic, and political information, earlier European research literrature has shown marginal interest in examining the role of law in framing processes*.[4] Rather than refering to two distinct legal orders that coexist, it seems more appropriate to refer to a multilevel one mixing the legal orders of the Member States and the European Union.

By means of the EU treaties, the Member States of the EU have not only endorsed reciprocal obligations, but they have also established an independant legal system to the national legal orders. The European Union has a number of legal instruments to its disposal to put into action this *autonomous* legal system. These are used to make or coordinate policies, to take measures and initiate programmes, to facilitate the implementation of policies and to issue advice to Member States. Legal instruments are generally seen as being binding (Hard law – Directive, Regulation, Decision, etc.), but we must also add non-binding instruments (soft law). Therefore,

[1] See G. Falkner, M. Hartlapp and O. Treib, 'Worlds of Compliance: Why Leading Approaches to European Union Implementation Are Only "Sometimes-True Theories"', (2007) 3 *European Journal of Political Research* 46

[2] See R. Eising, D. Rasch and P. Rozbicka, 'Institutions, policies, and arguments: context and strategy in EU policy framing', (2015) 4 *Journal of European Public Policy* 22

[3] See F.R. Baumgartner and C. Mahoney, 'The two faces of framing – individual level framing and collective issue definition in the European Union', (2008) 3 *European Union Politics* 9

[4] P. Müller and P. Slominski, 'Legal framing and the EU's external relations: how NGOs shaped the negotiations for an Israel-Europol cooperation agreement', (2019) 6 *Journal of European Public Policy* 26

the present Phd thesis will try to get an understanding of how the EU's cybersecurity policy was framed – or to say it differently, in which manner hard and soft legal rules have been employed to frame the EU's cybersecurity regulatory behaviour.

Two main types of legal rules contribute to legal framing, those that fall under hard law and those that fall under soft law. The concept of soft law is largely debated among legal scholars[1]. Stemming from the traditional theory of legal acts, legal positivists usually say that law is either hard or not law at all.[2] The use of soft law therefore tends to blur the distinction between what is or not legally binding. The present thesis is based on *Fabien Terpan* assumption "*that there is a continuum running from non-legal positions to legally binding and judicially controlled commitments with, in between these two opposite types of norms, commitments that can be described as soft law*"[3]. While the *instrumentum* (source), the *negotium* (content) and the mechanism of norm's control or sanction play an important role on the creation of hard law. Following the nature of the norm regarding soft law, either the obligation is not clearly established, or the obligation is established but has no control mechanism[4].

As it has been already said in the previous developments, legal norms are a a benchmark for actions. Therefore, if the subjects of law are guided, in part, according to legal framings. This does not necessarily lead to a systematic and correct application. Therefore, effectiveness is not only about legal framing but also about implementation.

Effectiveness and implementation

Directives are the most used legal tools in the EU. They are part of the EU law that Member States must transpose first into national law and then apply. The implementation of directives requires however (1) a transposition into national law and (2) an application by all national actors. Due to the relative short delay of application of the NIS Directive and the lack of decisions from the European and national courts,[5] the present

[1] See C. R. Rossi, 'The club within the club: the challenge of a soft law framework in a global Arctic context', (2015) 1 *The Polar Journal* 5; See also J. Ellis, 'Shades of Grey: Soft Law and the Validity of Public International Law', (2012) 2 *Leiden Journal of International Law* 25; L. Blutman, 'In The Trap of A Legal Metaphor: International Soft Law', (2010) 3 *International and Comparative Law Quarterly* 59

[2] See J. d'Aspremont, 'Softness in International Law: A Self-Serving Quest for New Legal Materials', (2008) 5 *The European Journal of International Law* 19; See also J. Sztucki, 'Reflections on international 'soft law'", in L. Ramberg, O. Bring and S. Mahmoudi (eds), *Festskrift till Lars Hjerner* (Norstedts, 1990), at 549

[3] See F. Terpan, 'Soft Law in the European Union—The Changing Nature of EU Law', (2015) 1 *European Law Journal* 21

[4] *Ibid.*

[5] Having regard a research conducted on the website of the Court of Justice of the European Union until 4 April 2022, no litigation case was founded evolving a Member State of the EU. The Case C-763/18 P, Wallapop, SL v European Union

PhD thesis is however focusing only on the transposition phase of implementation. In this phase of implementation, transposition may variate between Member States in term of speed and lenght. The constraint of timely integrating European directives into national law is considered as the speed of transposition. While the extent of transposition refers to "*the degree of which the original directive is translated into national law*"[1]. However, the lengths of the discretionary room allowed to national actors by the European directive could obstruct in reverse order (in a bottom-up direction) the effective transposition of the directive or divert it from its objective.

Late transposition and incorrect application of EU directives may therefore lead to a legal uncertainty. In the field of cybersecurity, divergent outcomes on NIS Directive transposition may thus lead to a *non-compliance* phenomenon. Compliance is a "*(...) behaviour which conforms to a predetermined set of regulatory measures*"[2] and thus refers to the extent to which "*agents act in accordance with, and fulfilment of the prescriptions contained in (...) rules and norms*"[3]. Compliance in the context of the EU refers then to the extent to which the Member States complies with the provisions of the Treaties and all secondary regulatory measures. Acceptable levels of compliance may change over time and context. In the European Union, compliance is not recorded since not all violations with European law are discovered[4].

Compliance within the EU is to a widely measured by considering the available infringement data (Article 258 Treaty on the Functioning of the European Union), which are published by the European Commission in its the Annual Reports on Monitoring the Application of European Law. However, when compared to other sources of information the reports shows "*disturbing discrepancies and apparent errors*"[5]. Since those reports mainly "*provide information on the transposition of directives into national law and do not address practical compliance*"[6].

Intellectual Property Office (EUIPO), Unipreus, SL was the only case in which a reference of directive 2016/1148. However, the case concerned, among others, the misunderstanding or misapplication of the definitions of 'online marketplace' in Article 4(1)(f) of Regulation No 524/2013 and Article 4(17) of Directive 2016/1148 by the Court of Justice and not, by a Member State of the EU.

[1] F. Duina, 'Explaining legal implementation in the European Union', (1997) *International Journal of the Sociology of Law* 25

[2] See D. Matthews, 'Enforcement of Health and Safety Law in the UK, Germany, France and Italy', (1993) *Economic & Social Research Council Working Paper* 18, London: National Institute of Economic and Social Research

[3] Retrieved from J. T. Checkel, 'Why Comply? Constructivism, Social Norms, and the Study of International Institutions', (1999) *ARENA Working Papers, 99/24*, Oslo: Advanced Research on the Europeanisation of the Nation-State, p. 3

[4] See T. A. Börzel, 'Why do states not obey the law?', (2002) *Paper prepared for presentation at ARENA*, University of Oslo.

[5] R. Williams, 'The European Commission and the Enforcement of Environmental Law: an Invidious Position', (1994) *Yearbook of European Law* 14, p. 3

[6] See E. Versluis, '"The Achilles Heel of European Regulation". The Commission's Neglect of Enforcement', (2004) *Paper presented at the ECPR Joint Sessions of Workshops*, Workshop 'International Organizations and Policy Implementation', 13-18 April 2004, Uppsala, Sweden.

In Europeanisation research, transposition outcomes of European Directives have been mainly studied in terms of normative and practical implementation phases.[1]. Regarding the normative implementation, the main variables are the "*national constitutional characteristics*"[2], the complexity and poor quality of many directives[3], the range and complexity of existing national laws[4], the "*gold-plating*"[5], and the "*national legal culture*"[6]. Administrative explanations concern the existence of important barriers between preparation and implementation in many Member States and ministries[7], internal co-ordination problems[8], lack of resources[9], the inefficiency of national institutions[10].

In the mid-to-late 1990s, researchers such as *Börzel*[11] and *Duina*[12] refined the concept by stating that, the levels of compliance varies along with the degree of (mis-)fit between EU policy demands and existing national policies (Goodness-of-fit theory). Despite the disappointing empirical results of the misfit theory, various other authors have continued to use it. Looking for explaining the impact of the EU on the Member States, *Héritier*

---

[1] See T. A. Börzel and A. Buzogány, 'Compliance with EU environmental law. The iceberg is melting', (2019) 2 *Environmental Politics* 28; See also J. C. Fjelstul and C. Carruba, 'The Politics of International Oversight: Strategic Monitoring and Legal Compliance in the European Union', (2018) 3 *American Political Science Review* 112; A. Zhelyazkova and N. Yordanova, 'Signalling "compliance": The link between notified EU directive implementation and infringement cases', (2015) 3 *European Union Politics* 16;

[2] S. Krislov, C. Ehlermann and J. Weiler, 'The political organs and the decision-making process in the United States and the European Community', in M. Cappelletti, M. Seccombe and J. Weiler (eds), *Integration through Law: Europe and the American Federal Experience* (Walter de Gruyter, Vol. 1, 1986), p. 3

[3] See D. G. Dimitrakopoulos, 'The transposition of EU law: "post-decisional politics" and institutional economy', (2001) 4 *European Law Journal* 7; See also G. Ciavarini Azzi, 'The slow march of European legislation: the implementation of directives', in K. Neunreither and A. Wiener (eds), *European Integration after Amsterdam: Institutional Dynamics and Prospects for Democracy* (Oxford University Press, 2000), at 52; J. Weiler, 'The White Paper and the application of Community law', in R. Bierber, R. Dehousse, J. Pinder and J. Weiler (eds), *1992: One European Market* (Nomos, 1988), at 337

[4] See K. Collins and D. Earnshaw, 'The implementation and enforcement of European Community legislation', (1992) 4 *Environmental Politics* 1

[5] See D. G. Dimitrakopoulos, 'The transposition of EU law: "post-decisional politics" and institutional economy', (2001)

[6] See K. Collins and D. Earnshaw, 'The implementation and enforcement of European Community legislation', (1992) 4 *Environmental Politics* 1

[7] See J. From and P. Stava, 'Implementation of Community law: the last stronghold of national control', in S. S. Andersen, and K. A. Eliassen (eds), *Making Policy in Europe: The Europeification of National Policy Making* (Sage, 1993), at 55

[8] See D. G. Dimitrakopoulos, 'Learning and steering: changing implementation patterns and the Greek central government', (2001) 4 *Journal of European Public Policy* 8

[9]See also G. Ciavarini Azzi, 'The slow march of European legislation: the implementation of directives', in K. Neunreither and A. Wiener (eds), *European Integration after Amsterdam: Institutional Dynamics and Prospects for Democracy* (Oxford University Press, 2000), at 52

[10] See R. Lampinen and P. Uusikylä, 'Implementation deficit – why Member States do not comply with EU directives', (1998) 3 *Scandinavian Political Studies* 21

[11] See T.A. Börzel, 'Towards Convergence in Europe? Institutional Adaptation to Europeanisation in Germany and Spain', (1999) 4 *Journal of Common Market Studies* 37.

[12] See F. Duina, *Harmonizing Europe: Nation-States Within the Common Market* (State University of New York Press, 1999)

et al. proposed a revised framework [1]. They argue that "*adjustment to European policies depends on the stage of liberalisation already present in a Member State, the capacity for national reform, the costs of adaptation and the dominant belief system or the approach to problem solving*[2]".

In the last two decades, the european compliance literature produced a consequent know-how on the "*full or partial (non-) compliance with EU directives, the timeliness and correctness of transposition, the amount of non-compliance and transposition rates*"[3]. While undoubtedly relevant, the emphasis on compliance upon implementation process in EU research gave place to its opponents as it "*insufficiently captures the implications of Member States being part of a multilevel system*[4]", and "*tends to prejudge the EU as the main source of domestic change*[5]".

The NIS Directive as a Case Study of Law Effectiveness

The study of the NIS Directive offers us the opportunity to try dealing with the notion of legal framing firstly by getting an understanding of how *hard* and *soft* legal rules have been employed to shape the EU's cybersecurity policy and then, by studying how the *domestic politics* can be used, mobilised by the subjects of law or the State authorities to affect the transposition outcome of the NIS Directive. While cybersecurity triggers the emergence of a new field of research in European law and European Studies more generally,[6] the existing literature, when the present Phd thesis got started to be written, is mostly generalized and stays on the surface of NIS Directive.

A first strand of the related literature aims to understand the cyberthreats that Europe faces from a policy perspective view[7]. A second strand highlights the various developments in European Cybersecurity policy by

[1] See A. Héritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A-C. Douillet, *Differential Europe: New opportunities and restrictions for policymaking in the Member States* (Rowman and Littlefield, 2001)

[2] E. Mastenbroek, *The politics of compliance: explaining the transposition of EC directives in the Netherlands*, Doctoral Thesis, Department of Public Administration, Faculty of Social and Behavioural Sciences (Leiden University, 2007).

[3] See A.E. Töller, 'Measuring and comparing the Europeanization of national legislation: a research note', (2010) 2 *JCMS: Journal of Common Market Studies* 48

[4] See S.K. Schmidt, 'Beyond compliance: the Europeanization of Member States through negative integration and legal uncertainty', (2008) 3 *Journal of Comparative Policy Analysis: Research and Practice* 10

[5] See T.A. Börzel and T. Risse, 'From Europeanisation to diffusion: introduction', (2012) 1 *West European Politics* 35

[6] Retrieved from H. Carrapico and A. Barrinha, 'European Union cyber security as an emerging research and policy field', (2018) 3 *European Politics and Society* 19; See also R.S. Dewar, *Cyber Security in the European Union: An Historical Institutionalist Analysis of a 21st Century Security Concern*, (2017) PhD thesis University of Glasgow

[7] See J. Andreasson and J. Kim, *Cybersecurity : Public Sector threats and Responses* (CRC Press, 2012); See also I. Pernice, 'E-Government and E-Democracy: Overcoming Legitimacy Deficits in a Digital Europe?', in L. Papadopoulou, I. Pernice and J.H.H. Weiler, (eds), *Legitimacy Issues of the European Union in the Face of Crisis*, (Dimitris Tsatsos in memoriam, 2018), at 287; See also A.N. Guiora, *Cybersecurity: Geopolitics, law, and policy* (Routledge, 1st edn, 2017);

considering the EU as a relevant player both inside and outside its borders[1]. This is mostly due to the fact that cybersecurity can be seen as a cross-cutting policy area as it may not only concern EU's Digital Single Market (hereafter DSM), but also policies related to the internal market, the Area of Freedom, Security and Justice (hereafter AFSJ) and the Common Security and Defence Policy (hereafter CSDP) / Common Foreign and Security Policy (hereafter CFSP). Relevant references, for example, on self and co-regulation in Cybercrime, Cybersecurity and National Security[2] or on comprehensive normative approach to Cyber Security,[3] will be certainly used for the needs of the present thesis. However, few documents indicate the progress or the constraints that the NIS Directive transposition will generate among Member States confronted to their respective national rights.

The aim of the present research thesis is therefore to fill those gaps by assessing the effectiveness of the NIS directive through the study of the EU's cybersecurity legal framing on the one hand and the study of the transposition of the NIS directive on the other. The study of NIS Directive transposition will contribute to more generally better understanding the effectiveness of European directives[4]. As it has already been mentioned, the legal and practical implementation, as well as the enforcement of EU law are not exclusive prerogatives of the EU. Although EU legislation often refers to the European Commission for implementing measures, implementation by Member States remains the general rule. Like the discipline of political science, the field of law has also borrowed concepts and methods from other disciplines.[5] Considering thus that studying law and policy in the EU resides on a varied and multidisciplinary process, the present thesis will also use a law and politics perspective.

See also G. Christou, *Resilience and Adaptability in Governance Policy* (Palgrave Macmillan, 2016); See also K.J. Andreasson, *Cybersecurity: Public Sector Threats and Responses* (CRC Press, 1st edn, 2011).

[1] See E. Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking : Mapping the Internal and External Dimensions of EU Security', (2014) 1 *European Journal of Risk Regulation* 5; See also A. Bruni, 'Promoting Coherence in the EU Cybersecurity Strategy', in A. Vedder, J. Schroers, C. Ducuing and P. Valcke (eds), *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security* (Intersentia, 2019), at 253; See E. Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security', (2014) 1 *European Journal of Risk Regulation* 5

[2] See T. Tropina and C. Callanan, *Self-and Co-regulation in Cybercrime, Cybersecurity and National Security*, (Springer, 2015)

[3] E. Tikk-Ringas, *Comprehensive Normative Approach to Cyber Security*, (2015) ICT4PEACE Norms project.

[4] See E. Korkea-Aho, 'EU Soft Law in Domestic Legal Systems: Flexibility and Diversity Guaranteed?', (2009) 3 *Maastricht Journal of European and Comparative Law* 16; See also C. And one and S. Greco, 'Evading the Burden of Proof in European Union Soft Law Instruments: The Case of Commission Recommendations', (2018) 1 *International Journal for the Semiotics of Law* 31; F. Terpan, Soft Law in the European Union—The Changing Nature of EU Law, (2015) 1 *European Law Journal* 21

[5] P. J. Cardwell and M. Granger, *Research Handbook on the Politics of EU Law* (Cheltenham, UK: Edward Elgar Publishing, 2020); F. Federico, *The Law & Politics of Brexit* (New York, NY : Oxford University Press, 2018); M. Dawson, 'Better regulation and the future of EU regulatory law and politics Better regulation and the future of EU regulatory law and politics', (2016), 5 *Common Market Law Review* 53, 1209-1235; N. Scicluna, 'Politicization without democratization: How the Eurozone crisis is transforming EU law and politics', (2014) 3 *International Journal of Constitutional Law* 12, 545–571; C. Joerges and E. Vos, *EU Committees: Social Regulation, Law and Politics* (Oxford: Hart Publishing, 1999).

The present research thesis is thus divided into two parts. The first part is dedicated to the EU's legal framing of cybersecurity issues which was further hardened since the adoption of the NIS Directive. Focusing on the effectiveness of the European legal framework through the nature of the European norm, it will examine the EU's governance schemes on the development of a common cybersecurity policy, as well as the nature of NIS Directive's provisions which will serve as field of empirical study for the present thesis (**Part I**). The second part will focus on the implementation dimension of the effectiveness through the analysis of domestic factors (**Part II**).

Part I. The EU's Cybersecurity Legal Framework and the case of the NIS Directive

The effectiveness of the NIS directive depends on its legal framing. Both hard and soft legal rules have been employed by EU institutions in their framing ofthe EU's cybersecurity policy. European *hard* law is having a binding legal force, "*as producing general and external effects; being adopted by the Union institutions according to specific procedures; and having a legal basis in the founding Treaties*"[1]. However, between the non-legal positions and the legally binding commitments, it is possible to find instruments and norms that can be described as *soft* law.[2]

Soft law involves the use of non-binding rules that "*are nevertheless expected to produce effects in practice*"[3]. Among the non-binding instruments used by the EU, and especially by the Commission, we can find communications. The European Commission issues a wide variety of communications. In the field of cybersecurity, The Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions adopted on February 2nd, 2013, and entitled as, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, outlines the EU's vision to strengthen the level of EU's Cybersecurity and its capabilities by enhancing inter alia cooperation between Member States. The 2013 Cybersecurity Strategy (CSS) is defining strategic priorities and actions and sets above all the guidelines for legally framing the cybersecurity policy within the EU.

Since 2013, we assisted consequently in the hardening of cybersecurity policy with the adoption of two major directives information systems protection: Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA; Directive dealing with (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).[4]

Despite the absence of express competencies related to cybersecurity, the EU's activities have been triggered by the cross-border dimension of cyber threats. With its Member States being obliged to co-operate in many areas, voluntarily granting part of their sovereign rights to its institutions, the EU's legal framework became thus rich and complex at the same time. The first chapter will present the EU's cybersecurity legal framing, which moves between a variety of legal sources and governance structures (**Chapter I**), while the second

[1] L. Senden, *Soft Law in European Community Law*, (Hart Publishing, 2004), p. 45

[2] See F. Terpan, 'Soft Law in the European Union - The Changing Nature of EU Law', (2015) 1 *European Law Journal, Wiley*, 21

[3] D. Trubek, M. Cottrell and M. Nance, "Soft Law", "Hard Law", and European Integration: Toward a Theory of Hybridity, (2005) *University of Wisconsin Legal Studies Research Paper*, No. 1002.

[4] *Ibid*, p. 17

chapter will discuss the content and the binding nature of the obligations provided by the NIS Directive (**Chapter II**).

Chapter I. The Cross-Cutting Nature of Cybersecurity Rulemaking: Moving from Soft Law to Hard Law

A clear definition for cybersecurity cannot be found in the EU Treaties. Whenever we look in the treaties' provisions in the field of the CSDP or of the internal market and the AFSJ, no reference to cybersecurity is made.[1]

Cybersecurity in the EU starts with 1994 Bangemann's report[2] and the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data protection directive). But back then they did not call it cybersecurity. Furthermore, when the EU's mandate allowed it started acting on cybercrime. Thus, the initial focus was the telecom and data protection as well as the cybercrime offenses. Yet, all initial measures were justified as necessary for the proper functioning of the internal market. Nevertheless, after several earlier policy initiatives in the field, cybersecurity was defined with the adoption of the 2013 CSS[3] by the European Commission (updated in 2017[4] and 2020[5]) and the 2015 Council conclusions on cyber-diplomacy. A major step was taken with the adoption of the EU-CSS in 2013, since it has established the first comprehensive approach to the field of cybersecurity.

The EU's approach to cybersecurity is therefore scattered across three policy domains, which are affected by cyber-threats: the European Digital Single Market (DSM), the Area of Freedom, Security and Justice (AFSJ) and the CFSP/CSDP. Tthese domains, under the European Treaties, are very different in terms of comptences and powers, ranging from highly integrated (internal market) to mostly intergovernmental (CDSP). Therefore,

[1] Art. 43(1) TEU: 'The tasks referred to in Article 42(1), in the course of which the Union may use civilian and military means, shall include joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation. All these tasks may contribute to the fight against terrorism, including by supporting third countries in combating terrorism in their territories.'

[2] Europe and the global information society Recommendations of the high-level group on the information society to the Corfu European Council (Bangemann group). Available at http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf (accessed on January 22nd, 2022).

[3] See European Commission Communication 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 7 February 2013, JOIN(2013) 1 final.

[4] See European Commission Communication, 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', 13 September 2017, JOIN(2017) 0450 final.

[5] European Commission Communication 'EU's Cybersecurity Strategy for the Digital Decade', 16 December 2020, JOIN(2020) 18 final.

the EU's cybersecurity policy may vary from soft to hard governance according to the related policy domain, which may hamper the effectiveness of the EU norms in this field. Legal modes of governance range from supranational hierarchical governance, such as regulations and directives including legally binding commitments (Hard law), up to forms of soft governance that are intended to steer behaviour without legally binding action (Soft law). They also involve EU supranational and intergovernemental institutions in various ways. Using *Hooghe* and *Marks*' terminology, "*hard institutional governance relies on the institutional architecture that composes the EU polity: the European Commission, the Council of Ministers, and the European Parliament*"[1]. While soft institutional governance is characterised "*by mechanisms, implying flexible structures and task-specific policy-making arrangements, such as committees, forums, and networks*"[2].

The purpose of the present chapter will be to supply an overall landscape on proportions of hard and soft legal governance in the European cybersecurity policy mix (**Section I**), as well as on the modes of institutional governance used for (**Section II**).

Section I. EU laws and Policies in the field of Cybersecurity

The present thesis is desirous of exploring the linkages between law, policy, and cybersecurity. The cyberspace is considered to be a comprehensive sector that has no specific boundaries. The pervasive and cross-cutting nature of information and communication technologies – cyberspace matters included – provides thus the EU with an equally pervasive and cross-cutting position as a global actor in the field of cybersecurity. The 2013 EU-CSS was drafted as a cross-sectoral policy between DG Home Affairs, DG Connect, and the European External Action Service (with an active contribution from DG JUST). However, its implementation has been divided along three main streams with its own set of policies and legal framework: the critical information infrastructure protection, the cybercrime and the cyberdefence. Therefore, the first section will present evolutions on hardening the cybersecurity related legal framework of the EU in the European Digital Single Market and the Justice and Home Affairs policies (**§1**), while the second section will focus on external policies, and CFSP/CSDP more specifically (**§2**).

§1. Cybersecurity and EU Internal Policies: Hardening the Cybersecurity Legal Framework

[1] L. Hooghe and G. Marks, *Multi-Level Governance and European Integration* (Rowman and Littlefield Publishers, 2001).

[2] *Ibid*

In this paragraph, we will look into the harmonization of the cyber resilience across the European Digital Single Market (DSM), a Policy field where the EU has exclusive competences to regulate (**A**), before highlighting the EU's vision for a more *comprehensive* approach vision of EU's cybercrime law within the Area of Freedom, Security and Justice (AFSJ) (**B**).

A. The Digital Single Market Policy and Data Security: Harmonizing Cyber Resilience across the Union

When it comes to the DSM, we realize that there is a certain parallelism between the physical market and the digital market. The reliability and security of network and information systems are essential for economic and societal functions, and the functioning of the internal market. The European Commission has therefore justified the need for a coordinated action at EU level for building a DSM, as "*a space where individuals and businesses can access and develop online activities in a framework that guarantees fair competition and a high level of protection for consumers and personal data*"[1].

The impact of immateriality reached its peak with the recognition of the movement of data as the 5th freedom of the European single market, and it should be mentioned at this point that the legal nature of the DSM is questionable. It is indeed permissible to question its true place in the development of Union law by figuring out whenever it is only an attractive formula aimed at mechanically extending the single market to the digital domain, or if it takes on the characteristics of a true European Union policy, thanks to the development of transversal axes and principles which go beyond sectoral approaches.

The internal market legal framework, as we know it today, is the outcome of a long evolution.[2] A process which, from the origins of the European Economic Community (hereafter EEC) to the present day, has been characterized by close interconnection and alternation between the case law of the Court of justice and the revisions of the Treaties.[3] Article 2 of the 1957 Treaty of Rome establishing the EEC expressed the will of the *Founding Fathers* to establish a common market in order to guarantee the economic and social well-being of all Community's nationals. This expression, so vague and generic, was further clarified by the Court of Justice, in the *Schul case* of 5 May 1982, by ruling that "*the concept of a common market […] involves the elimination of all obstacles to intra-community trade in order to merge the national markets into a single market bringing*

[1] Council of the European Union 'Proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centre - Examination of possible compromise proposals and preparation for the trilogue', 26 March 2019, 7616/19 LIMITE, Available at https://data.consilium.europa.eu/doc/document/ST-7616-2019-INIT/en/pdf (Accessed on 04/12/2019).

[2] Interview 1

[3] See C. Blumann, B. Bertrand, L. Grard, F. Peraldi-Leneuf, Y. Petit and C. Soulard, 'Introduction au marché intérieur. Libre circulation des marchandises', in C. Blumann (eds), *Commentaire J. Mégret*, (Éd. de l'Université de Bruxelles, 3rd edn, 2015), at 9

about conditions as close as possible to those of a genuine internal market" [1]. In other words, it results that the common market, to which Article 2 of the EEC Treaty referred, does not only include the four freedoms of movement, but also seeks to remove any obstacle to trade between Member States, pursuing the final goal of creating a single large European market.

From the *Cassis de Dijon case*[2] to the Commission's 1985 White Paper[3] and from the 1986 Single European Act to Article 26§2 TFEU, the construction of the internal market has resulted through the abolition of the main barriers (physical, customs, fiscal, monetary etc.) to intra-Community trade. So, with a few exceptions linked to the cultural and socio-political specificities of the Member States (e.g., bets and games of chance as well as health), almost all goods, services, workers, and companies enjoy the freedom of movement. It is only in specific cases, which have been carefully analysed by the Court from the point of view of the proportionality test, that these fundamental principles are disentangled from.

The main obstacles to intra-Community trade have disappeared and a real European single market without internal borders has been created. However, this does not mean that the goal has finally been reached. On the contrary, the internal market is a constantly evolving phenomenon, which must be sustained throughout its development. However, digital has been an integral part of people's lives since the beginning of the 90's, especially with the first internet platforms. This moment marked the starting point of a digital revolution, which led to the increasingly rapid and uncontrolled diffusion of these new instruments in society. Therefore, this progress has led to considerable growth for the digital sector in just a few years.

It was therefore necessary to realise that the European market had grown.[4] The construction of the DSM was one of the strategic priorities of the Commission chaired by Jean-Claude Juncker. The appointment of a Vice-President, Andrus Ansip, in charge of the DSM and of the Commissioner for the digital economy and society, Günther Oettinger, reflected the strong ambition of the new Commission in this area.[5] The heavy task of carrying out a substantial reform package with 30 measures (regulations or directives) presented by the Commission was given to them. 28 from these 30 measures were adopted before the end of Commission's mandate. All attest to a resolutely pragmatic approach, promoted by a Commission concerned with efficiency and which has remained faithful to the logic of *problem solving*.

---

[1] Case 15/81, *Gaston Schul Douane Expediteur BV v Inspecteur der Invoerrechten en Accijnzen, Roosendaal*, ECLI:EU:C:1982:135

[2] Case 120/78, *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein*, ECLI:EU:C:1979:42

[3] Commission of the European Communities white paper from the Commission to the European Council, 28-29 June 1985, COM(85) 310 final.

[4] Interview 1

[5] European Commission Communication 'A coherent framework for building trust in the Digital Single Market for e-commerce and online services', 11 January 2012, COM(2011) 942 final.

The establishment of a free data flows throughout the adoption of the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons regarding the processing of personal data and on the free movement of such data (hereafter GDPR);[1] made the legal framework on the security of network and information systems stricter. So far, the legal framework mostly relied on a set of directives establishing in 2002 a common regulatory framework for electronic communications network[2], and on a number of communications from the Commission. The adoption of the Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereafter Directive NIS) marked the first EU-wide legislation on cybersecurity aiming to enhance the overall level of network and information systems' security in the EU. At the same time, the adoption of the Regulation (EU) 2019/881[3] established a European cybersecurity certification framework, which accomplished the digital market and led to the European cybersecurity legal framework hardening further.[4]

The NIS directive is therefore the centrepiece of a larger system of legal frames, such as the Free Flow of Data and Regulation (EU) 2019/881, which hardened the legal framework further by establishing a European cybersecurity certification framework.

1. The Free Flow of Data

Data protection is a field of EU law that has suffered substantial, if not ground-breaking, changes over the past years. In early 2012, the European Commission presented its proposals for the EU data protection reform package. This *package* comprised a proposal for a Regulation, the General Data Protection Regulation (intended to replace the 1995 EU Data Protection Directive[5]) and a proposal for a Directive, the Law Enforcement Directive[6] (intended to replace Framework Decision 2008/977/JHA on the protection of personal data processed

[1] European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

[2] Namely the Access Directive (2002/19/EC), Authorisation Directive (2002/20/EC), Framework Directive 2002/21/EC), and Universal Service Directive (2002/22/EC)

[3] European Parliament and Council Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69

[4] See B. Brunessen, (2021), 'Chronique Droit européen du numérique - La volonté de réguler les activités numériques', *RTDeur. Revue trimestrielle de droit européen* 1, p. 160

[5] European Parliament and the Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50

[6] European Commission (2012), Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention,

in the framework of police and judicial cooperation in criminal matters[1]). In April 2016, a five-year law-making process finally came to an end, with the formal adoption of the Regulation (EU) 2016/679 on General Data Protection Regulation (GDPR) and Directive (EU) 680/2016 on Law Enforcement (LED).[2]

Undoubtedly, the biggest change in the regulatory landscape regarding data confidentiality refers to the extension of the scope of the GDPR, as it applies to all companies that process personal data regardless of the place of business within the EU.[3] Before that, the application of the Directive locally was questionable. If for example one company had a location in country A of the EU but processed data of all citizens across the Union, then only the Data Protection Authority of country A was responsible for this processing. Furthermore, if there was no establishment in any EU country, then no European legislation had jurisdiction. This issue raised thus several cases falling under the jurisdiction of the supreme courts,[4] which the GDPR clarified by setting the limits of its applicability.

Therefore, the GDPR applies to the entities responsible for controlling and processing data within the EU, whether the processing takes place within the EU or not. These activities are related to the furnishing of products or services to EU citizens, regardless of whether payment is required or not, and to the supervisory behaviour taking place within the EU. Businesses outside the EU that process EU citizenship data should also appoint a representative within the EU. Special mention should also be made on the nomination of a Data Protection Officer (DPO). The primary role of the DPO is to ensure that "*his/her organisation processes the personal data of its staff, customers, providers, or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules*"[5].

The personal data breach notification procedure is another key innovation of the GDPR. In the case of a personal data breach, the controller has the obligation "*to communicate without undue delay and, where feasible, no later than 72 hours after having become aware of it, the personal data breach to the supervisory authority*

investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.

[1] Adopted 27 November 2008 and published in Official Journal 30 December 2008. Implementation deadline was 27 November 2010.

[2] European Parliament and Council Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016, L 119/89-131.

[3] See B. Brunessen, (2021), 'Chronique Droit européen du numérique - Perfectibilité de la protection des données personnelles', *RTDeur. Revue trimestrielle de droit européen* 1, p. 143

[4] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650; Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317; Case C-28/08 P., *European Commission v The Bavarian Lager Co. Ltd.*, ECLI:EU:C:2010:378; Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2008:54; Case C-139/01 (Joined Cases C-465/00, C-138/01, C-139/01), *Lauermann*, ECLI:EU:C:2003:294.

[5] Retrieved from https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"[1]. In the case of the notification to the supervisory authority not being made within 72 hours, it shall be accompanied by reasons for the delay.

The concept of *data protection by design* is furthermore introduced. This concept has been present for years but under the GDPR, it has now become a legal obligation. It is now therefore necessary to integrate data protection from the beginning of the design of the systems, rather than in the form of post-addition. When designing an application or system proper to technical and organisational measures must be taken to effectively meet the requirements of the GDPR and protect the rights of data subjects. Article 25 of the GDPR also sets the requirements for retention and processing of only the personal data, which is strictly necessary to fulfil the purpose of the processing (e.g., data minimization - principle of proportionality), as well as to limit the access to personal data, considered necessary to complete the processing. This is called data protection by default.[2]

Failure to comply with the GDPR requirements may thus result in significant penalties of up to 4% of their annual global turnover or 20 million euros (whichever is greater). This is the largest fine that can be imposed for the most serious infringements, such as failure to obtain a sufficient consent from the customer for processing personal data. It should be emphasized that this regulation applies to both the persons responsible for controlling and the persons responsible for processing personal data. The GDPR also promotes the concept of transparency on personal data processing. Therefore, those who process personal data must provide even more detailed information on the persons whose data is processed. The regulation (EU) 2018/1807[3] of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union reinforces the movement of data about non-personal data.

Non-personal data is defined as all data other than personal data referred to in article 4 of the GDPR. This residual definition has the advantage of covering a large amount of raw data, both public and private, their main characteristic being that it cannot be linked to natural persons. The processing of non-personal data is also defined, in an identical manner to that of the GDPR, as including "*any operation or any set of operations carried out or not using automated processes and applied to data or data sets under electronic form.*" The users of such processing can be both natural and public persons or private legal entities, and carry out these for professional or personal purposes. To guarantee the free flow of data, regulation intends to break down national "*digital barriers*" which could hinder them. The internal market is thus not only transformed by the assertion of the protection of personal data, but also by strengthening the free movement of non-personal data.

[1] Article 33 GDPR

[2] See T. Christakis, 'The relations between cybersecurity, data protection and privacy: a european perspective', in Ingolf Pernice, Jörg Pohle (Eds.), Privacy and Cyber Security on the Books and on the Ground, Berlin: Alexander von Humboldt Institute for Internet and Society, 2018, 26-30

[3] European Parliament and Council Regulation (EU) 2018/1807 of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, PE/53/2018/REV/1, OJ L 303, p. 59–68

When it comes to data protection, we usually think of data protection and the General Data Protection Regulation (GDPR). But often omits Directive (EU) 2016/1148 which aims to create a uniform legal framework for network and information system security. The establishment and the preservation of the Free Flow of Data forced therefore the EU for further hardening rules on network and information systems security.

2. Adopting the First EU-Wide Legislation Enhancing the Cyber Resilience of the Digital Single Market, Directive (EU) 2016/1148

Over the last ten years, the Commission has adopted multiple *soft* instruments,[1] in the form of communications, which aimed to enhance Network and Information Security in the EU. This approach has led to a fragmented cybersecurity legal landscape across the EU. In this context the adoption of Directive (EU) 2016/1148 (NIS Directive) represents thus the first EU-wide cybersecurity legislation intended to harmonize fragmented approaches of Network and Information Systems across the Union (**i**). The Commission favoured the Article 114 TFEU over the Article 196 TFEU as NIS Directive's legal basis, to push the harmonization process forward (**ii**).

i. The Fragmented Approach of NIS Security Legal Frameworks across the Union

Until the adoption of the NIS Directive, the European Union has held a more passive role in promoting network and information systems' protection issues[2]. This passiveness from the European Union together with no clear notion on what exactly cybersecurity is, has led the whole Union and its Member States to a lack of mutual understanding, but also a lack of harmonisation between Member States' related strategies[3]. For example, in Germany it is widely considered that protecting critical infrastructure is a task that must be

[1] Namely Communication on "i2010 – A European Information Society for growth and employment" COM(2005) 229 final; Strategy for a Secure Information Society COM(2006)251; Council Resolution on a Strategy for a Secure Information Society in Europe (2007/C 68/01); Communication on Critical Information Infrastructure Protection (CIIP) "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" COM(2009)149; Communication on A Digital Agenda for Europe COM(2010) 245 final; Communication on CIIP 'Achievements and next steps: towards global cyber-security' COM(2011) 163 final; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013).

[2] See K. R. Sliwinski, 'Moving beyond the European Union's Weakness as a Cyber-Security Agent', (2014) 3 *Contemporary Security Policy* 35, 468-469.

[3] K. R. Sliwinski, 'Moving beyond the European Union's Weakness as a Cyber-Security Agent', (2014) 3 *Contemporary Security Policy* 35, pp. 470-472.

conducted jointly by the government, companies and civil society.[1] The guiding principles are the relationships of trust in state-business cooperation at all levels and the existence of appropriate and proportionate measures to use resources to increase the level of protection. France defends the idea that the country should be a global power in cyber defense, while maintaining its autonomy, thus guaranteeing freedom of decision-making, the protection of national sovereignty information and the enhancement of the security of critical infrastructures.

To achieve these goals, seven axes have been created: Better environmental forecasting and analysis to make appropriate decisions, identify and respond to attacks, alert potential victims, and provide assistance, increase scientific, technical, and industrial skills, towards maintaining the necessary autonomy, protecting state-owned information systems and critical infrastructure operators, in order to improve national competitiveness, adapting laws to take account of technological developments, developing international partnerships in the field of information security, cybercrime, and cybercrime, communication, and information, so that French citizens can better understand issues related to the security of computer systems. Regarding Poland, the Poland Cyberspace Protection Program 2011-2016,[2] recommends actions to prevent and combat threats and includes proposals for legal, organisational, technical, and educational activities.

Although the European Union has promoted cooperation between Member States in different areas since 1999, this did not immediately lead to enhanced collaboration in the protection of network and information systems.[3] This is why over the last ten years the EU institutions have proposed and adopted multiple regulatory instruments which aim to enhance Network and Information Security in the EU. Since 1999, the *e*-Europe initiative[4] and the EU's Communication on Network and Information Security: Proposal for a European Policy Approach,[5] are the first documents highlighting the importance of information infrastructure protection. The importance of the security of the DSM was also recognized in the EU's i2010 initiative, which underlined the "*reliability and security of networks and information systems*"[6], as well as the European Commission's communication a "*Strategy for a Secure Information Society*"[7] that followed under the broader Digital Agenda

[1] See Federal Ministry of Germany, 'National Strategy for Critical Infrastructure Protection (CIP Strategy)', Berlin, 17th June 2009. Available at https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf?__blob=publicationFile (Accessed on January 3rd, 2022).

[2] Available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf (Accessed on December 4th, 2019).

[3] Interview 1

[4] Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_99_953 (accessed on December 4th, 2019).

[5] European Commission, Communication 'Network and Information Security: Proposal for A European Policy Approach', 6 June 2001, COM/2001/0298 final

[6] Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_05_643 (accessed on December 4th, 2019).

[7] European Commission Communication 'A strategy for a Secure Information Society - Dialogue, partnership and empowerment', 31 May 2006, COM/2006/0251 final

for Europe initiative[1]; the latter providing a comprehensive set of actions for managing the challenges presented by network and information security.

The communication pointed towards the need for the EU to "*develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment*"[2], on a three-pronged approach embracing: NIS security measures, the regulatory framework for electronic communications and the fight against cybercrime. The initiatives launched by the EC within these three dimensions were designed to complement the objectives outlined in the Commission's Green Paper on the EPCIP[3] underpinned by "*a security logic and sectoral approach which meant enhancing the security and resilience of network and information systems through a multi-stakeholder dialogue approach*"[4]. In this sense, the objective of the EPCIP was to "*receive feedback concerning possible EPCIP policy options by involving a broad number of stakeholders*" [5].

The process culminated with a 2008 Council directive that emphasised on "*the identification and designation of European critical infrastructures and an assessment of the need to improve their protection*"[6]. In particular, the directive defined the "*Critical Infrastructure"*[7] and "*European Critical Infrastructure"*[8] concepts, as also a common path for the identification and the protection of the European critical infrastructures. The identification by the directive of two areas in which the procedures for identifying European critical infrastructures must be applied – energy and transportation and their related sub-sectors – is noteworthy. The implementation of the directive imposed on Member States a set of requirements, which impacted the activities of the identified stakeholders as European critical infrastructure assets. The underlying rationale was to seek how it might be applied to other sectors, highlighting Information Communication Technologies (hereafter ICT) as a priority sector.

---

[1] European Commission Communication 'A Digital Agenda for Europe', 19 May 2010, COM(2010)245 final

[2] European Commission Communication 'A strategy for a Secure Information Society - Dialogue, partnership and empowerment', 31 May 2006, COM/2006/0251 final

[3] European Commission 'Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP)', 17 November 2005, COM/2005/0576 final.

[4] G. Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy* (Palgrave,2016), 122

[5] G. Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy* (Palgrave,2016), 122

[6] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, 23.12.2008, p. 75–82

[7] Assets, systems, or parts thereof located in European Union Member States, which are essential for the maintenance of vital social functions, security, safety, health and economic/social welfare of the population, and whose destruction or malfunction would have a significant impact in a member state (loss of service).

[8] Critical infrastructures located in European Union Member States whose destruction or malfunction would have a significant impact in at least two European Union Member States. The significance of the impact is to be assessed in terms of cross-cutting criteria, including the effects of cross-sector dependencies on other infrastructures.

In 2009, the European Commission drafted therefore a communication in 2009 for Protecting Europe from large-scale cyber-attacks and disruptions, which highlighted "*the need for achieving a security of resilience*"[1] and proposed an action plan to address key challenges. In the above context, the Critical Information Infrastructure Protection (hereafter CIIP) proposed, was based on a five pillars action plan: "*Preparedness and prevention; Detection and response; Mitigation and recovery; International cooperation; Criteria for European Critical Infrastructures in the Information and communications technology (ICT) sector*"[2]. But if in the review of the CIIP (2011)[3] conducted by the Commission, several achievements were noted related to each pillar. However, authors notify that "*certain initiatives were more successful than others with regard to enhancing the conditions necessary for security as resilience to emerge, in particular in relation to establishing sustainable platforms for effective public-private interaction and collaboration*"[4].

It should also be noted that in the review of the European Program for Critical Infrastructure Protection[5], the Commission concluded to a limited and irregular application, as there were wide discrepancies noted in the application of the Directive between Member States, even if quickly transposed in their national laws. The conclusions of the review also suggested that the sector-focused approach of the Directive represented a challenge to some Member States, as the analysis of criticalities is not restricted to sectoral boundaries but follows a systems approach, wider and therefore preferable. After the unsuccessful use of soft law methods[6], the Union legislators set its aims at more constructed regulation methods. The adoption of the NIS Directive in 2016, represents the first EU-wide cybersecurity legislation harmonising national cybersecurity capabilities, cross-border collaboration, and the supervision of critical sectors across the EU. The general and main rule used for the approximation of national legislations is the first article of Chapter 3 of the Treaty on the Functioning of the European Union (TFEU): Article 114, which has been described as of positive harmonisation.

ii. The NIS Directive's Legal Basis and The Choice of Article 114 TFEU, Pushing Harmonization Forward

In so far, the harmonization approach of the Commission was mostly intented in an economic perspective. Since digitalisation can be seen as a new catalyst for further expansion. The *digital single market* aimed to fully

[1] European Commission Communication 'Critical Information Infrastructure Protection (CIIP) – Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', 30 March 2009, COM(2009) 149 final

[2] *Ibid*

[3] European Commission Communication 'Critical Information Infrastructure Protection – Achievements and next steps: towards global cyber-security', 31 March 2011, COM(2011) 163 final

[4] See G. Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy* (Palgrave, 2016), 125

[5] European Commission Staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP), 22 June 2012, SWD(2012) 190 final

[6] It is important to note that the European Commission does not completely back down from the soft law methods, as the EUCSS does involve awareness raising exercises, transatlantic cooperation etc...

and comprehensively address the digital dimension of the single market. Conceptually, the DSM is built on the following four pillars: access to online goods and services, environment, digital networks and European digital economy.

As physical location becomes less important, territoriality as a presumption of nation state and sovereignty based legal systems is challenged. This global phenomenon required harmonising European legal framework to a greater extent. While the NIS Directive was finally adopted on the legal basis of article 114 TFEU. During the debates on the NIS Directive proposal, the Council's Legal Service (here after CLS) seems to have opted – in its opinion on the legal basis proposed in NIS Directive's proposal – for a legal basis combining articles 114 TFEU and the 196 TFEU.[1] The CLS argued that "t*he proposed Directive pursues two inextricably linked objectives, without one being secondary and indirect in relation to the other"*[2]. This hesitation, or controvery, makes it even more important to dedicate a few developments relating to this choice dilemma on legal basis.

Under European Union law, the legal basis can be defined as the provision of the treaty detailing the procedure for adopting an act in a given situation. By defining the applicable procedure, the legal basis of an act makes it possible to know the respective powers of the institutions in decision-making and establishes their relationships for the accomplishment of a common action or policy. The legal basis also makes it possible to obtain information on the field of action and therefore on the nature of the competence available to the Union, as well as possibly on the type of act which may be adopted by the institutions.

The Court of Justice has held that "*the choice of the appropriate legal basis is of constitutional importance*"[3] both in its vertical aspect – distribution of powers between the Union and the Member States – and in its horizontal aspect – procedure to be followed by the institutions of the European Union. These two elements represent two aspects of the attribution principle. The latter can in fact be broken down as follows: to adopt an act, the Union must be competent under a provision of the Treaty; this provision also grants powers to the institutions of the Union which must respect the procedure laid down by not encroaching on the powers granted to the other institutions. The choice of a legal basis is not always easy since a legislative measure may affect several policies or sub-policies which support different adoption procedures.[4] The Court of Justice has gradually refined the criteria for finding the appropriate legal basis. First, the choice must be made based on objective criteria formed by elements liable to judicial review, including, in the first place, the aim and content of the act. And the choice of the legal basis for the adoption of a measure depends on the content rather than title of the

[1] Council of the European Union, Opinion of the legal service on NIS directive proposal legal basis, 27 June 2014, 11395/14

[2] *Ibid*, p. 30 point 91.

[3] Case C-687/15, *European Commission v Council of the European Union*, ECLI:EU:C:2017:803

[4] See G. Marti, 'Les conflits de base juridique', in L. Clément-Wilz (eds), Le rôle politique de la Cour de justice de l'Union européenne, Bruxelles, Bruylant, 2019, pp. 73-100.

measure. Then, if an act pursues a double, or even a multiple purpose, it is necessary to find out if one of the aims is preponderant[1].

In the case of the DSM, the Commission using its right of initiative is generally opting for Article 114 TFEU[2] as a proper legal basis to adopt measures intended to ensure a high common level of security of networks and information systems in the Union. Article 114 TFEU is worded as follows:

> "*Save where otherwise provided in the Treaties, the following provisions shall apply for the achievement of objectives set out in Article 26. The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have the establishment and functioning of the internal market as their object*".

Following research carried out in the database of the EU law (Eur-lex) on the number of documents related to the digital market, we found that 35 legal acts were adopted within the period 2013 to 2018 (**Table 1**). For the research the advanced research function of the Eur-lex site has been used. The exact wordings researched in the legislative text were *digital dimension of the internal market* and *Digital Single Market*. Among the findings, 10 legal instruments, for the most regulations, have used the Article 114 TFEU either as a unique legal basis or as a combined one, and have the Council of the Union and the European Parliament for authors.

2013-2018		Legal basis					
Type	Authors	Treaties			Legislative acts		
		Art. 114 TFEU	Combined with Art. 114	Other(s)	Regulation	Directive	Decision
Regulation	European Commission	0	0	0	0	0	0
	Council of the European Union	0	0	1	0	0	0
	Council of the European Union, European Parliament	4	3	4	0	0	0
Directive	European Commission	0	0	0	0	0	0
	Council of the European Union	0	0	1	0	0	0
	Council of the European Union, European Parliament	1	1	3	0	0	0
Decision	European Commission	0	0	1	8	1	2
	Council of the European Union	0	0	1	0	0	0
	Council of the European Union, European Parliament	1	0	2	0	0	0

[1] *Ibid*, para 13 and 17

[2] Article 114 TFEU is worded as follows: Save where otherwise provided in the Treaties, the following provisions shall apply for the achievement of objectives set out in Article 26. The European Parliament and the Council shall, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee, adopt measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have the establishment and functioning of the internal market as their object.

Table 1: *Digital Market related legal documents with a legal basis analysis*

Table made by author and Source based on eur-lex data

When using Article 114 TFEU, the EU legislator can adopt measures "*for the approximation of laws in the Member States which have the establishment and functioning of the internal market*"as their objective.[1] Its use is a matter of controversies. This has been criticised for the last two decades as being an expanding legal basis. Its usage is considered to entail a risk for the EU legislator oversteping their competence and that the definition of measures have as their object the establishment and functioning of the internal market erodes.

According to the Court of Justice of the European Union (CJEU), a measure could be based on Article 114 TFEU "*only when the conditions for recourse to it are fulfilled*"[2]. In other words, the purpose is to improve the conditions for the establishment and functioning of the internal market and disparities between national rules; "*as to obstruct fundamental freedoms and thus have a direct effect on the functioning of the internal market or to cause significant distortions of competition*"[3]. Concerning cybersecurity more particularly, the EU legislator has already recognised the need to harmonise NIS rules to ensure the development of the Internal Market. This was the case for Regulation 460/2004[4] establishing ENISA, which is based on Article 114 TFEU. So, it makes sense somehow to having used the Article 114 TFEU as a legal basis for the NIS Directive.

According to the Opinion delivered on June 27th, 2014, by the CLS on the choice of article 114 TFEU as legal basis of the NIS Directive proposal, another basis could have been however also chosen. [5] A proposal for a combined legal basis has been therefore made from the CLS which uses the articles 114 TFEU and 196 TFEU on civil protection. Civil protection is the protection of people, the environment and property against natural and man-made disasters. In addition to deploying forces and equipment for emergency response, it also provides for planning and preparation for such events. This includes, among other things, conducting risk analyses and approving protection and rescue plans and procedures. EU action in the field of civil protection is covered by Article 196 TFEU.

This new legal basis has a very wide scope since it does not limit the areas in which the Union can act (e.g., health-related emergencies, environmental disasters, terrorism etc..). Likewise, the legal basis does not restraint Union action to physical areas (land, water, or air). As it can be seen bellow, in **Table 2**, Article 196 TFEU was

[1] Article 114 of the TFEU

[2] Case C-377/98, *Netherlands v. European Parliament and Council*, EU:C:2001:523, paras 27-28; Case C-491/01, *British American Tobacco (Investments) and Imperial Tobacco*, EU:C:2002:741, paras 93-94.

[3] Council of the European Union, Opinion of the legal service on NIS directive proposal legal basis, 27 June 2014, 11395/14

[4] European Parliament and Council Regulation (EC) No 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77, 13.3.2004, p. 1–11

[5] Council of the European Union, Opinion of the legal service on NIS directive proposal legal basis, 27 June 2014, 11395/14

only used for the adoption of two legal acts within the period 2013-2018, among which we denote, the decision 1313/2013/EU[1] on the Union civil protection mechanism.[2]

	Title	Type	Author	Domain	Legal Basis
1.	2014/364/EU: Council Decision of 12 June 2014 on the position to be adopted, on behalf of the European Union, within the EEA Joint Committee concerning an amendment to Protocol 31 to the EEA Agreement, on cooperation with specific fields outside the four freedoms	Decision	Council of the European Union	European Free Trade Association (EFTA)	Regulation (CE) n° 2894/94, Article 218 TFEU, Article 196 TFEU
2.	Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism	Decision	European Parliament, Council of the European Union	Safety at work and elsewhere, Cooperation	Article 196 TFEU, Article 294 TFEU

Table 2: *Article 196 TFEU related legal documents within period 2013-2018*

Table made by author and Source based on eur-lex data

According to decision 1313/2013/EU, the general objective and scope of the civil protection

"*cover primarily people, but also the environment and property, including cultural heritage, against all kinds of natural and man-made disasters, including the consequences of acts of terrorism, technological, radiological or environmental disasters, marine pollution, and acute health emergencies, occurring inside or outside the Union. In the case of the consequences of acts of terrorism or radiological disasters, the Union Mechanism may cover only preparedness and response actions*" [3].

The EU has therefore already considered that, the provisions for requirements related to Member States' risk planning and risk management are compatible with the EU's competence in the area of civil protection. It follows from this that "*Article 196 TFEU could be a suitable legal basis to cover the planning requirements and the requirements for the competent authorities within the network, provided that the nature and limits of Union competence in the area of civil protection and the principle of proportionality are respected*"[4]. But the most important consequence is that, for any measures under Article 196 TFEU the main role of the Commission is only to monitor the general implementation of any legislation and to coordinate, supplement and support Member States. This is therefore in line with the conclusion formulated by the CLS according to which, "*since the proposed Directive pursues two inextricably linked objectives, without one being secondary and indirect in*

[1] European Parliament and Council Decision 1313/2013/EU of 17 December 2013 on a Union Civil Protection Mechanism, OJ L 347, 20.12.2013, p. 924–947

[2] The same method has been followed as for the article 114 TFEU. The wording used this time for identifying related text was 'Having regard to the Treaty on the Functioning of the European Union, and in particular Article 196'.

[3] Article 1 para 2 of Decision 1313/2013/EU

[4] Council Opinion of the Legal Service, 27 June 2014, 11395/14, para 68

relation to the other, Article 114 TFEU and Article 196 TFEU may be a suitable dual legal basis for the proposed Directive as long as it is possible to identify which measure relates to which legal basis"[1].

However, it should be noted that CLS opinions are not legally binding acts, and it is ultimately up to the Council to decide whether or not to follow them in any given case. The CLS is part of the General Secretariat of the Council. Among other roles, the advisory role of the CLS consists of giving legal opinions to the Council (and European Council) or its preparatory bodies (working parties and COREPER), either orally or in writing, on any legal or institutional questions which may be raised during the Council's work.The CLS' advice may be given on questions such as whether the Commission has proposed the correct legal basis in the Treaty for a draft legislative act. CLS views are rarely ignored. Nevertheless, they are not always followed even if the CLS concluded in its opinion on the legal basis of the NIS Directive that "*Article 114 TFEU does not constitute a sufficient legal basis to cover the entire content of the proposal and the objectives it pursues*"[2].

The choice of Article 114 TFEU as the only legal basis for adopting the Directive NIS has prevailed. One plausible explication would be that article 196 TFEU was never combined with article 114 TFEU and mostly, has not been used as a legal basis for digital market related legal acts. The EU-wide cybersecurity certification is such an example.

3. EU-wide Cybersecurity Certification: Toward a Digital "CE"?

After enforcing the NIS Directive, the European institutions have continued their legislative efforts onlevelling the security framework of NIS. Following the adoption and the end of the transpositioning phase of the NIS Directive, the EU also gave more authorities to the EU Agency for Cybersecurity (hereafter ENISA) and established an EU-wide cybersecurity certification framework for digital products and services.

Adopted on April 9th, 2019, regulation (EU) 2019/881[3], the so-called Cybersecurity Act, is pursuing two essential goals for the development of the DSM namely, (a) the strengthening of citizens' confidence in its digital devices and (b) the harmonised enhancement of cybersecurity across the Union. To this end, the legislator aims to strengthen cooperation and the sharing of information within the various Member States. Furthermore, he would like to regularly assess the Union's cybersecurity to predict future challenges and threats as much as possible. With a view to enhancing the EU's experience in protecting information networks and systems, as well as people exposed to those threats, the regulation is developing an harmonised European cybersecurity

[1] Council Opinion of the Legal Service, 27 June 2014, 11395/14, para 91

[2] *Ibid*

[3] European Parliament and Council Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15–69

certification framework, for which Member States will have until June 28th, 2021, to comply. Specifically, the first strand of measures of the Cybersecurity Act relates to the enhanced role and mandate of ENISA, since ENISA had a temporary and limited mandate that expired in 2020. The Cybersecurity Act intends "*to reinforce the role of ENISA by guaranteeing a permanent mandate and allowing it to perform more operational tasks*"[1]. ENISA will also have a leading role in the management and support of the certification system introduced by the Cybersecurity Act.

More precisely, the Cybersecurity Act introduces an EU wide ICT security certification system for digital products and services that are essential for the proper functioning of the DSM. Given the presence of a wide variety and multiple uses of ICT products, services and processes, the EU is also implementing the mechanism of the European Cybersecurity Certification scheme. This scheme enshrines a set of standards and technical requirements common to all Member States' certification schemes; thereby correcting a fragmentation of the internal market and avoiding the practice of *certification shopping*. A practice which reflects manufacturer or seller behaviour to choose the country in which to obtain certification according to flexible security requirements.

The certificate to be issued will be recognized by all Member States in order to ease cross-border trade for businesses and users, and to understand the security features of the ICT product or service.[2] This allows beneficial competition between suppliers in the EU market, resulting in improved products and better value for money. Indeed, the Union denounces the urgency to adopt:

> "*a common approach and establishing a European cybersecurity certification framework, establishing the main horizontal requirements for the cybersecurity certification schemes to be developed and allowing recognition and use in all Member States of European cybersecurity certificates and European Union declarations of conformity for ICT products, ICT services or ICT processes*"[3].

It should be stressed that the certification mechanism cannot be self-sufficient and must be accompanied by real awareness on the part of the stakeholders and the development of a common culture of security. Thus, this regulatory framework also encourages manufacturers or suppliers, involved in the design and development of products, services or processes, "*to apply measures at the early stages of design and development (cyber-hygiene)*[4]. This will supply maximum protection for ICT product, service or process security to prevent and minimize the occurrence of cyberattacks (design-based security).

---

[1] Interview 5

[2] Interview 1

[3] Recital 69 of Regulation (EU) 2019/881

[4] Recital 8 of Regulation (EU) 2019/881

This framework is based on international standards as much as possible in order to avoid trade barriers or problems of technical interoperability. However, cybersecurity law requires the assessement, effectiveness and use of the approved European cybersecurity certification systems from the Commission. It will assess whether a specific European cybersecurity certification system should be made mandatory through relevant European legislation to guarantee an adequate level of cybersecurity for ICT products, services, and procedure.

If the European certification mechanism is set up to ensure coherent security harmonisation within the Union[1], the legislator allows the Member States to keep national certification schemes.That is if they are not covered before by a European scheme cybersecurity certification. Therefore, existing national certificates covered by a European scheme also remain in force until their end date. The legislator enjoins the Member States to refrain from creating new national certification schemes for ICT products, services and processes already guaranteed by a European scheme. Note, however, that the provision does not appear to be a prohibition in principle.[2] This can be explained by the fact that the regulation is mostly composed of obligations of results achieving thus a minimal harmonisation of national legislations (**Table 3**).

	Type of obligations			
	To act		**To abstain**	**Non-obligation (Voluntary)**
Actors	*Of result*	*Of means*		
Commission	23	9	0	10
European Union	3	0	0	0
ENISA	7	2	0	1
Member States	22	5	1	2
European Cybersecurity Certification Group (ECCG)	5	0	0	2
Manufacturer or provider of certified ICT products, ICT services or ICT processes or of ICT products, ICT services and ICT processes	4	0	0	1
Conformity Assessment Bodies	3	0	0	2

Table 3: *Provisions typology of Regulation (EU) 2019/881*

Table made by author with source based on NIS Directive

As stated at article 46§1 of the regulation (EU) 2019/881:

> "*The European cybersecurity certification framework shall be established in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity within*

[1] *Ibid*, Recital 66 and 67

[2] *Ibid*, Recital 941

the Union and enabling a harmonised approach at Union level to European cybersecurity certification schemes, with a view to creating a digital single market for ICT products, ICT services and ICT processes".

The basic philosophy of this vertical approach is to end technical barriers throughout the adoption of product-specific directives, which will set out all the technical details that manufacturers should follow if they want to release their products freely on the European single market. These common technical rules will replace therefore the national ones. However, this "technical" harmonising strategy is not new.

On May 7th, 1985, the Council issued a Resolution adopting a *new approach* upon technical harmonisation and standardisation of industrial products.[1] With a view to easing the accomplishment of the single market, it encourages the adoption of flexible and technologically neutral legislation. In fact, this Resolution included a draft of a Directive, on the basis of which the n*ew Approach* directives should be designed. This resolution was supplemented by a Council Resolution on a comprehensive approach to the issue of conformity assessment in 1989.[2] This was then followed by two other Council Decisions laying down more detailed specifications on testing procedures and certification, and guidelines for the use of CE conformity marking (CE, constituting the acronyms of the European Community in French), the latter being intended for use in the Harmonisation Directives (Decision 90/683/EEC[3], as replaced by Decision 93/465/EC,[4] repealed by Decision 768/2008/EC[5]). Under this *new approach*, Member States legislations' harmonisation would take place in sectors or categories of products (such as toys, machines, etc.), and would be limited to the adoption of essential safety requirements to which the products would have to respond.In the meantime the creation of technical characteristics was left to the competent bodies.

This *new approach* was essentially intended to transform the regulatory model of 'reference to standards' adopted by Directive 73/23/EEC[6] (then replaced by Directive 2006/95/EC[7]), in a general legislative

[1] Council Resolution of 7 May 1985 on a 'new approach to technical harmonization and standards', OJ C 136, 4.6.1985, p. 1–9

[2] Council Resolution of 21 December 1989 on 'a global approach to conformity assessment', OJ C 10, 16.1.1990, p. 1–2

[3] Council Decision 90/683/EEC of 13 December 1990 concerning 'the modules for the various phases of the conformity assesment procedures which are intended to be used in the technical harmonization directives', OJ L 380, 31.12.1990, p. 13–26

[4] Council Decision 93/465/EEC of 22 July 1993 concerning 'the modules for the various phases of the conformity assessment procedures and the rules for the affixing and use of the CE conformity marking, which are intended to be used in the technical harmonization directives', OJ L 220, 30.8.1993, p. 23–39

[5] European Parliament and Council Decision 768/2008/EC of 9 July 2008 on 'a common framework for the marketing of products, and repealing Council Decision 93/465/EEC', OJ L 218, 13.8.2008, p. 82–128

[6] Council Directive 73/23/EEC of 19 February 1973 on 'the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits', OJ L 77, 26.3.1973, p. 29–33

[7] European Parliament and Council Directive 2006/95/EC of 12 December 2006 on 'the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits', OJ L 374, 27.12.2006, p. 10–19

harmonisation strategy.[1] The manufacturer must therefore manufacture its product following the essential requirements of the Directive. This conformity may occur either by manufacturing the product following the harmonised standards (if any), developed by the relevant European standardisation bodies, or by testing it throughout a *notified body*, which has been certified by a Member State for this purpose. If the product complies with these essential requirements, it may carry the CE logo, which allows it to circulate freely on the European market.This creates a rebuttable presumption that all the requirements of the Directive are met. By a sort of parallelism, it could be deduced that the establishment of a certification system for ICT products, services or processes should ultimately lead to a kind of *digital CE*. It is therefore difficult to give a clear and precise answer on the legal nature of the European digital market.

The digital transition taking place these last years means that we are witsnessing a transformation from the classic physical market to a dematerialised market. The digital market would therefore transcend the physical market.[2] A product or service would *ipso facto* fall under digital regulations from the moment it is connected or whether it processes personal data or not. However, it is too soon and difficult to say whether the digital market would be a concrete European Union policy or a gradual extension of the single market to the digital domain. The European Commission retains that "*although the treaties do not contain specific provisions on ICT, the European Union can take action in this area within the framework of sectoral and transversal policies*"[3]. The harmonisation of rules concerning the free movement of non-personal data and establishing a principle of unicity within the internal market means that, we would be more inclined to see it more as a EU's policy intended of clearing axes and transversal principles going beyond sectoral approaches.

Recruiting and keeping sufficient numbers of cybersecurity professionals in the workplace is a constant battle. The problem is the lack of cybersecurity skills in the European labour force to work toward cybersecurity certification schemes. As part of this cybersecurity reform, the EU institutions also forwarded the establishment a *European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres* with the adoption of Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021.[4]

According to recital 30 of the Regulation (EU) 2021/887, the Centre will have the aim of "*promoting, where possible, the implementation of the European cybersecurity certification framework as established by Regulation (EU) 2019/881*". This future centre will be supported by a Network of National Coordination

[1] Commission Communication on 'Technical Harmonization and Standards: A New Approach', 31 January 1985, COM (85) 19 final; Commission Communication on 'Strengthening the Implementation of the New Approach Directives', 7 May 2003, COM (2003) 240 final

[2] Interview 1

[3] Available at https://www.europarl.europa.eu/ftu/pdf/en/FTU_2.4.3.pdf (accessed on January 22nd, 2020).

[4] European Parliament and Council of the European Union, Regulation (EU) 2021/887 of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, PE/28/2021/INIT, OJ L 202, 8.6.2021, p. 1–31

Centres. In this regard, the Council's Permanent Representatives Committee mandated the Romanian Presidency in March 2019 to start negotiations with the European Parliament on the creation of a high-level knowledge base on cybersecurity. The adoption of the proposal took two years of discussions either for reasons related to the place of this centre's headquarters, or for reasons related to its funding.

The regulation sets up three structures. The first structure will be the European Centre for Industrial, Technological and Research Skills, which will help to better coordinate cybersecurity research and innovation. It will also be the EU's hand tool for raising funds for research, technological and industrial development in the field of cybersecurity. The second structure will be the Cybersecurity Capacity Network, which will be made up of national coordination centres appointed by Member States. These coordination Centres will have access to technological expertise in the field of cybersecurity, for example in areas such as cryptography and intrusion detection or human security. Finally, regulation also establishes a third structure, a Community of Cybersecurity Skills bringing together the main stakeholders, non-profit research organizations, public entities dealing with operational and technical issues and, where appropriate, agents from other sectors facing cybersecurity challenges, in order to improve and disseminate cybersecurity expertise across the EU.

The EU's DSM Strategy relies on "*the better access to digital goods and services across Europe; the creation the right conditions and a level playing field for digital networks and innovative services to flourish and; the maximization of the potential growth of the digital economy*"[1]. In 2015 the European Commission adopted the Digital Single Market strategy, aiming to set up a set of common European data protection rules, reform telecoms rules and modernise copyright rules, among other goals. This strategy has led to the adoption of a series of legal acts which has hardened the cybersecurity policy in the DSM. The GDPR has enforced data privacy and online consumer protection. The NIS Directive has enhanced cyber resilience throughout a set of measures for a high common level of security of network and information systems across the Union, while the Cybersecurity Act strengthened the mandate of the ENISA and established a cybersecurity certification framework for products and services.

Making the European Union's single market fit for the digital age still requires tearing down unnecessary regulatory barriers and moving from individual national markets to one single EU-wide rulebook. That is the major challenge: building an agile economy that guarantees citizens' rights. In December 2020, the European Commission proposed an ambitious regulatory package to define its new digital strategy. It is made up of three regulations: one on digital markets, another on digital services and the third on data governance. In these three regulatory proposals where everything is extremely interconnected because they also involve intellectual property, competition law, data protection, freedom of expression, social media regulation, service provider responsibility, etc. The legislative process, however, is slow and complex, given that these Commission proposals will be worked on by the European Council and then by the European Parliament, before finally

[1] European Commission Communication on 'A Digital Single Market Strategy for Europe', 6 May 2015, COM(2015) 192 final

reaching the phase known as the trialogue between these three bodies. Much of the difficulty lies also in the 27 Member States of the European Union reaching an agreement they can all adopt with a single voice.

Another policy area in which the EU has been relatively active when it comes to regulating cyberspace, is the cybercrime Area of Freedom, Security and Justice policy.

B. EU's Shared Competences and The Area of Freedom, Security and Justice Policy: Fostering a 'Comprehensive' Vision of EU's Cybercrime Law

The EU's action on cybercrime legally falls within the Area of Freedom, Security and Justice (hereafter AFSJ), which is shared with most Member States. The EU-CSS describes cybercrime as "*a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target*"[1]. Such criminal activities may relate to fraud, on-line distribution of child pornography, or even attacks against information systems.

It is the first time that a definition of cybercrime appears within an EU document. The content of the Council of Europe Convention on cybercrime (understood here as an external norm) is proposed to form the basis for EU rulemaking on internal and external cyber policies. While the EU is not a party to the main international treaty in this area, the EU-CSS encourages "*Member States that have not yet ratified the Council of Europe Convention on Cybercrime (Budapest Convention) to ratify and put these provisions in place as soon as possible*"[2].

While the Cybercrime Convention (or Budapest Convention) was the first legal step internationally for the internet space (**1**), the adoption on February 24th, 2005, of the Council Framework Decision 2005/222/JHA on attacks against information systems marks, was however, the first legal instrument adopted by the EU in relation to cybersecurity in the AFSJ (**2**). But the inability to directly apply this Decision combined with the post-Lisbon approach offered by Article 83 TFEU, led on further hardening the EU law in the field of Information Systems with the adoption of Directive (EU) 2013/40 (**3**).

1. The Cybercrime Convention

[1] See European Commission Communication 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 7 February 2013, JOIN(2013) 1 final

[2] See European Commission Communication 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', 7 February 2013, JOIN(2013) 1 final

Most of the EU Member States have already ratified the Budapest Convention nowadays, but Sweden is not yet one of them[1]. It is noteworthy that the European Commission strongly encourages, throughout the EU-CSS document, those Member States of the Union that have not yet ratified the Convention to do so as soon as possible. However, the European Union itself is not a party to it.

The explanatory report to the Convention on Cybercrime characteristically mentions:

> "*By connecting to communication and information services, users create a kind of common space called 'cyber-space' which is used for legitimate purposes but may also be the subject of misuse. These 'cyber-space offences' are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g., when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities. [...] Only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena*"[2].

The Budapest Convention aims to establish a common anti-criminal policy. Regarding its content, the Convention lays the groundwork for the harmonisation of internal criminal law in the field of cybercrime with the adoption of internal procedural provisions for the investigation, prosecution, and adjudication of cybercrime, as well as the rules of reference with international cooperation. However, the Budapest Convention does not include an overall definition of cybercrime. It only provides that, states should criminalise not only behaviours against information systems and their data, namely so-called *genuine cybercrime*, but also, behaviours that infringe various other legal goods and are perpetrated via a computer (e.g., fraud) and behaviours that should be reduced to crimes because of the content being handled by information systems (e.g., child pornography). In this sense, and in view of its detailed provisions for interventions in the field of procedural law and judicial cooperation, it has been argued that the Council of Europe Convention appears to be the most comprehensive international instrument in this respect.

Specifically, the content of the Budapest Convention is structured in three main categories: provisions of substantive criminal law, provisions of criminal procedure law and provisions of international judicial cooperation. Its first chapter provides definitions of concepts such as computer system, computer data and service provider, in order to establish a commonly accepted terminology for some basic and difficult techniques. Understandable concepts thereby ensure a homogeneous conceptual approximation of these terms by national legal orders. The first part of its second chapter sets then out the measures to be taken at national level. The Budapest Convention explicitly states that any member accepting it undertakes to criminalise the conducts

[1] Chart of signatures and ratifications of Treaty 185 - Convention on Cybercrime. Available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (accessed on January 11th, 2019).

[2] Available at https://rm.coe.int/16800cce5b (accessed on January 22nd, 2020)

mentioned therein on the internet. Finally, the third chapter of the Convention holds provisions on international judicial cooperation referring to the issuance, in general terms, of mutual assistance, the provision of automated information, the rapid safeguarding of data stored on computers and the rapid disclosure of stored trafficking data.

An overall assessment of the Budapest Convention on Cybercrime should be made in addition to the criticism it has occasionally raised. One might say that it was an important first step towards common consensus on internet issues among States. More than a decade after its passage, it is still up to date, offers answers to new challenges and appears to be the map on which the legal positive manipulation of the internet will move. The conclusions reached by the Commission under Article 46 of the Cybercrime Convention Committee[1] on updating the Convention are characteristic. It further shows that, new forms of attack on important information infrastructures (e.g., botnet, DDoS) are also covered by existing provisions. However, one cannot overlook the fact that there is no reference to the penalty fees that should be imposed on criminal offenses, which was mainly due to failure to reach a common agreement among implicated parties.

The Budapest Convention adoption in 2001 is unfortunately outdated as it struggles to integrate technological developments. It also suffers from the fact that Russia has not signed it and that China is against it. Both countries believe that the Convention is too repressive-oriented. In any case, this instrument still needs to be modernised, in the framework of a third protocol, to define new infringements, to reinforce the security of the networks and to extend the responsibility to new actors. A second protocol on the fight against terrorism would be under development. However, history has shown that the Cybercrime Convention was simply the first legal step in the internet space. The next one was being prepared within the EU throughout the adoption on 24 February 2005 of Council Framework Decision 2005/222 / JHA on attacks against information systems.

2. The 2005 Council's Framework Decision: EU's First Legal Instrument

The European Council recognised in Tampere in October 1999, the need for an approximation of national laws on crime and penalties in cybercrime, which was confirmed approximately one year later in a communication of the Commission entitled "*Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*"[2]. Regarding the differences between the Member States' criminal systems, the European Commission sought to find minimum points of agreement, which subsequently transformed the minimum requirements of the States for harmonisation into their national legal systems and so produced a dynamic of redefinition of national criminal systems. In line with this

[1] Available at https://www.coe.int/fr/web/cybercrime/tcy (accessed on January 22nd, 2020).

[2] Commission Communication on 'Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime', 26 January 2001, COM(2000) 890 final, p. 2-3.

communication, the Framework Decision 2005/222 / JHA of February 24th, 2005,[1] on attacks against information systems was adopted. As part of the wider context of the *e-Europe initiative*[2] for the information society, this Framework Decision aimed at implementing a safer society of information.

Facing a new form of transnational crime, the primary purpose of the Framework Decision 2005/222 / JHA was to strengthen cooperation between judicial authorities and other competent authorities through an approximation of their criminal rules on illegal access to information systems (Art. 2), on system's integrity infringement (Art. 3) and on data's integrity infringement (Art. 4). Incitement, assistance, complicity or attempt to commit one or more of the above acts are also recorded as punishable (Art. 5). It also stipulates that Member States should provide for the possibility of punishing the abovementioned acts with effective, proportionate, and dissuasive criminal penalties (Art. 6). The criminal offense perpetuation within the meaning of Joint Action 98/733 / JHA, as well as the infliction of serious harm and prejudice to essential interests, may be considered as an aggravating circumstance (Art. 7). In addition, the Framework Decision proposes criteria for figuring out the liability of the legal person and penalties that may be imposed if the liability of that legal person is declared, such as, for example, a temporary or definitive ban on the exercise of commercial activity, a judicial winding-up order, loss of public benefits etc. (Art. 8 and 9). Accordingly, matters of jurisdiction and exchange of information are dealt with in Articles 10 and 11, respectively.

The Framework Decision states in its second article that it is a criminal offense to punish intentional and unlawful access to an information system. At the same time, it allows Member States to sanction such acts only in case of a breach of a security measure. However, the difficult issue of defining the limits of simple access and the definition of minor cases is left to the discretion of the national legislature.

Lastly, the Commission's report to the Council based on Article 12 of the Framework Decision is noteworthy.[3] In this Report, the Commission notes that the Framework Decision was still being transposed in the Member States, while there was important progress in the twenty evaluated Member States. The conclusions reached in the Commission Report, combined with the inability to apply directly to the Framework Decisions and the new approaches offered by Article 83 TFEU, led to a hardening out of the EU's legal framework in the field of Information Systems across the Union with the adoption of the Directive (EU) 2013/40.

[1] Council Framework Decision 2005/222/JHA of 24 February 2005 on 'attacks against information systems', OJ L 69, 16.3.2005, p. 67–71

[2] Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_99_953 (accessed on December 4th, 2019).

[3] European Commission Report to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, 14 July 2008, COM(2008) 448 final. Available at https://ec.europa.eu/transparency/regdoc/rep/1/2008/EN/1-2008-448-EN-F1-1.Pdf (accessed on November 3rd, 2019).

3. Directive (EU) 2013/40: Hardening the EU's Legal Framework in the Field of Information Systems Across the Union

Large-scale attacks, new methods of committing botnet crime, the need to fight organized crime and terrorism, as well as the need to remove obstacles on the investigation and prosecution of crimes in well-coordinated and broad-scale cross-border attacks have entailed the upgrading of the 2005 Council Framework Decision. On 14 August 2013, Directive 2013/40/EU[1] of the European Parliament and of the Council of 12 August 2013 on attacks against information systems replacing Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems was published in the Official Journal. This new Directive aims to tackle the increasingly sophisticated and large-scale forms of attacks against information systems, which have emerged since the adoption of Council Framework Decision 2005/222/JHA.

Comparatively with the Council's Framework Decision 2005/222 / JHA, the standardisation of the crime of illegal access to information systems (Art. 3) stays the same as that of the Framework Decision. The possibility of Member States sanctioning a security measure offense was however removed in the directive's proposal. That resulted essentially to an enlargement of the sentence for this crime compared to the Framework Decision and the Convention on Cybercrime. The broadening of criminality did not however meet the fundamental demand for the use of criminal law as an *ultima ratio*. Therefore, the proposal made by the Presidency of the Council has re-affirmed as a precondition the inclusion of security measures breach as a condition upon illegal access to information systems. A proposal which appears to have affected the legislative outcome as Article 3 of the Directive included the security measure breach again as a condition. The provision of minor cases has also been kept in the text of Article 3 of the Directive, in order to cover the need for national legislators to have some possibility of restraint of punishment.

Regarding sanctions, the Directive provides in Article 9 a broader scope for the relevant offenses than the Framework Decision, by going far beyond the general requirement for effective, proportionate, and dissuasive criminal sanctions. A sanction of more than five years' imprisonment is provided in the cases of a criminal organisation's attack, of significant damage and, of a critical infrastructure information system impact. In addition, the use of botnet networks supports a minimum sentence of three years in prison if there is financial loss or loss of personal data. Finally, the directive also imposes liability on companies that do not respect their supervisory and control obligations and thereby allow a person under their jurisdiction to commit any of the offenses listed in the directive.

The opinion of the German Green Party MP, Jan Philipp Albrecht, on the July 3rd 2013 European Parliament meeting in Strasbourg, is particularly interesting as he points out *inter alia* that:

[1] European Parliament and the Council, Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8–14

"*[…] The only problem […] is that we are not getting any more security with this directive, because this directive only relates to criminal law. And criminal law does not solve security problems, nor social problems per se. And by the way, criminal law is actually a means that should be used as a last resort. […] the effect that is created here, namely only increasing penalties, is the wrong effect. Instead, it would have been important to include […] the responsibility of operators in the event of gaps in information systems. Instead, those who point out these loopholes will now be punished. And we don't think that's proportionate*"[1].

As regards the information exchange procedure, the Directive aimed to improve judicial cooperation across the EU in criminal matters, strengthening the existing infrastructure of 24-hours and weekly information points of contact and establishing an obligation for Member States to respond to an emergency assistance request in eight hours. The innovation of the Directive is the introduction of an obligation for Member States to watch, record and collect statistics on crime.

The fight against cybercrime benefits from a strong political impulse for internal security. The desire to progress in this area is reflected in a consequent normative acquis. The renewed strategy for the period 2015-2020 approved by the Council conclusions of June 6th, 2015,[2] mentions the fight against cybercrime as a priority goal. In its conclusions approved on September 25th, 2017,[3] on the mid-term review of the renewed Internal Security Strategy for the EU 2015-2020, the Council names three key priorities around which the EU must focus its efforts: (a) terrorism, (b) the prevention of serious organized crime and (c) cybercrime. Regarding the latter, it is being suggested that they strengthen the fight against this phenomenon by regularly analysing the table of different threats, ensuring the availability of effective investigative tools and the cross-border access to electronic evidence; the latter being one of the issues currently dealt with in the context of cybercrime coercion.

---

[1] Available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20130703+ITEM-018+DOC+XML+V0//EN (accessed on November 3rd, 2019). Translated text from German language: "Natürlich ist es wichtig, dass wir mehr Sicherheit vor Angriffen auf Informationssysteme brauchen. Natürlich ist es richtig, dass wir da politische Schritte ergreifen. Das Problem ist nur, dass wir – Herr Díaz de Mera – mit dieser Richtlinie nicht mehr Sicherheit bekommen, denn diese Richtlinie bezieht sich ja nur auf das Strafrecht. Und Strafrecht löst Sicherheitsprobleme, gesellschaftliche Probleme per se eben nicht. Und das Strafrecht ist übrigens auch eigentlich ein Mittel, das man als Ultima Ratio einsetzen sollte.

Nun ist es so, dass wir uns darauf einigen, Strafmaße zu harmonisieren – grundsätzlich ein richtiges Anliegen! Aber man muss eben auch dazusagen, der Effekt, der hier erzeugt wird, nämlich Strafen immer nur weiter zu verschärfen, ist der falsche Effekt. Stattdessen wäre es wichtig gewesen, genau das aufzunehmen, was Herr Enciu vorgeschlagen hat, nämlich auch die Verantwortlichkeit von Betreibern bei Lücken in Informationssystemen. Stattdessen werden jetzt diejenigen bestraft, die diese Lücken aufzeigen. Und das halten wir nicht für verhältnismäßig."

[2] Available at https://data.consilium.europa.eu/doc/document/ST-9798-2015-INIT/en/pdf (accessed on February 26th, 2021)

[3] Available at https://www.consilium.europa.eu/en/documents-publications/public-register/public-register-search/results/?AllLanguagesSearch=False&OnlyPublicDocuments=False&DocumentNumber=11901%2F17&DocumentLanguage=EN (accessed on February 26th, 2021).

In conclusion, it could be told that significant progress has been made since 2001 regarding issues related to information system criminalisation. As we will see in Section II, cybersecurity resilience and cybercrime related measures have been so far more elaborate than cyberdefence measures, as the EU disposes limited competences in the field of the CFSP/CSDP.

§2. Cybersecurity and EU External Action: the 'Soft' Legal Nature of CFSP/CSDP

The EU uses the term 'cybersecurity' as a term primarily related to the civilian aspect of security, whereas 'cyber defence' is broadly used for the military domain. The two concepts are dealing however with the same threats and require similar measures and procedures. Among presented priorities, the 2013 EU-CSS highlights the need to develop cyberdefence policy and capabilities under the framework of the CSDP, as well as establishing a coherent international cyberspace policy for the European Union, which promotes EU's core values.

The Council adopted in 19 June 2017 conclusions on a framework for a joint diplomatic response to malicious cyber activities (the *Cyber Diplomacy Toolbox*) and affirmed that

> "*measures within the CFSP, including, if necessary, restrictive measures adopted under the relevant provisions of the Treaties are suitable to a framework for a joint Union diplomatic response to malicious cyber activities, with the aim of encouraging cooperation, facilitating the mitigation of immediate and long-term threats, and influencing the behaviour of potential aggressors in the long term*"[1].

Soft law creates ambiguous situations where soft and hard norms are combined. In external action, *hard* law is sometimes taken based on a *soft* position adopted within the framework of CFSP[2]. While the wording of the EU treaty makes it clear that "*common actions and common positions are legally binding*"[3], the *soft* nature of CFSP[4] is often related to the absence of a role of the Court of the EU and to the impossibility for domestic courts to engage in CFSP issues[5].

[1] European Council Decision concerning 'restrictive measures against cyber-attacks threatening the Union or its Member States', 14 May 2019, 7299/19

[2] As in the case of economic sanctions implementing a CFSP position

[3] See F. Terpan, 'Soft Law in the European Union – The Changing Nature of EU Law', (2015) 1 *European Law Journal* 21

[4] See R. A. Wessel, 'Resisting legal facts: are CFSP norms as soft as they seem?', (2015) 2/1 *European foreign affairs review* 20

[5] Two exceptions are provided by the TEU. The CJEU monitors CFSP's compliance with the rules of horizontal power sharing in the EU. CFSP's intergovernmental rules of functioning cannot be applied where supranational rules shall be

Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy figures among the strategic priorities and actions of EU's CSS: An Open, Safe and Secure Cyberspace. The sensitivity and reluctance of certain Member States to participate in a common defence policy in the field of cybersecurity, given their own cyberdefence strategies, has hindered the development of a Common Cyberdefence Policy. Cyberdefence is an issue rarely addressed and marked by the existence of a number of instruments of soft law (e.g., strategies) and of soft institutional governance (**A**).

On the other hand, the non-binding nature of the norms and principles of international law constitute an obstacle to their effective implementation by EU Member States' policies. It is accentuating the soft nature of the cybersecurity policy when it comes to defence matters. Hence, it does not offer a comprehensive framework able to serve as a set-up base for the EU to harden its cybersecurity/defence related policy (**B**). There are indeed several situations in which international law leaves the victim State of cyber operations helpless. Among them, the State's responsibility is the more obvious. Hence the law of State responsibility "*does not provide an answer in every case and it cannot solve the problem related to technical capabilities of the victim*"[1].

The EU Cyber Diplomacy toolbox initiative could offer a palliative effect. But it still suffers from the soft governance mechanism of the CFSP.Thus, the solidarity and mutual assistance clauses seems to be the only two available 'hard' solutions of the EU on addressing external attacks to EU's cybersecurity (**C**).

A. Cyber-related 'Soft' Rules and European External Security Policies

With the adoption of the EU-CSS, the EU started to implement concrete policies and to increase cyber defence capabilities across the EU. In consequence, the Heads of State / Government acknowledged in their conclusions of the European Council that, cyberspace is one out of four key capability shortfalls in the EU and called so for a common *Cyber Defence Policy Framework*. Cyber defence also forms part of the Permanent Structured Cooperation Framework (PESCO)[2] and EU-NATO (North Atlantic Treaty Organization) cooperation. For each area, the strategy proposes actions to undertake. An annual report will be made every year, to take stock of developments, and the next revised version of the framework "*should be presented by mid-2022 at the latest, in close consultation with the Member States*", says the Council. However, EU's role regarding cyber resilience and deterrence stays relatively restraint. So, the CSDP stays the most intergovernmental part of the Common Foreign and Security Policy (hereafter CFSP).To understand the place of EU's cybersecurity in CSDP, we shall expose its post-Lisbon legal basis (**1**), and the decision-making process

applied. The second exception is that the CJEU has jurisdiction on sanctions decided on the basis of a previous CFSP decision.

[1] F. Delerue, *Cyber Operations and International Law. In Cyber Operations and International Law*. (Cambridge: Cambridge University Press, 2020).

[2] Available at https://pesco.europa.eu/ (accessed on February 26th, 2021)

and scope of CSDP (**2**). Being also a core plank of external cybersecurity, the new *Cyber Diplomacy Toolbox* of the EU will also be discussed next (**3**).

1. EU's Common Security and Defence Policy and Cyberdefence

Despite the new nature of the threat of cyber warfare, no alliances were created with the sole purpose of joint cyberdefence. Instead, cyber warfare was seen as another form of armed threat. Thus, existing alliances adapted their institutions and their means to this new dimension, since for each alliance the advent of cyber warfare did not in itself create new enemies, it simply gave the already designated enemies additional capabilities. NATO, already in the seventh decade of its existence and after its successive adjustments to the reality of its geographical area of responsibility, faced another challenge: cyberspace. Recognising the seriousness of this new form of threat relatively early and making the necessary adjustments to its structure so that it is prepared for any eventuality was vital. Naturally, NATO did not suddenly realise the need for protection from cyber warfare, nor did it reach the current level of capability overnight. It took time, research, analysis, and knowledge (which sometimes came at a price, as in the case of Estonia) to crystallize today's cybersecurity policy.

In contrast to NATO, where cyber defence has evolved into a crucial action in the last decade, the EU seems to have failed to appreciate how catalytic cyber warfare can be for business development. It should not be overlooked that the CSDP and EU's defence dimension in general have neither the degree of NATO maturity nor the real permanent staffing force. NATO was thus the first to adopt a Cyber Defence Policy in January 2008, five years before the EU.[1] The latter having started to implement concrete policies and to create cyber defence capabilities with its European Cybersecurity Strategy, published in 2013.

As it has been developed until now cyberspace has become for the EU an element of the Digital Single Market. Moreover, in the globally changing world, typical interior policy areas, such as cyber security, migration, or terrorism issues, are becoming fields of action for the Common Foreign and Security Policy (CFSP) and its military component,the Common Security and Defence Policy. CFSP/CSDP are increasingly engaged in military matters. In recent years, cyber defence has thus become part of both CSDP defence issues and EU's internal security issues.

Therefore, the 2013 Strategy established the first multilevel guidelines for the further addressing of cyber defence and articulated cross-sectoral cyber defence objectives. The 2013 Strategy connected internal security questions (the area of freedom, security, and justice), and external security questions (CFSP/CSDP) - two levels of Union security defence that cannot be functional if not connected. The EU Cyber Defence Policy Framework[2]

[1] Available at https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed on January 3rd, 2022)

[2] Council Outcome of Proceedings 'EU Cyber Defence Policy Framework', 18 November 2014, 15585/14

was endorsed in 2014 and became the reference policy document on cyber defence. This policy endorsed five objectives:

> "*supporting the development of Member States' cyber-defence capabilities related to CSDP, enhancing the protection of CSDP communication networks used by EU entities, promoting civil-military cooperation and synergies with wider EU cyber policies, relevant EU institutions and agencies and the private sector, improving training, education and exercise opportunities, enhancing cooperation with relevant international partners, especially NATO*"[1].

However, it was only in 2016 that EU-NATO collaboration started to be shaped as an agreement on greater security cooperation between the two institutions. The EU-NATO Joint Declaration[2] set specific objectives for enhancing cyber-defence cooperation by: "*(a) fostering interoperability of cyber defence in missions and operations; (b) strengthening cooperation on training and exercises; (c) promoting cooperation on cyber-defence research and technology innovation; and (d) mainstreaming cyber aspects into crisis management*"[3]. Since then, European cyber defence has been extended by several strategic documents. The EU Global Security Strategy published in June 2016[4] considers cyber as one of the key components of EU's security and defence.

Cyber defence was also pursued in 2017 under the Permanent Structured Cooperation (hereafter PESCO) framework, "*although participation is voluntary and not EU-wide*".[5] Two current PESCO projects illustrate a persistent demand for tactical and operational solutions to cybersecurity challenges: the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security and the Cyber Threats and Incident Response Information Sharing Platform.

Even though not all objectives set in the 2013 CSS have been achieved, the number of cyber security (hybrid) threats motivated EU institutions to adopt the 2017 CSS by way of a Joint Communication of the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy on Resilience, Deterrence and Defence titled "*Building strong cybersecurity for the EU*"[6]. In the field of CSDP, the 2017 CSS promotes mainly the development of cybersecurity deterrence capabilities across the Member States of the EU. Given that Member States are already developing cyberdefence capabilities, and considering the blurred line

---

[1] Available at https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence (accessed on November 12th, 2019)

[2] See European Union External Action Service, 'EU-NATO cooperation – Factsheet, 17 June 2020, available at https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-natocooperation-factsheet_en (accessed on November 6th, 2019)

[3] *Ibid*

[4] Available at https://eeas.europa.eu/topics/eu-global-strategy_en (accessed on January 9th, 2022).

[5] S. Blockmans, 'Europe's defence train has left the station—Speed and destination unknown', (2017) *CEPS Commentary*.

[6] European Commission, Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, Brussels, 13.9.2017

between cyberdefence and cybersecurity, as well as of the considerable differences between Member States' approaches, the EU is determined to promote synergies between military and civilian efforts.

It is also important to mention the report from the European Parliament on Cyber Defence approved on 25 May 2018. It emphasises that

> "*while cyber defence remains a core competence of Member States, the EU has a vital role to play in providing a platform for European Cooperation […] and that whereas current vulnerability is due mainly to the fragmentation of European defence strategies and capabilities, […] much more needs to be done as it is becoming more and more difficult to counter cyber-attack at Member States level, […] whereas cyber defence and deterrence are activities that can best be tackled cooperatively at European level*"[1].

In June 2018, the European Commission, the European Parliament and the Council issued a joint communication titled 'Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats'[2] also putting emphasis on the need for cyber defence coordination at the EU level. Based on the 2017 CSS, the 2014 EU Cyber Defence Policy Framework was updated in 2018.[3]

It is important to articulate that the military concept for cyber defence in CSDP is based on the Member States' capabilities and cooperation, and that the EU's conception of cyber defence is a soft power approach based on support of Member States. It must also be emphasized that not all EU Member States cooperate on cyber defence, which hampers collaboration as well as shared understandings and approaches. EU's cyber defence capacity remains largely fragmented and siloed. If CFSP remains the most intergovernmental policy of the EU, CSDP remains then the most intergovernmental part of CSFP.[4]

In general, CFSP / CSDP is exercised, in accordance with Article 25 TEU, in three ways: (a) with general orientations; (b) with decisions that determine either the actions of the Union or the positions of the Union or the detailed rules for the implementation of the positions. and actions; (c) with systematic cooperation between Member States. Regarding the last point, Article 24, para. 3 TEU stipulates that, "*the Member States shall support the Union's external and security policy actively and unreservedly in a spirit of loyalty and mutual solidarity and shall comply with the Union's action in this area*"; and that they "*work together to enhance and develop their mutual political solidarity. They shall refrain from any action which is contrary to the interests of*

[1] European Parliament's Committee on Foreign Affairs, 'Report on Cyber Defence', (2018). Plenary Session. 25 May, p. 5.

[2] European Commission, Joint Communication to the European Parliament, the European Council, and the Council Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final, Brussels, 13.6.2018

[3] Council of the EU, EU Cyber Defence Policy Framework (2018 update), 14413/18, Brussels, 19.11.2018

[4] See P.J. Cardwell, 'Institutional balances, competences and restraints: The EU as an autonomous foreign policy actor', in Collins, R. and N. D. White (Eds), *International Organizations and the Idea of Autonomy: Institutional Independence in the International Legal Order* (Routledge, 1st edn, 2011)

the Union or likely to impair its effectiveness as a cohesive force in international relations". As it has been already seen, all these circumstantial aspects of CFSP are set out and implemented by the European Council and the Council; and are implemented by the HR/PV and the Member States. Therefore, the EU's current approach is to support Member States in the implementation of their individual strategies and operations rather than build out and maintain a defence posture of its own. This situation is largely due to the decision-making process retained in the context of the CFSP/CSDP.

2. CSDP Decision-Making Process: Intergovernmental Procedures combined with Supranational Practice

The Lisbon Treaty introduced important changes aiming to achieve a more effective and coherent CSDP. However, the focus on effectiveness and coherence overshadowed questions of input legitimacy and parliamentary accountability for CSDP decisions. Even after the Lisbon Treaty, the CSDP decision-making processes remain an *intergovernmental island* within the EU. In CSDP, the decisions are taken unanimously (Article 15§4 TEU) by 27 national Foreign Ministers sitting as the Foreign Affairs Council (FAC) and, in the case of certain high-profile issues, by the Heads of State and Government themselves, sitting as the European Council. Each Member State retains a veto over any collective decision (Article 235§1 TFEU). The principle of intergovernmentalism suggests "*a process of rational bargaining in negotiations, where each Member State seeks to defend the national interest and lays down red lines which it will not be prepared to see crossed*"[1]. Most of these decisions are even taken much lower down the command chain and only comparatively rarely do elected politicians actually arbitrate on important policy issues.

Moreover, a critical reading of the Treaty suggests that CSDP remains largely out of parliamentary reach at the European level even though the Lisbon Treaty has considerably extended the European Parliament's powers around EU external relations in general (e.g., extended control of the European External Action Service budget and the non-military parts of the CFSP/CSDP budget, scrutinisation of diplomatic personnel and accessibility to sensitive documents etc…). However, the EP's possibilities of controlling the HR, let alone the Council, are extremely limited. The Lisbon Treaty has thus maintained CSDP as an intergovernmental area of policy making par excellence,[2] by underlining in Declaration No. 14 that the TFEU provisions covering CFSP, including CSDP

[1] A. Moravcsik, *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht* (Ithaca, NY: Cornell University Press, 1998).

[2] See further J. Santos Vara, 'The Establisment of the European External Action Service: The EU in Search of a Stronger Role on the International Stage', (2011), *Croatian Yearbook of European Law*, pp. 109-134.

as an *integral* part thereof (Article 42§1 TEU), "*do [not] increase the role of the European Parliament*".[1] The role of the Court of Justice of the EU is also extremely limited.

While the Lisbon treaty gives a dominant position to the Council on the CSDP decision-making process, it must be cleared that the Council's position remains essentially the same as in the treaty of Nice. By doing so, Article 16§6 TEU still states that the Council, in the composition of the Council on Foreign Affairs, chaired by the High Representative, "*shapes the external action of the Union*" in accordance with the guidelines of the European Council and "*ensures its coherence*". Specifically, the Council together with the European Council determines and implements CFSP (Article 24§1). Article 26§2 of the TEU entails a general competence for the Council to "*frame the common foreign and security policy and take the decisions necessary for defining and implementing it based on the general guidelines and strategic lines defined by the European Council*". The Council may then adopt general guidelines for laying down the strategies of the EU in relation to a particular third state, or theme, such as "*Guidelines on the implementation and evaluation of restrictive measures (sanctions) within the framework of the EU's common foreign and security policy*"[2] (Article 26(1) TEU). Decisions may also be adopted by the European Council. When related to the CFSP, these issues usually take the form of *Conclusion*. As CSDP can be seen as forming part of CFSP, the decision-making take place along similar lines.

It should be noted however that policy options and stated preferences are largely being agreed in advance at a lower level. Decisions in CSDP are taken at different policy making levels. Hence, they are shaped and formulated by a host of working groups and committees labouring away in the Council Secretariat, the Commission, and national capitals. Therefore, the European Council, the Council, and the intergovernmental committees (Permanent Representations, Policy and Security Committee, Military Committee, Crisis Management Policy Committee) have the final wording both formally and practically on the decision-making process and also define its framework. The recommendations of intergovernmental and trans-governmental[3] bodies then go to the PSC and COREPER, which transform them into policy options to be, in most cases, rubber-stamped by politicians. In the *new world order*, one witnesses governmental networks which – in their search for answers to pressing global questions – interact, consult and decide.[4]

The vast majority of the *spade work* in this policy area is therefore carried out by the many working groups, committees, and agencies (e.g., COREPER, Political and Security Committee, the European Union Military

[1] Consolidated version of the Treaty on the Functioning of the European Union A.DECLARATIONS CONCERNING PROVISIONS OF THE TREATIES 14.Declaration concerning the common foreign and security policy; OJ C 202, 7.6.2016, p. 343–343

[2] Council Guidelines on 'the implementation and evaluation of restrictive measures (sanctions) within the framework of the EU's common foreign and security policy', 8 December 2017, 15598/17

[3] See S. Hofmann, 'CSDP: Approaching Transgovernmentalism?'. In: Kurowska X., Breuer F. (eds) *Explaining the EU's Common Security and Defence Policy* (Palgrave Macmillan : London, 2012).

[4] See A.-M. Slaughter, *A New World Order* (Princeton: Princeton University Press, 2004)

Committee, Committee for Civilian Crisis Management or the European Defence Agency). All of them, without exception, are formally "*intergovernmental*" agencies composed of one or more representatives per member state.

In an assessment of the *clash of institutional logics* involved in the EDA's existence and work, Jozef Bátora, in 2009 sought clues as to how the Agency will evolve and how it will impact on the eventual political direction taken by CSDP.[1] He suggests that "*the rules and norms set up by the EDA in its effort to bring about greater coordination and cohesion in the field of defence provide a framework for trans-governmental regulation and socialization among participating Member States and thereby possibly a transcendence of the inter-governmental nature of second pillar agencification*".[2] The adoption of the European Defence Fund (EDF) reinforced the embedding of the supranational logic within the CSDP.

In June 2017, the European Commission launched a proposal for European fund aimed at financing transnational defence research and development. The growing involvement of the Commission around defence has been described as "a *game changer*" for European defence cooperation.[3] Even in the CSDP, in which it lacks formal power, the Commission has been able to de facto influence decisions in the past. In his article on "*how the European Commission Influences EU Security and Defence Policies*", Riddervold shows how the Commission has influenced the EU Maritime Security Strategy by reorientating the strategy from a CSDP to a cross-sectoral strategy.[4] The EDF initiative illustrates moreover "*a renewed striking resurgence of supranationalism in a domain that was supposed to be the most immune to this dynamic, at a time viewed by many as the golden age of intergovernmentalism*"[5].

After having exposed the legal framework on cyberdefence related issues within the context of EU Security and Defence Policies, as well as the *intergovernmental supranationalism* of the CSDP decision-making and the role of the implicated actors, it is also worthy to get an oversight of how the international scene, and more specifically the international law, applies to cyberspace and is implemented by the EU.

---

[1] J. Bátora, 'European Defence Agency: A Flashpoint of Institutional Logics', (2009) 6 *West European Politics* 32, 1075-1098.

[2] *Ibid*, p. 1092

[3] P. Haroche, 'Supranationalism strikes back: a neofunctionalist account of the European Defence Fund', (2020) 6 *Journal of European Public Policy* 27; F. Terpan, 'La relance du projet européen de défense au-delà du contrôle des États', (2020) 4 *Politique européenne* 70

[4] M. Riddervold, '(Not) in the Hands of the Member States: How the European Commission Influences EU Security and Defence Policies', (2016) 2 *JCMS: Journal of Common Market Studies* 54

[5] P. Haroche, 'Supranationalism strikes back: a neofunctionalist account of the European Defence Fund', (2020) 6 *Journal of European Public Policy* 27

B. International Norm-Setting on Cyber-Related Operations: From EU's Cyberdiplomacy to the Usage of Force

The EU strongly promotes the idea of an international law, and in particular the Charter of the United Nations (CUN), which applies in cyberspace. As stated in EU-CSS, "*if armed conflicts extend to cyberspace, International Humanitarian Law and, if appropriate, Human Rights law will apply to the case at hand*". The specific set of legal problems relating to questions of responsibility or liability, for the conduction of cyber operations, stems from their nature as an instance of multi-level governance involving both the EU and its Member States and, possibly, third states and/or international organisation.[1] Terms such as cyber security, cyber-attack, cyber-crime, cyberwar(fare) and cyber terrorism have then entered in the public discourse. However, there is no consensus on their definitions, making it in consequence difficult to create a conceptual framework in which relations and international agreements related to cyber-space can be developed.[2]

States have proven for centuries their willingness to become involved in defining the boundaries between peace and war. However, *deterrence* in the cyber domain is not a game of great powers or that of nation-states alone. Although it was claimed in the early days of the internet that cyberspace is not subject to legal regulation,[3] it is accepted nowadays that international law applies to cyberspace and to cyber activities, by regulating the use of force in case of cyber-attacks.

With its 2013 EU-CSS, the EU committed to applying existing international law in cyberspace. The application of international law on cyberspace is however amongst the most highly controversial and politicised issues in international cybersecurity. Studies have been able however to argue that deterrence needs to be viewed from a different perspective by moving away from usual normative frameworks, such as treaties. Academic efforts have been made to establish a legal framework for cyber activities, with the most prominent work of the *Tallinn Manual 2.0 on International Law of Cyber Operations*.[4] However, international legal frameworks for the application of the law of cyber peacetime operations, such as the Tallinn Manual, are the most advanced.

[1] See K. Bannelier and T. Christakis, 'Reinventing Multilateral Cybersecurity Negotiation after the Failure of the UN GGE and Wannacry: The OECD Solution', February 2018, *EJIL:Talk!*, available at https://www.ejiltalk.org/reinventing-multilateral-cybersecurity-negotiation-after-the-failure-of-the-un-gge-and-wannacry-the-oecd-solution/ (accessed on November 11th, 2019)

[2] See C.-C. Cirlig, 'Cyber defence in the EU, Preparing for cyber warfare?', [Online Article], October 2014, *European Parliamentary Research Service*, available at https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf (accessed on November 11th, 2019)

[3] See N. Tsagourias, 'The Law of Cyber Warfare: Restrictions, Opportunities and Loopholes', (2017) 1 *Canadian Journal of Law and Technology* 15

[4] The document was produced by an international group of legal scholars and practitioners at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence in 2009-2017; See K. Bannelier-Christakis, 'Rien que la Lex Lata ? Etude critique du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations', (2017), *Annuaire Français de Droit International*, CNRS, pp. 121-160

They serve more as guides for the development of international normative policies, rather than as workable agreements between states.

In view of this situation, government groups, such as the United Nations Group of Governmental Experts on Cyber Security, have therefore promoted confidence-building measures at the end of which, standards have indeed shown *clear signs of emergence* (e.g., responsible reporting of vulnerabilities in information and communication technologies, cooperation to put an end to the terrorist and criminal use of ICTs, etc. …). Instead of a pure maximisation of interests, normative deterrence would then make it possible to do what is right, and the United Nations Group of Governmental Experts (GGE) on cybersecurity recommends that States agree on standards and rules, covering actions below the threshold of international conventions, such as confidence-building measures. The EU thus endorses "*the voluntary non-binding norms, rules and principles of responsible State behaviour that have been articulated by the UN Group of Governmental Experts*"[1], as a complement to binding international law.

Before talking about what the EU institutions say about these rules, as well as how and to what extent these rules apply to the EU (**2**), it is important first to mention the activity of the EU for promoting an international rules and norms on cyber operations, whether offensive or defensive (**1**).

1. The EU Cyber Diplomacy and States' Responsible Behaviour

International law has long been one of the key vehicles for regulating the behaviour of states and state-sponsored actors in cyberspace. When it comes to international peace and security, however, there are no cyber-specific conventions. As such, international law's application to cyberspace will largely depend on customary international law (i.e., state practice accepted as law). I am primarily concerned here with the law of international responsibility of States and the law of the use of force, also known as *jus in bellum* or *jus contra bellum*. The law of State responsibility and the law of the use of force are intended to determine the lawfulness of the actions of the States concerned and, consequently, they treat the responsible State in a different manner from the victim State.[2]

[1] Retrieved from https://eucyberdirect.eu/atlas/country/european-union/compare/south-korea (accessed on January 3rd, 2022)

[2] See also K. Bannelier-Christakis, 'Laws of Gravitation. Due diligence Obligations in Cyberspace', in P. Pawlak, T. Biersteker eds., *Guardian of the Galaxy. EU Cyber Sanctions and Norms in Cyberspace*, Chaillot Paper 155, oct. 2019, 62-69; K. Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2015), 14 *Baltic Yearbook of International Law Online* 1, 23-39.

The States are responsible in general for actions which violate their international obligations. In such cases, cyber operations may be put into action to atone for cyber campaigns or cyber-attacks.[1] This State responsibility is customarily founded and reflected by the International Commission on International Law within the articles upon Responsibility of States for Internationally Wrongful Acts.[2] Article 2 states that, such an act from a State exists when the conduct, which constitutes an act or omission, is imputable to the State in accordance with international law and constitutes a violation of its international obligation (**i**).

But cybersecurity is an issue not only for states but for the EU as well. After discussing in February 2015, the necessity for joint cyber diplomacy, the EU adopted the "*Cyber Diplomacy Toolbox*" in October 2017. Its main goal is to guarantee the responsiveness of its foreign and security policy below the threshold for armed conflict. At the EU level, responding to attacks with cyber diplomacy, triggers the political measures contained in the CFSP, including restrictive measures. Measures under the Cyber Diplomacy Toolbox do not require legally secured attribution in every case. However, difficulties with reliable attribution represent a key challenge in planning cyber sanctions (**ii**).

i. State Conduct of Cyber Operations and the Attribution Issue

The nature of cyberspace as well as the design of the internet, which did not foresee the capabilities of tracing and tracking its billions of users, make today naming perpetrators of both cyberattacks and other cyber activities a difficult task. On the one hand, the perpetrators are given the opportunity to cover up and disappear, and on the other it requires sustained and significant effort, modernisation, development, and sufficient time on the part of victim-states to give the cyberattack the precision needed to its real perpetrator. It may thus be understood that this is a problem involving technical issues,[3] which must be considered and resolved on a possibly parallel basis. Power and capabilities vary considerably from country to country, and the gap is even greater in cyberspace as it is more difficult to prevent cyberattacks compared to conventional data attacks of inherent difficulties in naming the perpetrators discussed above.

Attribution refers therefore to "*the process of attributing an act or conduct to its perpetrator. The process of attribution is at the same time legal, factual and technical*"[4]. To tackle the problem of attribution in these cases,

---

[1] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 84-85

[2] Available at https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (accessed on February 26th, 2021)

[3] See P. Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility', (2013) 14 *Melb. J. Int'l L.* 496

[4] Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229, 233

the adoption of presumed state responsibility, which carries the burden of proof and puts the responsibility on those States which do not take the necessary measures to prevent, investigate and repress, has been supported. Cyberattacks may also be carried out by non-state actors in their territory. But when can a cyberattack or equivalent action be attributed to the state and what are the criteria that can be used?

Regarding the two main criteria supported, the effective control and the overall review, the first was formulated by the ICJ in the Nicaraguan case,[1] while the second one was analysed in the *Tadic* case by the International Criminal Tribunal for the former Yugoslavia (ICTY).[2] However, no criterion has so far been unanimously and definitively adopted by the States. On the contrary, both criteria are criticised for presenting specific weaknesses. For example, the criterion of effective control, and less so of the total, is considered quite demanding when one considers the intrinsic difficulties inherent in cyberspace. So, given that their conditions are difficult to meet, there is a risk that some states will exploit this gap and the resulting impunity for carrying out cyberattacks through non-state actors serving their interests moving to the limits of legitimacy (Sponsored or Proxies' actions) probabilities of escalation due to some cases.

Other similar or non-similar criteria have therefore been supported in the context of how best to address the problem. Based on the case of *Homer* at the Unite States Embassy in Tehran[3], the government's criterion of knowledge has been proposed. The rationale for this criterion is based on the parallel knowledge that the Iranian government had with its obligation to protect the US Embassy and its staff under the 1961 Vienna Conventions on Diplomatic Relations and the 1963 Consular Relations, with knowledge of a government's obligations under international law to deter citizens from conducting cyberattacks (whether through its information infrastructure or not). If the government fails to comply with its obligation, then it will bear the corresponding responsibility. It is doubtful, however, whether and to what extent States would accept to commit themselves to undertaking such obligations in such a vast and field. On the other hand, states that are threatened or found to be victims would obviously be tempted by a less demanding criterion like the one above.

The criterion of knowledge has been formulated in another form without altering its essence. More specifically, it has been referred to as the *blind-eye standard* based precisely on the obligation of States not to knowingly allow their territory to be used for acts which may prejudice the rights of other States. As will be discussed below, this obligation is also supported in cyberspace by explicit reference to the second edition of the Tallinn Handbook[4]. Among the proposed criteria also figures the criterion of total control driven by the much faster and more complete access to information about a cyberattack by non-state actors, which the state may have funded or supplied with the software needed, compared to the victim state. Thus, the information

[1] Case Concerning Military and Paramilitary Activities in and against Nicaragua (n55) para. 105.

[2] Case No. IT-94-1-A (Prosecutor v. Tadić), Appeals Chamber Judgment, 1999, ICTY, 15, para. 131.

[3] Case Concerning United States Diplomatic and Consular Staff in Tehran (n107).

[4] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 30-50

supplied may indicate either that the state, which supplied the non-state actors, was not involved in the cyberattack, or that it was incapable of controlling the perpetrators, or that it ultimately had any effective involvement. In case of refusal to cooperate and supply information, it is proposed that measures and sanctions be taken, up to the level of violence in the context of legal defence per Article 51 of the CUN.

Steming from the existing international law and the obligation of any State not to allow knowingly its territory to be used for acts contrary to the rights of other States, it is worthing also to mention the concept of *cyber-dilligence*, which was developed by *Karinne Bannelier* and *Théodore Christakis*.[1] Following this approach, "*states are required to be reasonably vigilant with respect to the activities that are conducted within their territories according to their respective capacities*"[2]. Since the principle of due diligence is an obligation of conduct and not one of result. Knowledge, capacity, risk and harm constitutes therefore the four main variability factors for the evaluation of its effectiviness.

From what has been mentioned until now, it can be concluded that the criterion of total control may meet the needs of cyberspace to a greater extent than the strict and dysfunctional criterion of effective control.[3] However, the proposed criterion of effective control, combined with that of total control, is quite tempting, although it will be difficult to be adopted by all States at this stage, since it is burdensome and does not satisfy the interests of most. The addition of Rule 6 and 7 to the second edition of the Tallinn Handbook, which explicitly now entrusts States with the task of guarding, proves however that we are facing a field that is fully evolving, capable, and not adequately supported.

The "*Cyber Diplomacy Toolbox*" incites the Member States of the EU on "*using different methods and procedures for attributing malicious cyber activities, as well as employ different methods and procedures to establish a degree of certainty on attributing a malicious cyber activity*". The member states are not meant to coordinate their actions, since attribution is remains a sovereign act. A sitatuation that may lead to a lack of coherence when imposing cyber sanctions.

ii. EU's Framework for a Diplomatic Response to Malicious Cyber Activities

[1] See K. Bannelier and T. Christakis, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors* (Les Cahiers de la Revue Défense Nationale, 2017); See also K. Bannelier-Christakis, (2017), 'Obligations de diligence dans le cyberespace : qui a peur de la cyber-diligence?' 2 *Revue belge de droit international*, 612–665; K. Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2015), 14 *Baltic Yearbook of International Law Online* 1, 23-39.

[2] K. Bannelier-Christakis, 'Laws of Gravitation. Due diligence Obligations in Cyberspace', in P. Pawlak, T. Biersteker eds., *Guardian of the Galaxy. EU Cyber Sanctions and Norms in Cyberspace*, Chaillot Paper 155, oct. 2019, 62–69

[3] Interview 7

The "*EU Cyber Diplomacy Toolbox*" was adopted in 2017.[1] In terms of the inclusion of the CSDP in cyber defence, this toolbox makes use of the restrictive measures, to prevent and respond to malicious cyber activities. Its measures can be divided into "*preventative, cooperative, stabilising, and restrictive, as well as Member States' lawful responses for self-defence*"[2]. It also supports *confidence building measures* (hereafter CBMs), which aim minimizing causes of mistrust between states.

Instead of a pure maximisation of interests, normative deterrence would then make it possible to do what is right, and the UN-GGE on cybersecurity moreover recommends that States should get along with norms and rules, covering actions below the threshold of international conventions, such as confidence-building measures. However, there is a plethora of information sharing mechanisms that have a reasonable chance of being successfully adopted in the cyber arena. Nevertheless, significant obstacles remain regarding the acceptance of other categories of confidence-building measures - such as notification,[3] observation[4] and stabilisation measures.[5] For example, the notification of a cyber event or exercise, including allowing potential adversaries to observe it, can be counterproductive in the realm of cyberspace since this might reveal information about vulnerabilities that an observant adversary might later exploit.

The EU strongly promotes the position that international law, and in particular the United Nations (UN) Charter, applies in cyberspace. After introducing the legal framework for targeted restrictive measures against cyber-attacks in May 2019, [6] the EU uses its *cyber diplomacy toolbox* to prevent, discourage, deter and respond to malicious cyber activities. The EU listed thus six individuals and three entities responsible for, or involved

[1] Council of the European Union, 'Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") - Adoption', 9916/17, 7 June 2017, Brussels.

[2] A. Bendiek, 'The EU as a force for peace in international cyber diplomacy', (2018), SWP Comment, 19/2018, Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit.

[3] The notification concerns the prior warning of major military activities within a geographic concentration, such as a military exercise or a major change in the distribution of forces.

[4] Observation measures include activities such as inviting potential adversaries to physically observe military exercises, commissioning new weapon systems, or other related military activities first-hand.

[5] Stability in a crisis (relative absence of pressure to undertake early military action to prevent the movements of the adversary); stability of the arms race (relative lack of incentive to expand military forces); and political stability (relative absence of pressure for the collapse of international order). Johan Jørgen Holst, "Confidence-Building Measures: A Conceptual Framework," Survival 25, no. 1 (January / February 1983): pp. 2–15

[6] Council of the European Union, 'Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive meas-ures against cyber-attacks threatening the Union or its Member States', L129 I/1. Art. 2. Available at https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX%3A32019R0796 (Accessed on January 8th, 20212.

in cyber-attacks affecting the EU and its Member States under the regime in July 2020.[1] Another two individuals and one body were listed in October 2020. [2]

Each Member State can submit a proposal to activate a specific measure or escalatory step from the repertoire of the cyber diplomacy toolbox. The preparatory work for the Council decision is conducted by the Political and Security Committee (PSC), the Horizontal Working Party on Cyber Issues, the Commission President, and its deputies, as well as the High Representative for Foreign Affairs and Security Policy. Cyberattacks are debated and managed in the Horizontal Working Group. The later receives evidence (comprehensive intelligence, publicly available information, technical indicators etc…) which is investigated and verified by law enforcement agencies and intelligence services of Member States, in cooperation with the Computer Security Incident Response Teams (CSIRTs), the European Cybercrime Centre (EC3), the ENISA or the EU Computer Emergency Response Team (CERT-EU).

In so far, the EU has imposed sanctions only for recent malicious campaigns, which were attributed by at least one EU member state.[3] As far as tangible evidence goes, there is no proof that sanctions deter anyone, impose costs or restrict an adversary's ability to conduct their malicious campaigns.[4] Furthermore, attribution of responsibility to a State or a non-State actor may also hamper deterrent effectiveness of this legal framework, as it "*remains a sovereign political decision based on all-source intelligence and should be established in accordance with international law of State responsibility*"[5], though the political attribution of cyber incident's responsibility may be a long run, lowering the standard of legal attribution for cyber incidents.[6] The dangers posed by proxies, i.e., non-state actors acting on behalf of the state, reduce the effectiveness of trust- and security-build-ing actions. The question that arises however is to what degree the EU and its Member States may have recourse to counterattacks.

[1] Council of the European Union, 'Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', ST/9568/2020/INIT, OJ L 246, 30.7.2020, p. 4–9; Council of the European Union, 'Council Implementing Regulation (EU) 2020/1744 of 20 November 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', OJ L 393, 23.11.2020, p. 1–2.

[2] Council of the European Union, 'Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States', OJ L 351I , 22.10.2020, p. 1–4.

[3] Source: https://www.sanctionsmap.eu/ (accessed on January 8th, 2022).

[4] Soesanto, S. 'Europe Has No Strategy on Cyber Sanctions', 20 November 2020. Available at https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions (accessed on January 8th, 2022).

[5] Council of the European Union, Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Mali-cious Cyber Activities (9 October 2017).

[6] Homburger, Z. 'Conceptual Ambiguity of International Norms on State Behaviour in Cyberspace', (2019), *EU Cyber Direct*. Available at https://eucyberdirect.eu/wp-content/uploads/2019/05/zine-homburger-conceptual-ambiguity-of-norms-april-2019-eucyberdirect.pdf (accessed on January 8th, 2022).

2. CSDP Missions and the Cyber Based Operations in Cyber Armed Conflict

Any engagement of the EU for promoting or implementing IHL should be based on the rule of law. The CJEU affirms that "*the EU must respect international law in the exercise of its power*"[1], even when EU-led forces become "*engaged in an armed conflict*"[2]. However, the EU has mainly referred to IHL in its policy and in non-binding sources.

As sovereign and self-governing entities, states enjoy exercising their political autonomy not only within their territories but also in their external activities and foreign affairs. Foreign policy provides states with opportunities to formulate interests, make decisions and act independently in their attempts to influence events outside their territories. The CSDP has equipped the EU with autonomy in international conflict management. It has provided the EU with an independent capacity to launch autonomous missions outside the UN framework (**i**). The rules of engagement for EU missions are therefore decided by the EU countries.

The EU and its Member States accept that when EU-led forces become a party to an armed conflict, IHL will fully apply to them. When IHL does not apply, the EU primarily looks however towards human rights law as the proper standard for the conduct of EU military operations. Two principles of customary IHL may affect the conduction of cyber-operations, when conducted by EU-led operations: the principles of military Necessity, Discrimination and Proportionality (ii) and the principle of impartiality (**iii**).

i. Ensuring EU's Autonomy from United Nations Framework

With the establishment of the CSDP, EU states previously active in UN peacekeeping turned their attention and resources away from the UN to their own instruments. This shift occurred despite the EU states' pledged commitment to the UN peace missions. Scholars are noticing that the development of the CSDP logically encouraged the EU block to revisit its relationship with the UN as it increased the EU's independence from the UN in international conflict management. EU countries enjoy having autonomy in their international engagements, including in the area of civilian and military conflict management. For these reasons, they prefer to participate in UN mandated rather than UN-led operations.[3]

The UN aims to keep international peace and security, promote international relations between states based on the principle of equal rights and the self-determination of peoples, and work together to solve international economic, social, cultural, and humanitarian problems. as well as in promoting respect for human rights and

[1] Case C-285/12, *Aboubacar Diakité v Commissaire général aux réfugiés et aux apatrides*, OJ C 93, 29.3.2014, p. 6–7

[2] See F. Naert, 'Observance of international humanitarian law by forces under the command of the European Union', (2013) *International Review of the Red Cross* 95, 637–643.

[3] Ojanen, H. 'The EU and the UN: a shared future', (2006), *Finnish Institute of International Affairs Report* 13.

human freedoms (Article 1 CUN). It should be noted that, the end of World War I coincided with the rise of the principle of ethnicity ,while the end of World War II was associated with the emancipation of peoples on a global scale. The belief that prevailed in the functioning of the UN was more realistic than League of Nations function because it focuses on the principle of balance of power and not on a theoretical legal approach. The UN works based on the sovereign equality of Member States and emphasises non-interference in the internal affairs of its sole responsibility.

However, the Union is not a member of the United Nations. It is thus not bound by the decisions of this organization and does not have to apply them. As stated by advocate's General Wathelet in his opinion to the CJEU in the case C-266/16[1],

> "*the possibility of relying on the rules of international law must indeed be subject to certain conditions, (...) namely that the Union must be bound by the rule relied on, the content of which must be unconditional and sufficiently precise and, last, the nature and the broad logic of which do not preclude judicial review of the contested act*."[2]

The Member States of the EU have transferred part of their powers to the EU, and as a result an interweaving of the community as well as international systems have been created.

The EU Treaty accords an important role to international law in the EU's external relations, even more so after the Treaty of Lisbon. Article 3(5) EU Treaty now states that the EU shall contribute to "*the protection of human rights, ..., as well as to the strict observance and the development of international law, including respect for the principles of the United Nations Charter and international law*". Thus, the EU Treaty requires that the EU respects international law and human rights in the conduct of its external relations.[3]

In the *Yussuf*[4] and *Kadi*[5] judgments, which was confirmed by two other judgments of the General Court of the EU, the *Ayadi* case of 12 July 2006, T-253/02[6] and the *Minin* case of 31 January 2007, T-362/04,[7] the Community judge took a position on the place occupied by the law stemming from the Charter of the United

[1] Case C-266/16, *Western Sahara Campaign UK v Commissioners for Her Majesty's Revenue and Customs and Secretary of State for Environment, Food and Rural Affairs*, ECLI:EU:C:2018:118

[2] Case C-366/10, *The Air Transport Association of America, American Airlines, Inc., Continental Airlines, Inc., United Airlines, Inc. v The Secretary of State for Energy and Climate Change*, OJ C 260, 25.9.2010, p. 9–10

[3] There is no specific mention of international humanitarian law, but this branch of international law is obviously covered by the more general term international law.

[4] Case T-306/01, *Ahmed Ali Yusuf and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities*, ECLI:EU:T:2005:331

[5] Case T-315/01, *Yassin Abdullah Kadi v Council of the European Union and Commission of the European Communities*, ECLI:EU:T:2005:332

[6] Case T-253/02, *Chafiq Ayadi v Council of the European Union*, ECLI:EU:T:2006:200

[7] Case T-362/04, *Leonid Minin v Commission of the European Communities*, ECLI:EU:T:2007:25.

Nations. It notes that, the international treaties and the rules which stem from it, cannot affect the autonomy of the legal order of the EU, nor its constitutional principles.[1] The Court has proven that the protection of fundamental rights, including liberty, democracy and respect for human dignity, is subject to compulsory Community law. By analogy, we could speak of an *ius commune europaeum*, a non-negotiable hard core of the EU authorities under which, each EU operation is controlled even if it was issued based on a resolution emanating from the United Nations Security Council.

These cases have raised an extremely important question for the legal world. Is a rule initiated by a resolution of the Security Council of the United Nations treated differently according to its association to EU's rule? At this point, it should be recalled that, it is common for sanctions to be imposed against a third country by a United Nations resolution. The content of which, reintroduces then a common position of the Council of the EU and finally implements a regulation community. This practice has become so widespread that, it is considered to serve and to defend international legitimacy against threats from globalization, such as terrorist attacks and serious human rights violations under totalitarian regimes.

In both cases, the Court's decision was awaited with particular interest, the latter being called upon to authentically clarify and adjust the position of the Community legal order vis-à-vis international law regarding sanctions. The international sanctioning mechanism has since presented a complex picture, which refers to a "*waltz in three stages*"[2] because it required a participation to varying degrees and levels of, international, European and national law. Nevertheless, it admits that United Nations Security Council resolutions do not bind the Community under international law, the Community not being a member of the United Nations. The General Court of the EU has documented the commitment to the resolution in Community law itself in two ways: as a reflection and negative obligation, on the one hand and, as independent and a positive obligation, on the other. The judgment on the indirect obligation of the resolution on the Community implied a significant weakening of the Court's supervision, by effectively placing it under the jurisdiction of international law. It stressed that, in very exceptional cases, the Court could carry out a fortuitous review based on *jus cogens*, within the meaning of international public policy and in terms of "*imperative rules for the universal protection of human rights*".

The General Court thus made the *Yussuf* and *Kadi* judgments a case law reference which it does not hesitate to cite in its later judgments. The Lisbon Treaty reform seems to follow on from these judgments reaffirming the superiority of the Charter in various articles. The position of Attorney General M.P. Maduro, who stressed that the autonomy of the Community legal order on the international level does not mean isolation, even less the rejection of international law, because it is explicitly recognised that the organizations must carefully examine the Community's obligations at international level and take them into account. However, these

[1] See further, J. Santos Vara, 'The Consequences of Kadi: Where the Divergence of Opinion between EU and International Lawyers Lies?', (2011), 2 *European Law Journal* 17.

[2] See F. Naud, 'L'embargo : une valse à trois temps - Nations Unies, Union européenne et Etats membres', (1997) RMCUE 404

obligations under international law are not accepted by the Community as such and without preconditions but are figured out on the basis of the conditions laid down by Community law itself.

In the EU Treaty, the relevant goals of the CFSP to the issue of defence are stated as follows:

> "*to safeguard the common values, fundamental interests, independence and integrity of the Union in conformity with the principles of the UN Charter; and to preserve peace and strengthen international security, in accordance with the principles of the UN Charter, as well as the principles of the Helsinki Final Act and the objectives of the Paris Charter, including those on external borders.*"[1]

Even though the EU is not a member of the UN though all its Member States are, and have to therefore comply with the CUN. However, the EU Treaty is vague on the issue of whether the EU may act unilaterally or whether the authorisation of the Security Council is necessary before the EU may use international force. Furthermore, there is still little consensus on standards for responding to cyber actions below the thresholds relevant under international law (retorsion).

There are no signs of the EU undertaking humanitarian interventions or of undertaking military interventions without the authorisation of the UN Security Council. The Treaty itself, however, does not rule out such action. However, an EU intervention would only be initiated under a UN mandate, irrespective of what is stated in the TEU, and according to current international law, in which the UN Security Council is the only body that can provide legal authorisation of the use of force[2]. Thus, EU's primary law does not give the right to start a war or an act of retaliation against a cyber operation/incident/attack leaving place for international law application. However, whenever the EU initiates CSDP missions which use cyber-based operations, the principles of military necessity, discrimination, and proportionality and of impartiality should be observed.

ii. Principles of Military Necessity: Discrimination and Proportionality

By the principle of military necessity, a military attack is only permissible during a time of war when it is directed against objectives which, by their nature, their location and the purpose they serve, contribute substantially to military action and to total or partial destruction or offers a clear military advantage, leading to a successful end to the conflict. Consequently, military attacks on protected civilian targets are forbidden. In the case of cyberattacks, the question arises therefore to know whether a cyberattack may be linked to the concept of *military attack* or not, to assess whether it may be considered (or not) prohibited against civilian targets as cyberattacks do not inflict material damage and casualties and therefore cannot be classified as banned attacks.

[1] Article 21 §2 TEU

[2] Article 53, Chapter VIII, UN Charter

The inclusion of cyberattacks in the protective area of the principle of military necessity adds extra confusion. Because according to this principle, many of the infrastructures that support such operations and the needs of the urban population are targets of cyberattacks, which serves both the military and civilian needs. On the other hand, attacking such a *dual-use* target is tolerated when it effectively contributes to military action and offers a clear military advantage, but should be pursued as far as possible rather than destroyed.[1] In conclusion, if the target of this category were an infrastructure that supports its operation on an electronic network, a cyberattack aimed at disrupting the network and so disabling the facility would probably be in line with the principle of military necessity.

The purpose of the principle of discrimination is to protect the urban population of citizens and their material goods serving their needs, by separating them respectively from persons who are actively fighting. Members of the regular armed forces have the right to directly take part in hostilities and are protected by special rules in the event of their captivity or injury. On the contrary, ordinary citizens are prohibited from being targeted and are not actively involved in armed confrontation. In the case of cyberattacks, the above limits are indistinguishable. On the one hand, such an attack can also be carried out by a person who is not formally part of the armed forces of a state, which raises the question of whether this person's status as a soldier automatically changes.

Regarding the principle of proportionality, it prohibits the exercise of any kind and intensity of violence that goes beyond what is necessary to achieve a specific military objective. The occurrence of collateral damage during hostilities does not automatically amount to a breach of the above prohibition insofar, as it is proportionate to the military advantage secured. Given the simultaneous servicing of military and non-military needs by these infrastructures, a cyberattack on the electronic networks is highly likely to cause side damage.[2] The question then arises as to whether these effects are justified as a compensation for military benefits. To assess the proportionality of the reaction to a cyberattack, it is considered more appropriate to exercise defence by attacking the electronic systems from which it originates, on the grounds that the resulting damage will be less restrictive and less severe, than if conventional weapons are chosen as countermeasures.

iii. Principle of Impartiality

[1] Interview 7

[2] Interview 7

The principle of neutrality is customary and is codified in the Hague Conventions of 1899 and 1907, and in Conventions V[1] and XIII[2], which also apply in cyberspace. The basic obligation of neutral states is to refrain from specific actions and to pursue others with a view to enhancing and maintaining the neutrality regime by working impartially and keeping equal distances from the opposing parties.[3] On the other hand, the territory of the neutral state is inviolable, and the opposing parties must refrain from actions that may have a negative impact and may involve the latter in conflict, at the same time as maintaining commercial relations and official communications. [4]

It can therefore be noted that to keep the status of neutrality, there are specific obligations and rights. Starting with the inviolability of the territory of the neutral state,[5] the latter must not allow specific actions within it.[6] These prohibited actions include, for example, the transfer of troops, ammunition, and other related supplies through its territory[7] and the construction of a wireless station or other telegraph system for the purpose of communicating with hostile forces or using such installed (and non-public) infrastructures for purely military purposes.[8]

Concerning the prohibition of Article 3 V of the Hague Convention, it appears to include both virtual communication stations and, on the other hand, to extend beyond the territory of the neutral state to the cyber-infrastructures of the opposing parties and to exercise the rights of the latter and other cyber-infrastructures under their control[9]. In addition, it is worthy to note that, the use of neutral cyber-communications (and more specifically public, international, and freely accessible networks such as the Internet)[10] does not affect the status of neutrality, even if such use is for military purposes[11]. It is however accepted that the neutral state must monitor

[1] Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 18 October 1907, 205 CTS 299.

[2] Hague Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War, 18 October 1907, 205 CTS 395.

[3] See W. Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', (2013) *International Law Studies* 89, 141-142

[4] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 562

[5] Article 1 V of the Hague Convention

[6] *Ibid*, Article 5 V

[7] Article 2 V of the Hague Convention

[8] *Ibid*, Article 3 V

[9] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 55

[10] *Ibid*, p. 556

[11] See W. Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', (2013) *International Law Studies* 89, 150

actions within its territory and prevent corresponding violations according to the means at its disposal and according to its powers.[1]

The question arises therefore on whether the neutral state should consciously allow the conduct of cyber-infrastructures within or within its territory. The theory has been argued that in both cases there is a relevant task, which is even breached (with respect to alleged knowledge) if the neutral state, despite its efforts, fails to prevent a hostile cyber-operation. This approach, however, does not appear to be in line with cyber related data and conditions. Given the high speed of conduct of cyber operations it is therefore argued that the knowledge on the conduction of cyber operations from its territory by a neutral state will only result in a violation of the law of neutrality if the cyber operation has not already ended at the time of exposure[2]. Based on the above, it would be impossible to deal with presumed knowledge differently. Prevention, which is equivalent to the task of monitoring state-of-the-art infrastructure by a neutral state, becomes extremely difficult even if it is implemented in proportion to the capabilities of each state.[3] The obligation to act impartially is clearly reflected in Article 9, which also explicitly states that the neutral state must ensure that individuals and private companies owning telecommunications infrastructures comply with this obligation.[4] By combining the above and considering Articles 2 and 5 V of the Hague Convention, the following approach has been advocated. If the neutral state has, either detected a malicious cybercrime or cyberattack and is therefore aware of it, or reasonably and reliably informed that such action has been initiated or transmitted through its cyber infrastructure, then the latter should not still be in progress in order not to violate the law of neutrality.

At this point, there is a particularity about the access to communications services as reflected in Article 8 V of the Hague Convention of 1907, which states that a neutral state "*(...) shall not use telegraph or telephone cables or wireless telegraphy apparatus belonging to it or to companies or private individuals*". It is argued for example that the notion of telegraph (not explicitly defined) and related services can now be extended to include telecommunications and satellite communications. Article 8 V of the Hague Convention is also applicable to cyber communication systems, while neutral states have the option of restricting or prohibiting the use of their cyber infrastructures by opposing parties, always addressing the latter in the same way[5]. The important issue however, has to do with the likelihood of transmitted information, data and loads through neutral cyber-

[1] The Hague Commission of Jurists, 'The Hague Rules of Air Warfare, 25 February 1923, Article 42.

[2] See W. Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', (2013) *International Law Studies* 89, 151

[3] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 559

[4] Interview 7

[5] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 557

infrastructures not merely communicating data but potentially cyber-weapons[1]. In short, Article 8 V can in this context protect not only the flow of information useful to a cybercrime or cyberattack but also the cyber-attack itself. Despite this possibility, it has already been noted that the use of public, international and freely accessible networks, such as the Internet, even for military purposes, does not violate the law of neutrality.

In addition to the obligations and tasks outlined above, the neutral state is likely to either fail or be unwilling to act appropriately, thus failing to counter offensive actions by one of its adversaries, which violates neutrality. It is therefore possible for the affected party to react by relying on the right of necessity to put an end to the above infringement. This customary right, also described as a form of self-help[2], is granted and only valid if certain conditions are met. Initially, it should be acknowledged that this should be a serious infringement, which offers a substantial military advantage over the adversary[3]. The existence of this condition may depend on several factors and should be examined on a case-by-case basis in the light of prevailing circumstances.[4] Subsequently, aggressive action on the territory of a neutral state should pose an immediate threat to the security of the affected party, while there should be no other (feasible and immediate) alternative response[5]. If the above conditions are met, the affected party may intervene either through related and appropriate cyber-enterprises or even through a natural invasion of the territory of the neutral state in order to put an end to the offensive actions carried out through neutral cyber-infrastructure. Finally, unless the security of the affected State is immediately threatened, the latter's cource of action requires prior notification of the neutral State, which provides a reasonable period of time for the settlement of the violation.[6]

The question arises however over how far EU governments should prepare to take technical countermeasures. According to the cyber diplomacy toolbox, active cyber defence measures would be the highest escalation level after prior activation of the treaty-based solidarity or mutual assistance.

[1] See N. Melzer, 'Cyberwarfare and International Law', [Research report], (2011), *United Nations Institute for Disarmament*, 20

[2] M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 560

[3] *Ibid*, p. 561

[4] M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 561

[5] See W. Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', (2013) *International Law Studies* 89, 150-151

[6] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 561

C. EU's Member States Sovereignty and The Right to Defend Against Cyber Campaigns

The *jus ad bellum* regime has an interdependent relationship with the concept of the state's territorial sovereignty. Thus, the *jus ad bellum*, or right of war, defines the conditions of legitimacy of war.[1] The *jus ad bellum* allows a political entity to take up arms in three cases: (a) self-defence, where that State is the victim of aggression by another State (Article 51 CUN); (b) assistance to the United Nations (articles 2§5 and 42 to 47 CUN), aimed at restoring peace in the face of a threat to the international community as a whole; (c) the armed struggle for national liberation within the framework of the right of peoples to self-determination, involving the struggle against racist regimes[2].

NATO categorises attacks in cyberspace as a form of warfare, which can trigger the mutual defence clause under Article 5 of the North Atlantic Treaty. In the case of self-defence or mutual defence within NATO, both defensive and offensive cyber-defence capabilities may be used. Since the Wales Summit of 2014, analysts acknowledged that a cyberattack may reach the legal threshold that would trigger defensive actions. At the Cyber Defence Pledge Conference in 2018, NATO's Secretary General Stoltenberg affirmed that, "*a cyber-attack could trigger Article 5 of our founding treaty where an attack on one Ally is treated as an attack on all Allies*"[3]. Recently, in June 7th, 2021, Stoltenberg reaffirmed that a cyberattack may trigger Article Five.[4]

Collective defence is thus the cornerstone of NATO, in which the European partners rely heavily on the deterrence assets of the US. The right of self-defence can be exercised individually or collectively as depicted in NATO's collective defence clause of Article 5 of the North-Atlantic Treaty, and in the EU's mutual assistance (or mutual defence) clause of Article 42(7) of the TEU. Aside from an assistance clause, the Member States of the EU can also invoke a solidarity clause (Article 222 TFEU) in the case of terrorist attacks or natural and man-made disasters.

CSDP's scope of action seems therefore to be expanded with two key Lisbon innovations in this area: mutual assistance clause and solidarity clause, which provide two additional EU institutional issues for addressing cyber incidents (**2**). But even when having recourse to EU's self-defence clauses against cyberattacks, States have however the obligation to respect Article 2§4 CUN with its principle of non-intervention refrain from the threat or use of force against the integrity or political independence of another State or in any other manner inconsistent with the purposes of the Charter of the United Nations (**1**).

---

[1] See B. Orend, *The Morality of War* (Broadview Press, 2nd edn, 2006)

[2] See United Nations General Assembly (UNGA) Resolutions 2105 (XX) of 20 December 1965; 2625 (XXV) of the UNGA of October 24, 1970; 3314 (XXIX) of the UNGA of 14 December 1974.

[3] NATO, 'Speech by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference', 15 May 2018, Ecole militaire, Paris. Available at https://www.nato.int/cps/en/natohq/opinions_154462.htm (Accessed on January 9th, 2022).

[4] Available at https://www.nato.int/cps/en/natohq/opinions_184735.htm (Accessed on January 9th, 2022).

1. Article 2 (4) of the United Nation Charter and The Principle of Non-Intervention

Following Article 2§4 of the CUN: "*All Members in their international relations shall abstain from the threat or use of violence against territorial integrity or the political independence of any state or any other action incompatible with the purposes of the United Nations*". The above prohibition is customarily founded in the Nicaragua case[1] as the International Court of Justice (hereafter ICJ) typically refers to. But it is also based on Declaration 2625 (XXV) of the 1970 UN General Assembly. It becomes thus clear from the foregoing that; the prohibition applies to UN Member States but also to non-Member States precisely because of its customary nature[2]. On the contrary, it is argued that it does not apply to non-state actors unless, as stated in them, their actions can be attributed to a state[3]. Issues automatically arise about both the concept of *violence* and what amounts to *threat or use of force*.

The prohibition of the use of force enshrined in the United Nations Charter applies also to cyberspace, as certain cyberoperations may constitute a use of armed force. For example, on September 9th 2019, France reaffirmed in its 20-page document on "*International Law Applicable to Operations in Cyberspace*"[4] that, "*a cyberattack may constitute an armed attack within the meaning of Article 51 of the United Nations Charter, if it is of a scale and severity comparable to those resulting from the use of physical force*". Aggression refers to the action of regular armed forces across an international border, as well as the dispatch by or on behalf of a State of armed bands or groups, irregular forces or mercenaries engaged in acts of armed forces.[5] Thus, *jus ad bellum* is based on two principles: (a) the prohibition on States to resort to armed force and (b) the establishment of a collective security system.

However, questions arise on whether, to what extent, and which cyberoperations can be considered 'violence' within the above context. At this point, it is however worthy to point out that, cyberattacks are a new and rapidly evolving form of attack compared to those predicted by the creators and designers of CUN in 1945. Consequently, CUN does not explicitly mention them. Insofar the most comprehensive resource is the "*Tallinn Manual 2.0 on the International Law of Cyber Operations*", produced by an international group of legal scholars

[1] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicar v. U.S.), ICJ, Merits, Rep. 1986, 14, para. 191-194.

[2] M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 330

[3] M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 330

[4] Available at https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (accessed on November 11th, 2019)

[5] Available at http://egal.un.org/avl/pdf/ha/sicj/icj_statute_e.pdf (accessed on November 11th, 2019)

and practitioners at the invitation of the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence (CCDCE) in 2009-2017.

The Tallinn Manual, which attempts to define in Rule 69 what type of cyber operations constitute a use of force, cites as an attack "*a cyberattack or defence cyber operation that is reasonably expected to cause injury or death to persons or damage or destruction of objects*". It is understood here that the term 'cyber operations' is broader than the term *cyberattacks*. Indeed, this Manual also states that non-violent operations, such as those of a psychological nature or cyber espionage do not constitute attacks as such an attack does not require mobility (compared to biological, chemical attacks etc.). On the other hand, it is argued that even a non-violent operation could be described as an attack if its results are catastrophic, while a violent operation that ultimately does not result in immediate injury, death or destruction does not detract from the nature of the attack.

These issues have been of particular concern to the international community with many consultations taking place and several proposals being made. For example, few states had suggested in the context of the San Francisco Summit on the design of the CUN in 1945 that, political or economic coercion might be considered as *violence*. Politics, and not just pressure, is however a daily occurrence in transnational relations. Thus, the ordinary meaning of the term *violence* has been argued to include various forms of coercion, such as psychological, economic, or political coercion. It has been also considered that, the concept of *violence* refers only to armed or military form of violence.[1] The question arises, however, whether its concept is ultimately equated with *armed violence* and thus, the use of the term *threat or use of armed violence* would be more and more appropriate.

The international panel of experts in the second edition of the Tallinn Handbook selects the criterion of "*scale and effects*" [2], a criterion applied by the ICJ in the Nicaragua case[3] to distinguish what actions constitute armed attack. The proportional application of this criterion regarding the distinction between acts of cybercrime that constitute a threat or the use of violence and acts of cybercrime that do not reach this threshold was considered the most appropriate. This option is based on the fact that those cybersecurity firms whose scale and results are comparable to those of other conventional firms have no reason to exclude themselves from the range of actions that can be attributed to the use of force[4]. A more detailed reference to the characteristics of this criterion will be made, however, in the next section.

[1] See Y. Dinstein, *War, Aggression and Self-Defense* (Cambridge University Press, 4th edn, 2005), 85-87

[2] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 330

[3] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicar v. U.S.), ICJ, Merits, Rep. 1986, 14, para 195

[4] See M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 331

From the foregoing, cyber-enterprise cannot be characterized as a threat or use of force, when they are intended to coerce an economic or political force. It is also concluded that, the concept of *violence* in Article 2§4 CUN does not only cover the characteristic and clear case of armed violence since it has been judged to fall under the above context as well as cases that remain. So, it may be possible that, some cyber enterprises fall under this concept and threaten or use violence, but not armed violence. In practice, however, and according to current data, no corresponding examples have been formally noted.

This is due to the difficulty to attribute such actions to a state; the reluctance of states to reflect the consequences of being labelled as a cybercrime and the fact that many powerful states today are sometimes the victims of such actions. It is therefore noted that there is a gap between those companies that clearly threaten or use violence and those that do not, a large area whose content is controversial and has not been explicitly clarified. Finally, it is considered that cyber-espionage and other similar methods (such as those of the CUN category) do not fall under the framework under consideration, since it is now generally accepted that cases of espionage, surveillance, information extraction and commercial exclusion do not fall under the concept of *violence*.[1] However, interventions which are not equivalent to threats or to the use of force within the meaning of Article 2§4 of the CUN may violate the usual principle of non-intervention.

Both NATO and EU mutual defence clauses have a territorial scope[2] and refer to attacks on the territory of the Member States. NATO includes extraterritorial military assets within the region demarcated by Article 6 of the North Atlantic Treaty, but excludes overseas territories (e.g., Dutch or French Antilles).[3] The EU, on the other hand, includes the latter. The EU solidarity clause also relates to territory but to a lesser extent, meaning that the EU could, ex Article 222 TFEU, still request assistance for disasters happening to military forces or Embassies located outside the EU. The next part highlights the EU's collective cyber defence.

2.The EU's Solidarity and Mutual Assistance Clauses: An Institutional Solution for Collective Cyberdefence

According to the 2013 EU-CSS wording, "*a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause*", which figures at article 222 of TFEU. The EU Solidarity Clause requires that "*the Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster*". If such an

[1] See T. Christakis and K. Bouslimani, ' National Security, Surveillance and Human Rights' (December 1, 2019). R. Geiss, N. Melzer (Eds), Oxford Handbook on the International Law of Global Security, Oxford University Press, 2020 (Forthcoming), Available at SSRN: https://ssrn.com/abstract=3599994.

[2] Perot, "The Art of Commitments: NATO, the EU, and the Interplay between Law and Politics within Europe's Collective Defence Architecture." pp. 49-50.

[3] Sherrod L. Bumgardner, "Article 4 of the North Atlantic Treaty," Emory International Law Review 34 (2019). p. 76.

incident occurs, the EU shall mobilize – upon request of the Member State's political authorities – all the instruments at its disposal, including military resources made available by Member States, to "*prevent the terrorist threat in the territory of the Member States*" or to "*assist a Member State in its territory (...) in the event of a natural or man-made disaster*".

It should be noted that Article 222 TFEU uses the terminology of collective security by targeting both the threat and the terrorist attack. However, this mechanism is not part of the exercise of collective self-defence, which is authorised by Article 51 of the UN Charter and which (at least to date) seems to only be aimed at the assumption of the attacks from one State to another and not from non-State entities. The definition of the attack plays a fundamental role in collective defence clauses, which must necessarily be part of the law of self-defence authorised by international law. The fact that Article 222 TFEU also covers the assumption of assistance in the event of the occurrence of a natural disaster confirms its externality in relation to self-defence. The 2013 EU-CSS alluded however to the possibility to invoke Article 222 TFEU in case of a serious cyber-attack.[1] While the 2020 cybersecurity strategy expresses the need for the EU to 'reflect upon the (…) possible use of Article 42.7 TEU and Article 222 TFEU.[2]

The publicly available records do not reveal whether the meanings of a "*terrorist threat*" and a "*natural or man-made disaster*" were discussed at all during the drafting process. However, the Council of the European Union has subsequently defined these terms in its Decision 2014/415/EU,[3] which defines a *disaster* as "*any situation which has or may have severe impact on people, the environment or property, including cultural heritage*"[4]. This is a broad and flexible definition. The requirement of an impact being 'severe' echoes however the views expressed by national delegations according to which, the solidarity clause should be reserved for "*specific exceptional and emergency circumstances*". Thus, the disaster must be of such severity as to plainly overwhelm the capabilities that would otherwise be available to the affected country. Regarding the term of *terrorist attack*, the Council Decision 2014/415/EU defines it us a *terrorist offense*, as retained in Council Framework Decision 2002/475/JHA[5] ,while Directive 2017/541 on combating terrorism sets out a detailed list of terrorist offenses.[6] This list is extensive and includes acts, such as attacks upon a person's life which may cause death or upon private property likely to endanger human life or result in major economic loss.[7] It is also

[1] European Commission, Joint communication to the European Parliament and the Council on Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, Brussels, 7.2.2013, p. 19

[2] European Commission, Joint communication to the European Parliament and the Council on the EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, Brussels, 16.12.2020, p. 17

[3] OJ L 192, 1.7.2014, p. 53–58

[4] *Ibid*, Article 3(a)

[5] OJ L 192, 1.7.2014, p. 53–58, Article 3(b)

[6] OJ L 88, 31.3.2017, p. 6–21

[7] *Ibid*, Article 3

worth looking at how a cyber incident could fall within the categories of a *terrorist threat* and a *man-made disaster*.

Cyberattacks may be used as a means for terrorist attack when the action is committed "*with the aim of seriously intimidating a population, unduly compelling a Government or international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation*"[1]. In the same way, a cyber-attack can be a trigger for a man-made disaster, resulting in civilian casualties, loss of property or loss of basic services, as effects on critical infrastructures may be assimilated to a man-made disaster, if caused by deliberate or negligent human actions.

The principle of solidarity as found in Article 222 of the TFEU shall not be confused with the *mutual assistance clause* of Article 42(7) of the TEU, which obligates Member States to aid and assist another Member State that has been the victim of "*armed aggression on its territory*". Within the meaning of the UN Charter,[2] an act of *aggression* entails the unlawful use of armed force.[3] The fact that the mutual assistance clause refers to armed aggression confirms that it uses the word in this sense. It should be stressed here that that not only kinetic means of warfare can be considered as *armed aggression*.

The International Group of Experts estimated in Tallin Manual 2.0 that, the degree of seriousness of cyber-operations may be such as to justify an *armed attack*.[4] This is consistent with the insistence of the ICJ in its advisory opinion on nuclear weapons that "*the choice of means of attack is irrelevant to the question of whether an operation can be characterised as an armed attack*"[5]. Applying this reasoning to cyber-operations, Russia has reserved the right to use nuclear weapons in response to cyberattacks, while NATO has designated that cyberattacks could trigger NATO's Article Five.[6] In the case of the EU, it is about the impact rather than the choice of a weapon as Article 42(7) is not subject to the jurisdiction of the CJEU or any other compulsory interpretative process under the TEU.[7] Its interpretation falls to each individual member state. Following that, when a Member State invokes the Article 42(7) TEU, it also has to report to the Security Council on its national action or its common approach together with its EU partners[8], if the member states' security is significantly threatened by the consequences of an armed agression. It is thus a prerogative of the State to decide what means

[1] OJ L 164, 22.6.2002, p. 3–7

[2] Articles 1(1), 39 and 53(1) of the United Nations Charter

[3] Article 1 of the United Nations General Assembly Resolution 3314 (XXIX)

[4] Tallinn Manual 2.0 (n°2), 54, §3.

[5] ICJ, 'Legality of the Threat or Use of Nuclear Weapons', Advisory Opinion, 8 July 1996, para. 39.

[6] Available at https://www.nato.int/cps/en/natohq/topics_110496.htm (accessed on November 12th, 2019)

[7] Article 24(1) TEU

[8] *Ibid*

to utilise in case of a cyberattack against it. While the EU's mutual assistance clause would place any EU action within the context of armed aggression, the EU's solidarity clause would place it in the context of disaster response. Hence, in both cases the application of the clauses to situations of cyber agression is not always obvious. In practice, however, invoking a solidarity or a mutual assistance clause "*will most probably be driven more by political incentives than by legal doctrinal analysis*"[1].

The developments highlighted the *hybridity* of the legal framework of the EU, which oscillates between the hard and soft law across the European cyber policy mix. A limited transfer of competences, the lack of competences for the policy mix and its cross-cutting nature led the EU to apply different modes of governance in cyber policy. While decisions are made according to the ordinary legislative process for issues such as the security of the DSM, any decision having an impact on the national cyberdefence must employ soft governance.

Section II. The Institutions of Cybersecurity Policy: A Hybrid Mode of Governance

The idea of *governance* has become an increasingly central policy priority and organising principle for the European Union. In the Commission's report on European Governance 2003–2004, it is claimed that "*governance mechanisms seeking to enhance the effectiveness and efficiency of the decision-making system and ensure better involvement of more players will make the institutions more open, leading to increased responsiveness and accountability of institutions*"[2]. 'Governance mechanisms' refers to the empirical observable ways of coordinating the behaviour of political actors and reaching political decisions.

The changing design of EU governance is often characterised as marking a departure from the *Community Method* of governance to an arrival on *new modes of governance*. The traditional debates about EU governance opposed the *intergovernmentalists* (Soft Governance) against the *supranationalists* (Hard Governance) have evolved letting enough room for a new kind of debate between 'new' intergovernmentalists[3] – who insist that the more actively engaged, consensus-seeking member-state governments in the (European) Council have retaken control – and the *new supranationalists*[4] – who continue to see EU-level institutional actors such as the

[1] See R. A. Wessel, 'Cybersecurity in the European Union: Resilience through Regulation?', in E. Conde, Z. Yaneva and M. Scopelliti (eds), *The Routledge Handbook of European Security Law and Policy* (Routledge, 2020)

[2] European Commission Report on 'European Governance 2003–2004', 22 September 2004, SEC (2004) 1153, p. 38

[3] See C. J. Bickerton, D. Hodson and U. Puetter, *The New Intergovernmentalism. States and Supranational Actors in the Post-Maastricht Era* (Oxford University Press, 2015); See also U. Puetter, The European Council and the Council. New Intergovernmentalism and Institutional Change (Oxford University Press, 2014); S. Fabbrini, *Which European Union? Europe after the Euro Crisis* (Cambridge University Press, 2015)

[4] See M. W. Bauer and S. Becker, 'The Unexpected Winner of the Crisis: The European Commission's Strengthened Role in Economic Governance', (2014) 3 *Journal of European Integration* 36; See also R. Dehousse, 'The New

Commission as driving integration through their greater role in policy design and enforcement. But theoretical approaches to EU *hard* governance mainly relate to decision-making procedures[1], integration[2], Europeanisation[3] and enforcement[4]. While *soft* governance refers to "*compliance*" with *soft* law[5]. The consultation procedures and the Open Method of Coordination[6] are classic examples of *soft* governance.

The EU cybersecurity policy mix functions within several sectors and involves various stakeholders and institutions. Over the past decade, the EU has established several bodies that assist the Member States in the necessary cybersecurity and cyber defence capabilities development. Yet cybersecurity governance is fragmented at the EU level. This situation has led the EU to adapt the classic mode of *hard* institutional governance, with the reinforcement of the European Commission role through *soft* instruments (**§1**), while at the same time the Court of Justice of the European Union kept its traditional role as guardian of European citizens' rights (**§2**). The EU practice of *agencification* has resulted in an expediential development of EU's cybersecurity *soft* networked governance, with horizontal cooperation and information exchange between the various agencies being often limited (**§3**). Since a complex array of work among the 28 Member States and countries of the European Economic Area (EEA), including peer reviews of Member States, is done through the European Defence Agency (EDA), the ENISA, the European Cybercrime Centre (EC3) at Europol, and the future European Cybersecurity Competence Centre / Network.

§1. EU-Level Institutional Actors and 'New' Supranationalism: The Reinforced Role of the Commission in EU's Tradition Model of Hard Governance

With the entry of the Lisbon Treaty into force, the European Council has become an official institution of the EU providing the EU with *impetus* and *general political directions and priorities*. However, the European Council and its President have used of informally setting the agenda in a detailed way, often creating tension

Supranationalism', [Paper], 26-29 August 2015, *ECPR General Conference*, Montreal; V. A. Schmidt, 'Reinterpreting the rules 'by stealth' in times of crisis: a discursive institutionalist analysis of the European Central Bank and the European Commission', (2016) 5 *West European Politics* 39

[1] See F. W. Scharpf, 'Community and Autonomy: Multi-Level Policy-Making in the European Union', (1994) 2 *Journal of European Public Policy* 1

[2] See M. Cini, 'The Soft Law Approach: Commission Rule-Making in the EU's State Aid Regime', (2001) 2 *Journal of European Public Policy* 8

[3] See C. Knill and D. Lehmkuhl, 'How Europe Matters. Different Mechanism of Europeanisation', (1999) 7 *European Integration Online Papers* 3

[4] See J. Tallberg, 'Paths to Compliance: Enforcement, Management, and the European Union', (2002) 3 *International Organization* 56

[5] See G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States* (Cambridge University Press, 2005)

[6] See M. Egan and D. Wolf, 'Regulation and Comitology: The EC Committee System in Regulatory Perspective', (1998) *Columbia Journal of European Law* 4

with the Commission. A situation which leads the Commission to endorse a more *political role* and to intensify the usage of non-legislative policy instruments (**A**). Member States are however still primarily responsible for their own cybersecurity and mostly act at the EU level through the Council, which has still many coordination and information sharing bodies (**B**). The Commission and the Council having conserved important roles within the institutional cybersecurity governance, the European Parliament is still marginalised even if the Lisbon Treaty extended co-legislation to many policies (**C**). Lastly, regarding the Court of Justice of the EU actorness, its work is mostly focused on the respect of fundamental rights over cybersecurity matters, keeping thus its traditional role of guardian of the EU law's effectiveness (**D**).

A. The European Commission and The Usage of Non-Legislative Policy Instruments

Between 2007 and 2013, 73 out of 143 legal documents related to cybersecurity were adopted. The attacks against Estonia were considered as a threat to the internal market, hence the EU was able to initiate legislation and undertake the fortification of digital security measures.[1] The Commission decided to strengthen its intention to build a coherent approach to cybersecurity.

On 13 September 2017, Jean-Claude Juncker, President of the European Commission, stated in his regular annual report on the Union: "*in the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber- attacks. Therefore, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks*"[2]. The Commission and the EU High Representative proposed a reform package, which envisions EU's new, leading position in cyberspace.[3] The reform package includes the following six proposals:

> "*(a) Establishing a stronger European Union Cybersecurity Agency built on the Agency for Network and Information Security (ENISA), to assist Member States in dealing with cyber-attacks. (Proposal of the Cybersecurity Act); (b) Creating an EU-wide cybersecurity certification scheme that will increase the cybersecurity of products and services in the digital world; (c) A Blueprint for how to respond quickly, operationally and in unison when a largescale cyber-attack strikes; (d) A network of competence centres in the Member States and a European Cybersecurity Research and Competence Centre that will help develop and roll out the tools and technology*

[1] See R. S. Dewar, 'The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern', in M. O'Neill and K. Swinton (eds), *Challenges and Critiques of the EU Internal Security Strategy* (Cambridge Scholars Publishing, 2017), at 113

[2] European Commission, 'President Jean-Claude Juncker's State of the Union Address 2017', [Press Release], 13 September 2017, available at https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165 (accessed on September 8th, 2021).

[3] European Commission Joint Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', 13 September 2017, JOIN/2017/0450 final

needed to keep up with an ever-changing threat and make sure our defence is as strong as possible; (e) A Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and measures to strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO and; (f) Skills development for civilian and military professionals through providing solutions for national efforts and the set-up of a cyber defence training and education platform"[1].

The Commission's policy initiation activities are more specific than "*those involved in setting the broad agenda in that they involve the strategic formulation of, and the mobilisation of support behind, particular new policy initiatives, including legislative initiatives*"[2]. As with setting the broad agenda activities, policy initiation activities are highly politically contextualised. The number of legislative proposals has been however in a steady decline in recent years as EU decision-makers have looked to lighten the EU's legal load and have increasingly used non-legally binding policy instruments, having become more cautious about adopting Commission legislative proposals in topic areas that are strongly contested.[3]

The lack of precision of the TFEU in many respects has supplied with "*considerable opportunities for the Commission to also put forward new policy ideas via non-legislative policy instruments such as White and Green Papers, Communications, and Action Plans*"[4]. Ideas have often advanced in such instruments then subsequently re-appear in legislative proposals. Such, for example has been the case with the 2015 Communication on a Digital Single Market Strategy for Europe,[5] which set out "*a sixteen-point strategy for opening-up digital opportunities for people and businesses by removing regulatory barriers and creating a fully functional digital single market*".

Many EU institutions have started to include a cybersecurity in their national policies. Within the European Commission, two main directorates-general are tasked with addressing cybersecurity and cybercrime (DG CONNECT and DG HOME). The European External Action Service (EEAS) handles cyber diplomacy and cyber defence related to state activities and multinational or multilateral organisations (UN, NATO, OECD, etc.).

[1] Ibid

[2] See N. Nugent and M. Rhinard, 'The "political" roles of the European Commission, Journal of European Integration', (2019), 2 *Journal of European Integration* 41

[3] See C. J. Bickerton, D. Hodson and U. Puetter, 'The New Intergovernmentalism: European Integration in the Post-Maastricht Era', (2014) 4 *JCMS:Journal of Common Market Studies* 53

[4] See D. Dinan, 'Governance and Institutions: A More Political Commission', (2016) *JMCS:Journal of Common Market Studies* 54 (Annual Review)

[5] European Commission Communication on 'A Digital Single Market Strategy for Europe', 6 May 2015, COM(2015) 192 final

1. Commission's Services dealing with Cybersecurity Issues

DG Connect (Communications Networks, Content and Technology)

The European Commission Directorate General for Communications Networks, Content and Technology (DG Connect) (formerly Directorate-General for the Information Society (DG INFSO)) is in charge of policy activities on NIS and on CIIP, Electronic Signature Directive, eGovernment, the Safer Internet Programme, the ICT trust and security thematic of the Seventh Framework Programme for Research and Technological Development (FP7), the EU Regulatory Framework for Electronic Communications and the Digital Agenda.

DG Home

Ordinary criminals also make use of cyberattacks that threaten Europeans. That is why the Directorate-General for Migration and Home Affairs (DG HOME) of the Commission monitors and updates EU law on cybercrime and supports law enforcement capacity. The DG HOME seeks establishing an open and safer EU, so that the EU pursuits its development in a stable, lawful, and secure environment. Directorate D (Law enforcement and Security), more precisely its Unit D4 (Cybercrime) is the entity in charge of cybercrime issues. Directorate B (Borders, Interoperability, and Innovation), through Units B3 (Information Systems for Borders, Migration and Security) and C3 (Innovation and Industry for Security), is in charge of dedicated secure networks, databases and applications. In the field of cybersecurity, DG HOME focuses on:

- developing and implementing policies against cybercrime, including aspects of criminal law
- reducing vulnerabilities
- dealing with (criminal) threat alerts
- raising awareness
- providing ransomware-prevention advice
- dealing with issues related to deterring and investigating cybercrime, as well as judicial follow-up.

EEAS

When it comes to cyber diplomacy on a general level, the European External Action Service (EEAS) department specialised in cyber issues has progressively evolved in recent years. The EEAS cyber department is in charge of advocacy at NATO and the OSCE. The EEAS is also active in bilateral cyber dialogues between the EU and third countries and participates in both international conferences and more informal relationships.[1]

B. The Council of the EU and the Horizontal Working Party on Cyber Issues: Coordination through Intergovernmentalist Arrangements

The Council of the European Union, or more commonly known simply as the Council, is one of the main places where the osmosis of the national executive with the legislative power of the EU takes place and enjoys particular importance within the Union. It is the main instrument for representing the sovereignty of MS, at ministerial level, expressing on an equal footing the will of the latter for what is happening in the European Union.

Its main responsibility is to carry out legislative and budgetary tasks with the European Parliament while exercising policymaking and coordination functions. According to the agenda, it meets in a series of configurations, involving representatives of Member States' governments. Thus, in addition to the General Affairs Council, the Council meets in nine other compositions.[2] While the government representatives of Member States in the euro area meet at ministerial level, within the Eurogroup, which deals with issues of macroeconomic coordination and the single currency.

The General Secretariat of the Council regularly updates and publishes a list of the Council's preparatory bodies. Only committees and working parties on this list may meet as preparatory bodies of the Council. The list also includes horizontal groups strongly associated with COREPER and responsible for preparing its meetings[3]. Among COREPER's responsibilities is that of creating working groups or committees within the Council. The Councils working groups are responsible for preparing or examining the files to be created at COREPER and then at the Council. These ad hoc groups are set up to analyse and discuss proposals from the Commission to the Council, on issues requiring specialist and technocratic knowledge. Depending on the issue

[1] EEAS 3rd EU-Japan Cyber Dialogue – Joint Eléments, [Press release], 14 March 2018, available at:

https://eeas.europa.eu/topics/eu-international-cyberspace-policy/41330/3rd-eu-%E2%80%93-japan-cyberdialogue-joint-elements_en, (accessed on February 24th, 2021); EEAS, EU-US Cyber Dialogue, [Press release], 16 December 2016, available at https://eeas.europa.eu/headquarters/headquarters-homepage_en/18132/EU-U.S.%20Cyber%20Dialogue (accessed on February 24th, 2021).

[2] Based on the annex to the current rules of procedure of the Council, the Council meets at the level of: 1. General Affairs, 2. Foreign affairs, 3. Economic and financial affairs, 4. Justice and business internal, 5. employment, social policy, 6. Consumers, 6. Competitiveness (internal market, industry and research), 7. Transport, telecommunications and energy, 8. Agriculture and fisheries, 9. Environment and 10. Education, youth and culture (Council Decision 2009/937).

[3] These are the ANTICI Group, the Mertens Group, and the Friends of the Presidency Group.

to be considered, these groups have a time-limited mission. Of course, permanent working groups are also created within the Council and are set up by direct decision. The final reports and conclusions of these groups and committees are submitted to COREPER, essentially recommending their work. These teams are made up of officials from the Member States and the Commission. They are chaired by a representative of the country holding the presidency of the Council (unless COREPER decides otherwise) and are reasonably subject to the control of COREPER. All the intergovernmental bodies, constituting the basis of the Council's structure, are detailed in a note addressed to the General Secretariat of the Council.

The Horizontal Working Party on Cyber Issues was specifically created to offer additional co-ordination between Member States on cyber issues mainly the cyber policy and legislative activities. The working party closely cooperates with other related working parties as well as with the European Commission, EEAS, Europol, Eurojust, FRA, EDA, and ENISA. It has succeeded the Friends of the Presidency Group on Cyber Issues and it is responsible "*for bringing a large range of cyber related topics to the attention of COREPER and the Council in order to ensure coherence between areas as different as criminal justice in cyberspace and cyber diplomacy*"[1]. The main objectives of the working party are

> "*(a) ensuring a horizontal working platform providing for harmonisation and unified approach on cyber policy issues; (b) coherent progress in the cyber domain, while keeping up with cyber threats; (c) identify and expand cooperation with the Council preparatory bodies and other relevant actors; (d) information-sharing on cyber issues both among EU countries and national bodies; (e) setting EU cyber priorities and strategic objectives as part of a comprehensive policy framework and; (f) representation of the EU in accordance with the strategic EU cyber policy objectives*"[2].

C. The European Parliament: a Partial-Fledged Co-Decisive Entity

The European Parliament (EP) is the eminently political body of the EU since it is made up of representatives of the citizens of the Union (Art. 14 §2 TEU). Members of Parliament are elected by direct universal suffrage, free and secret, and simultaneously transported to all Member States. In this sense, the EP is the only one of the Union institutions where the idea of European integration has made the most progress compared to the other institutions. The European Parliament is the legislative body of the Union. It is elected by direct universal suffrage every five years. The last elections were held in May 2019. It has a legislative, supervisory, and budgetary role. The composition, the powers, and the way in which the EP works are governed by Articles 14

[1] H. Carrapico and A. Barrinha, 'The EU as a Coherent (Cyber)Security Actor? , (2017), 6 *Journal of Common Market Studies* 55

[2] Available at https://www.consilium.europa.eu/fr/council-eu/preparatory-bodies/horizontal-working-party-on-cyber-issues/ (accessed on February 22nd, 2021)

TEU and 223-234 TFEU, and by the EP's rules of procedure. It should be noted that a general revision procedure of this regulation entered into force on January 16th, 2017, which concerned the work of the committees, activities, and the administration of deputies and finally, the plenary sessions of Parliament.

The number of MEPs available to each Member State is proportional to its population, but it follows the principle of degressive proportionality. Members of the EP do not function as national groups but exercise their functions in political groups. These political groups are the European People's Party (EPP), the Progressive Alliance of Socialists and Democrats in the European Parliament (S&D), the European Conservatives and Reformists (ECR), the Alliance of Liberals and Democrats for Europe (ALDE), the Greens / European Free Alliance (Greens), European United Left / Nordic Green Left (GUE / NGL), Europe of Freedom and Direct Democracy (EFD) and Europe of Nations and Freedoms (ENF). Each political group is made up of at least 25 members, elected in at least a quarter of the Member States. The participation of members from several Member States within the same political group allows them to deal with different subjects in the interest of the Union, and not the narrow national interest.

To carry out the preparatory work for the plenary sittings of Parliament, the deputies are divided into several specialised standing committees. There are 20 parliamentary committees, made up of 25 to 81 MEPs with a chair, a bureau, and a secretariat. Their political composition depends on that of the plenary assembly. The committees prepare, amend, and adopt legislative proposals and initiative reports. Members of Parliament examine the proposals of the Commission and the Council and, if necessary, draw up reports which will be presented to the plenary assembly.

Parliamentary committees exercise an effective role in the legislative activity of the European Parliament. More precisely, the representativeness of the committees is linked to the cohesion of the groups. The latter is stronger in the most influential legislative committees and for legislative procedures.[1] The committees, by acting beyond their field of specialisation, give European policy-making a dimension that is both partisan and transversal. Some authors indeed describe parliamentary practices as highly technical in a field of specialisation limited to the scope of action of committees.[2]Four Committees have mostly participated in the legislative debate related to cybersecurity issues, by either proposing amendments or addressing opinions. These Committees are the Internal Market and Consumer Protection (IMCO) Committee, the Industry, Research and Energy (ITRE) Committee, (c) the Civil Liberties, Justice and Home Affairs (LIBE) Committee and the Foreign Affairs (AFET) Committee which includes two sub-committees: Human Rights (DROI) and Security and Defence (SEDE). All above mentioned Committees have participated in the legislative debate upon the adoption of the NIS Directive.

[1] See J. Navarro, 'Les rôles au Parlement Européen: Une typologie des pratiques de représentation', (2009) 3 *Revue française de science politique* 3

[2] See G. Marrel and R. Payre, 'Des carrières au Parlement : longévité des eurodéputés et institutionnalisation de l'arène parlementaire', (2006) *Politique européenne* 18

In the 2011 Working Document of Committee on Civil Liberties, Justice and Home Affairs on the European Union's Internal Security Strategy,[1] the Rapporteur, Mrs. Rita Borsellino, has draw attention to the marginalised role of the European Parliament:

> "*Incredible as it may appear, the principle strategic documents adopted to date by the European Council, the Council and the Commission seem to ignore the existence of the European Parliament altogether. While such a thing would, to say the least, have been surprising prior to the entry into force of the Lisbon Treaty, it is nothing less than inexplicable one year afterwards*".

Apart from cases in which the co-decision procedure applies, the European Parliament had indeed at that time only a limited role in cybersecurity policy.

The co-decision procedure is a legislative process introduced by the Treaty of Maastricht in 1991. Within this procedure, the European Parliament and the Council jointly adopt EU acts. The Parliament shares now a legislative authority with the Council. This legislative process can be considered as successful if a consensus has been reached between the Council and the Parliament. Since 1991, the co-decision procedure has been applied to most directives giving thus to the Parliament a much greater role in the formulation of EU legislation.

Now enshrined in Article 294 TFEU, the co-decision procedure or *Ordinary Legislative Procedure* made of the European Parliament a co-legislator only when provided by the Treaties. Otherwise, a consultation or consent procedure apply. The procedure comprises 1 or 2 readings, and if they fail, a conciliation procedure and the third reading. It has the effect of increasing contacts between the European Parliament and the Council, the co-legislators, with the European Commission. Although trilogues have no reference in the Treaties, within the 2009–2014 legislative period, "*1,541 trilogues were held for a total of 488 adopted co-decision files*"[2]. In the eighth term so far (from July 2014 to December 2017), EP committees have participated "*in a total of 683 trilogue meetings with the Council and Commission*", while "*198 trilogues had a single committee participating*".[3]

A comparative table presents which parliamentary committees have worked on legislative propositions, throughout the trilogue process (**Table 4**). It also reveals the widespreaded use of the ordinary legislative procedure on cybersecurity-related issues.

---

[1] European Parliament Working Document on the 'European Union's internal security strategy', 14 February 2011, PE458.598v01-00, available at https://www.statewatch.org/media/documents/news/2011/feb/ep-internal-security-working-doc-no-2-feb-11.pdf (accessed on September 8th, 2021)

[2] European Parliament Committee statistical report on '7th legislature 2009–2014', DGIpol – Unit for Legislative Coordination, available at https://www.europarl.europa.eu/cmsdata/198144/activity_report_2009_2014_en.pdf (accessed on February 23rd, 2021)

[3] Available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614733/EPRS_BRI(2018)614733_EN.pdf (accessed on February 23rd, 2021)

Document concerned	Type of Procedure (If applicable)	Committee(s) Report	Committee(s) Opinion
Regulation (EU) 2021/241	Ordinary legislative procedure	-	INTRE
Regulation (EU) 2019/2144	Ordinary legislative procedure	INTRE	-
Regulation (EU) 2019/943	Ordinary legislative procedure	INTRE	-
Regulation (EU) 2019/941	Ordinary legislative procedure	INTRE	-
Regulation (EU) 2019/881	Ordinary legislative procedure	INTRE	LIBE
Regulation (EU) 2017/1938	Ordinary legislative procedure	INTRE	AFET
Regulation (EU) 2017/1369	Ordinary legislative procedure	INTRE	-
Directive (EU) 2016/1148	Ordinary legislative procedure	IMCO	INTRE, LIBE, AFET
Regulation (EU) 2016/794	Ordinary legislative procedure	LIBE	-
Regulation (EU) 2014/513	Ordinary legislative procedure	LIBE	-
Regulation (EU) 283/2014	Ordinary legislative procedure	INTRE	IMCO
Regulation (EU) 2013/1291	Ordinary legislative procedure	INTRE	AFET
Directive (EU) 2013/40	Ordinary legislative procedure	LIBE	AFET, INTRE

Table 4: *Parliamentary Committees participation to cyber related trilogue processes*

Table made by author and source based on eur-lex

Regarding the EP's position on issues of cyber security and defence, it should be noted that from a formal and treaty point of view, this institution is not a fully-fledged co-decisive entity when it comes to shaping these issues.[1] Therefore, as a supranational institution, the European Parliament does not have decision-making powers with regard to the CSDP, which is dominated by intergovernmental cooperation mechanisms and of which cyber defence is one of the priorities. This means that, regarding the cyber defence policy, the EP's role comes down to being, first and foremost, a consultative institution.

For the most part, decision-making in the cyber policy field is characterised by lack of transparency and accountability. Parliaments still struggle to find their place in this policy area. Considering the importance of parliaments for democratic governance, this situation constitutes a serious problem. Important efforts are therefore needed to reinforce the position of the national parliaments for both to "*follow the development of European cyber security policy and to deliver well-founded opinions on cyber security issues*".[2]

[1] See European Parliament resolution of 12 December 2018 on the annual report on the implementation of the Common Security and Defence Policy, 2018/2099(INI), P8_TA(2018)0514; See also European Parliament resolution of 13 June 2018 on cyber defence, 2018/2004(INI), P8_TA(2018)0258; European Parliament resolution of 13 December 2017 on the Annual report on the implementation of the Common Security and Defence Policy, 2017/2123(INI), P8_TA(2017)0492

[2] A. Bendiek and L. Porter, 'European Cyber Security Policy within a Global Multistakeholder Structure', (2013), *European Foreign Affairs Review* 2

§2. The role of Court of Justice of the EU and The Judicial Review of National Measures: Preserving the Fundamental Rights of European Citizens

An increasing number of cases pertaining to digital issues and fundamental rights are brought before the Court of Justice of the European Union.[1] However, the European Court of Justice has not issued any rulings on cybersecurity specifically. The series of CJEU's cases law on data protection set however a clear precedent on the EU's approach to the protection of fundamental rights in cyberspace.

In the *Digital Rights Ireland* decision[2], the CJEU assessed the contended Data Retention Directive 2006/24/EC[3] and the fundamental rights to private life and privacy. The main objective of this directive is to harmonise the provisions of Member States on the retention of certain data generated or processed by providers of publicly accessible electronic communications services or of public communications networks. It thus aims to guarantee the availability of this data for the purposes of prevention, research, detection, and prosecution of serious offenses, such as offenses linked to organised crime and terrorism. Thus, the directive provides that providers must retain traffic data, location data and related data necessary to identify the subscriber or user.

The CJEU considers that this directive involves "*a large scaled and a serious interference in the fundamental rights in respect to private life and to the protection of personal data without this interference being limited to what is strictly necessary*". The Court considers that data retention does meet an objective of general interest, but that the Union legislature has exceeded the limits imposed in respect to the principle of proportionality. Indeed, the directive generally covers all individuals, electronic means of communication and traffic data without any differentiation, limitation or exception being made according to the objective of combating serious crime.

Access to data is not subject to prior checking by a court or an independent administrative entity. In addition, concerning the retention period of data, the directive imposes a period of at least six months (maximum 24 months) without making any distinction between the categories of data according to the persons concerned or the possible usefulness of data in relation to the objective pursued. The directive does not provide sufficient guarantees to ensure effective protection of data against the risk of abuse and against unlawful access and use of data. In *Tele2 and Watson*,[4] the CJEU confirmed thus that the standards set out in *Digital Rights Ireland* are mandatory and that the CJEU is indeed competent to review not only the retention, but also the access to data.

[1] Article 19 TEU

[2] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications*, OJ C 175, 10.6.2014, p. 6–7

[3] European Parliament and Council Directive 2006/24/EC of 15 March 2006 on 'the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC', OJ L 105, 13.4.2006, p. 54–63

[4] Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, ECLI:EU:C:2016:970

Barely a few days after the resounding invalidation of the *data retention* directive in the joined cases *Digital Rights Ireland* (case C-293/12) and *Seitlinger* (C-594/12), a new judgment delivered by the Court of Justice in Grand Chamber on the 13 May 2012 in the *Google Spain* case[1] confirms the judges' determination to fully ensure their role as guardian of fundamental rights. In 2014, the Court of Justice of the European Union established a "*right to be forgotten*" based on the provisions of Articles 12 under a and 14, paragraph 1, under b) of Directive 95/46 of 24 October 1995. It allows a natural person to obtain the deletion of the list of results, displayed following a request made in his name in a search engine, links pointing to web pages containing information about him.

The ruling of the Court of Justice of the European Union in the case of *Google Spain* is a pioneering decision, as it recognises the right of the data subject to delete personal data concerning him and which are included in the results lists of search engines on the Internet after a search. Of course, in this case, it is a limited recognition of the right to digital oblivion, as it concerns the search for information published on websites based on the name of a person and the recipients are search engines, not content providers (e.g., owners' websites), where the relevant information is published.

The direct consequence of this case law is that search engines must *filter* the results of searches they display when, at the request of a person, the question of the protection of his privacy is raised. This does not mean, of course, that information society service intermediaries will be censored for content posted on the Internet, as they are not the ones who publish the information themselves, but simply make it easier for Internet users to search. As a result, search engine service providers can no longer ignore the requests of people affected by the services they provide and, in particular, the ability provided by a search based on a person's name to obtain their full profile and/or negative information, for which that person has a legitimate interest in being forgotten. Of course, the decision leaves some gaps, such as the issue of the conflict between the right to be forgotten and freedom of expression, which is not adequately investigated. The directive having been repealed by the GDPR of April 27, 2016, recognizes now this right througouht its article 17, which specifically governs the "*right to be forgotten*". Following a recurrent pattern in EU law, the CJEU's rights-oriented approach has now been codified in article 16 TFEU, "*which provides an express legal basis for the EU to protect the fundamental right to data protection*"[2].

In a second judgment,[3] it defined the geographical scope of the "*right to be forgotten*". This time, the litigation opposed Google LLC, successor in law to Google Inc, to the French National Commission of Computing and Freedoms (Commission nationale de l'informatique et des libertés – CNIL). Google refused to

[1] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317

[2] C. McKay, 'Diminishing Sovereignty: How European Privacy Law Became International Norm', (2013) 2 *Santa Clara Journal of International Law* 11

[3] Case C-507/17, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772

follow up on a formal notice from the CNIL to apply the requested de-indexing to all domain name extensions of its search engine. The company confined itself to removing the links in question from the results displayed from the European versions of this engine. The French Council of State stated proceedings and questioned the Court of Justice on the interpretation of the provisions of Directive 95/46.

As a preliminary point, the judges, recalling the *Google Spain* case law, declared the European law applicable to the dispute. Indeed, the activities of Google in France – commercial and advertising – are inextricably linked to the processing of personal data carried out for the purposes of the operation of the search engine. In addition, given the existence of gateways between its different national versions, this engine must be regarded as carrying out a single processing which is carried out within the framework of the establishment located on French territory. Such a situation falls within the territorial scope of Article 4 (1) (a) of the Directive 95/46 and Article 3 (1) of the Regulation 2016/679.

The Court then considers that there is no obligation for the operator under Union law to dereference on all versions of its search engine.[1] It notes that the wording adopted by the legislator, for both the directive and the GDPR, does not go beyond the territory of the Member States. Moreover, while the regulation gives the supervisory authorities the means to cooperate to reach a common decision, it "*does not currently provide for such cooperation instruments and mechanisms as regards the scope of a de-listing outside the EU*"[2].

The judges qualify this position by adding that while the European legislator does not impose a 'global' de-listing, it does not prohibit it either. Thus, in their words,

> "*a supervisory authority or a judicial authority of a Member State remains competent to carry out, in the light of national standards for the protection of fundamental rights (...) a balance between, on the one hand, the data subject's right to respect for his private life and to the protection of personal data concerning him and, on the other, the right to freedom of information.' At the end of this review, it could 'order, where appropriate, the operator of the search engine to de-list all the versions of said engine*"[3].

In the context of data transfers with third countries' data, those countries are incentivised "*to adopt EU-level data protection standards by adequacy decisions and data protection standards in bilateral agreements*"[4]. The EU only categorically allows data transfers to a third country if an *adequate level of protection* is ensured. An adequacy decision exempts then "*the data controllers or processors established in or processing personal data*

[1] Case C-507/17, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772, para 64

[2] Case C-507/17, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:772, para 59 to 63

[3] *Ibid*, para 72

[4] Interview 9

belonging to data subjects in the EU from referring to any specific authorisation for data transfers"[1]. The CJEU's decision in the *Schrems* case heightened the standards for adequacy decisions by establishing that third countries need a level of protection which is "*essentially equivalent*" to that in the EU.[2] Again, these heightened standards are now codified in the GDPR.[3]

On July 16th, 2020, the CJEU invalidated the European Commission's adequacy decision, *Privacy Shield*, concerning the transfer of data between the EU and the US (case *Schrems II*).[4] The main reasons of the invalidation was:

> "*[a] that the requirements of U.S. domestic law, and in particular certain programmes enabling access by U.S. public authorities to personal data transferred from EU to the U.S. for national security purposes, result in limitation on the protection of personal data which are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, and [b]]that this legislation does not grant data subjects actionable rights before the courts against the US authorities. Additionally, [c] the Court underlines that certain surveillance programmes enabling access by US public authorities to personal data transferred from the EU to the US for national security purposes do not provide for any limitations on the power conferred on the U.S. authorities, or the existence of guaranties for potentially targeted non-US persons*".

Following this outcome, the European Commission Vice President Jourová acknowledged the invalidation of the Privacy Shield and stated that, "*transatlantic data flows can continue, based on the broad toolbox for international transfers provided by the GDPR, for instance binding corporate rules or Standard Contractual Clauses*"[5]. Jourová furthermore stressed that the Commission is committed to ensuring that data flows are in line with the judgment of the CJEU, respect EU law, and guarantee the protection of fundamental rights and therefore offer a high level of protection for personal data. She outlined the three priorities of the Commission which include: "*(a) Guaranteeing the protection of personal data transferred across the Atlantic; (b) Working constructively with our American counterparts with the aim of ensuring safe transatlantic data flows; and (c) Working with the European Data Protection Board and national data protection authorities to ensure our international data transfer toolbox is fit for purpose*"[6]. The European Commission Vice President furthermore stressed, as she has already done on multiple occasions in the past, that "*the Commission has already been*

[1] Article 3, article 13(1)(f) and article 45(1) of the Regulation (EU) 2016/679

[2] Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650

[3] Article 45(1) of the Regulation (EU) 2016/679

[4] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, OJ C 249, 16.7.2018, p. 15–17

[5] European Commission, Opening remarks by Vice-President Jourová and Commissioner Reynders at the press point following the judgment in case C-311/18 Facebook Ireland and Schrems, 16 July 2020

[6] *Ibid*

working intensively to ensure that this toolbox is fit for purpose, including the modernisation of the Standard Contractual Clauses"[1].

On July 17th 2020, the European Data Protection Supervisor (hereafter EDPS) issued a statement[2], which "*states that the Court of Justice of the European Union, in its landmark Grand Chamber judgment of 16 July 2020, reaffirmed the importance of maintaining a high level of protection of personal data transferred from the European Union to third countries*". And stresses that, "*the EDPS will continue to strive, as a member of the European Data Protection Board (EDPB), to achieve the necessary coherent approach among the European supervisory authorities in the implementation of the EU framework for international transfers of personal data*". Most importantly, the EDPS also noted that "*European supervisory authorities will advise the Commission on any future adequacy decisions, in line with the interpretation of the GDPR provided by the Court*". And that it "*trusts that the United States will deploy all possible efforts and means to move towards a comprehensive data protection and privacy legal framework, which genuinely meets the requirements for adequate safeguards reaffirmed by the Court*".

On October 6 2020, the CJEU handed down Grand Chamber judgments[3] determining that the e-Privacy Directive (2002/58/EC)[4] prohibits EU's Member States from adopting any legislation with the aim of restricting the scope of its confidentiality requirements "*unless they comply with the general principles of EU law, particularly the principle of proportionality, as well as fundamental rights under the Charter of Fundamental Rights of the European Union*"[5]. While on 3 January 2021, the Advocate General (hereafter AG) of the CJEU issued an important opinion in the case of *Facebook Belgium v. Gegevensbeschermingsautoriteit*,[6] which affirms the importance of the Lead Supervisory Authority's (LSA) role as a primary investigator and enforcer of data protection law within the EU. Regarding the conflict occurance between the NIS Directive and the GDPR, the latter shall prevail. Consequently, the right to data protection provided by the GDPR constitutes a

[1] European Commission, Opening remarks by Vice-President Jourová and Commissioner Reynders at the press point following the judgment in case C-311/18 Facebook Ireland and Schrems, 16 July 2020

[2] European Data Protection Supervisor 'EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II")', 17 July 2020; See also T. Christakis, 'Schrems III"? First thoughts on the EDPB post-Schrems II recommendations on international data transfers, Part III,' *European Law Blog*, 17 November 2020; T. Christakis, 'Schrems III ? First thoughts on the EDPB post-Schrems II recommendations on international data transfers, Part II,' *European Law Blog*, 16 November 2020; T. Christakis, 'Schrems III? First thoughts on the EDPB post-Schrems II recommendations on international data transfers, Part I,' *European Law Blog*, 13 November 2020.

[3] Judgments in Case C-623/17, Privacy International, and in Joined Cases, C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others.

[4] European Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47

[5] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407

[6] Case C-645/19, *Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, Opinion of Advocate General BOBEK delivered on 13 January 2021, ECLI:EU:C:2021:5

horizontal legal obligation within the EU.[1] This finding is further strengthened if the nature of potentially conflicting legal instruments is taken into consideration.

The EU plays an important role, as in many domains, as a regulator and a lawmaker. Thus, it has made cybersecurity one of its main security priorities. Such prioritisation has been reflected not only at the level of new initiatives being proposed, but also in the idea that for the EU to be an effective cybersecurity actor it needs to be fully coherent. Even if it has considerably raised its interest and role in cyberspace over the past two decades, the EU cannot be considered a major cybersecurity actor yet. The EU approach remains highly fragmented across a variety of dimensions – internal versus external security and operators versus policy elites – as well as within each of these dimensions. To understand EU cybersecurity architecture, we will present bodies and authorities implicated in EU cybersecurity.

§3. EU's Agencies in The Cybersecurity Domain: Hardening EU's Cybersecurity Law with a 'Soft' Networked-Governance

The early twenty-first century has seen a proliferation of European agencies, commonly mentioned by scholars as *agencification*. These EU level agencies, "*contribute to technical and sectoral knowhow […and] is one way for the Commission to control the implementation of community regulation […] as well as securing expertise, credibility and visibility*"[2]. Many of these functional reasons are applicable to agencies, as well as agency precursors and even the Commission. These bodies, made up of representatives of national administrations and mainly entrusted with technical and scientific functions, have gained a significant role over the years in EU decision-making, despite the lack of a clear legislative framework concerning their functions. Thanks to this institutional flexibility, they have also been able to perform — sometimes only indirectly, often together with other EU institutions — almost every type of EU law enforcement: monitoring activities, collection of evidence, technical and scientific evaluations, infringements and, most importantly, sanctions.[3]

In the absence of an explicit provision, the EU's competence to set up subsidiary bodies was not entirely clear before the entry into force of the Lisbon Treaty. While today, there is still no clear clause empowering legislators to set up and mandate a European agency. Especially since Articles 290 and 291 TFEU, which empower the Commission to adopt delegated and implementing acts, do not foresee any role for the agencies in

[1] See in particular the Breyer decision (CJEU, Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, par. 63 and 64)

[2] See J. Trondal and L. Jeppesen, 'Images of Agency Governance in the European Union', (2008) *West European Politics* 31

[3] See T. Christensen and P. Lægreid, 'Regulatory Agencies—The Challenges of Balancing Agency Autonomy and Political Control', (2007) *Governance* 20

these decision-making processes. Despite some exceptions, such as the European Defence Agency (Articles 42 and 45 TEU), EU agencies suffer a very scant recognition in primary law.

As a result, the agencification process was developed in a *constitutional vacuum*, leaving the question of the legislator's ability to confer powers to agencies unclear. The Court of Justice had however the opportunity to express its opinion on the question in the landmark *Short Selling* judgment for the first time.[1] The Court confirmed that the powers of European agencies are governed by the rules arising from the two *Meroni*[2] and *Romano*[3] judgments; and legitimised the practice of delegating sanctioning powers to agencies. Consequently, there may exist in the EU legal order acts adopted by agencies, both addressed to individuals (like the imposition of fines) and having general application (thanks to the explicit mention in Art. 277 TFEU).

If the Court followed a formalist approach by only prohibiting agencies from adopting binding acts, it has left enough leeway for the legislator to continue the process of agencification. The lack of a specific normative framework in the treaties is certainly among the reasons behind the success of EU agencies: they have been replicated for more than 30 years, basically in every field of EU law – including cybersecurity –, also because the Member States have found and are still finding in EU agencies a great platform for cooperation, starting from an almost blank page, without empowering an existing (and potentially hostile) institution,[4] deciding its functions, composition and powers on a case-by-case basis.

Circumventing the principle of subsidiarity, EU agencies create a common platform of shared governance, endowed with an autonomous legal personality that disrupts the classic bilateral relationship between the EU and its Member States.[5] The extent of the twist between these two levels may well vary from sector to sector: it ranges from mere coordination offered by the agency to national authorities, to an explicit substitution of the latter by the former for adopting binding legal acts vis-à-vis specific addressees or categories of individuals. EU agencies can be seen both as a boost for enhancing EU sanctioning powers, or as bodies that slow it down. Indeed, they can both foster a common legal and administrative culture of supervision, or they can push the political debate towards solutions that can be very different from sanctioning. Following Jacopo Alberti's

[1] Case C-270/12, *United Kingdom v. Parliament and Council (Short selling)*, OJ C 85, 22.3.2014, p. 4–4

[2] Case 9-56, Judgment of the Court of 13 June 1958. Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community. English special edition 1957-1958 00133. ECLI identifier: ECLI:EU:C:1958:7

[3] Case 98/80, Judgment of the Court (First Chamber) of 14 May 1981. Giuseppe Romano v Institut national d'assurance maladie-invalidité. Reference for a preliminary ruling: Tribunal du travail de Bruxelles - Belgium. Social security - Applicable exchange rate. European Court Reports 1981 -01241. ECLI identifier: ECLI:EU:C:1981:104

[4] See M. Shapiro, 'Independent agencies', in P. Craig and G. De Burca (eds), *The evolution of EU Law* (Oxford University Press, 2011)

[5] See D. Geradin, and N. Petit, 'The development of agencies at EU and national levels: conceptual analysis and proposals for reform', (2005) 1 *Yearbook of European Law* 23

analytical taxonomy of EU agencies' direct and indirect sanctioning powers,[1] EU agencies' contribution to EU and national sanctioning can be sorted out according to the following categories, which are lined up from the weakest form of involvement to the strongest: Collection and spread of information and best practices among national administrations; monitoring activities and inspections that might bring to sanction issued by national or EU authorities; the power of proposing the Commission to impose fees; assistance in the enforcement of EU law; and the power to impose fees.

The following developments will highlight the possible transition (or not) of a *soft* governance to a hard governance, by presenting and assessing the agencies' ability to adopt binding acts and to issue direct and indirect sanctions. From the 37 agencies three are running within the field of cyber-security: the European Union Agency for Network Information Security, the European Defence Agency, the European Cybercrime Centre (EC3) unit, established under the auspices of Europol, on which another one will be added very soon, the upcoming European Cybersecurity Industrial, Technology and Research Competence Centre. To ease the assessment of an eventual governance hardening, these four agencies will be presented according to their source of establishment, primary (**A**) or secondary (**B**) law.

A. EU Agencies Recognised by the Treaties of the EU: With A Soft Enforcement Mechanism

C ybersecurity-related agencies in the area of law enforcement and defence are recognised by the Treaties of the EU. Articles 85 to 88 TFEU set Eurojust's (1) and Europol's (2) missions, while Articles 42 and 45 TEU stress the EDA's missions (3).

1. European Union Agency for Criminal Justice Cooperation – EUROJUST (85 and 86 TFEU)

On October 1999 in Tampere, the European Council decided on the setting up of EUROJUST, a unit composed of prosecutors, magistrates, or police officers of equivalent competence as a means to ease the optimal coordination of action for investigations and prosecutions covering the territory of more than one Member States. By the Council's Decision 2002/187/JHA,EUROJUST was set with a view to reinforcing the fight against serious crimes.

[1] See J. Alberti, 'New Actors on the Stage: The Emerging Role of EU Agencies in Exercising Sanctioning Powers', in S. Montaldo, F. Costamagna and A. Miglio (Eds.), *EU Law Enforcement The Evolution of Sanctioning Powers: The Evolution of Sanctioning Powers* (Routledge, 1st edn, 2021)

EUROJUST supports and strengthens coordination and cooperation between national investigating and prosecuting authorities (Article 85 TFEU). It assists prosecutors and other investigators from EU Member States in cases of serious crime where that crime affects two or more Member States, or requires prosecution on common bases, on the basis of operations conducted and information supplied by the Member States' authorities, by Europol, by the European Public Prosecutor's Office (EPPO) and by European Anti-Fraud Office (OLAF). Eurojust acts at the request of the competent authorities of Member States or on its own initiative. In some cases, Eurojust can act at the request of the European Commission or the European Public Prosecutor's Office.

Council Decision 2002/187/JHA was amended twice since its adoption. Firstly by the Decision 2003/659/JHA which aimed to align Eurojust with the budgetary and financial rules applicable to EU bodies and agencies; and secondly by Decision 2009/426/JHA, which aimed to equip Eurojust with the means to improve the fight against serious crime. Amending Decision 2009/426/JHA set the term of office at a minimum of 4 years which may be renewed. The EU country decides on the nature of the judicial powers given to its national member. However, national members must have at least certain ordinary powers, as well as other powers to be exercised in agreement with the competent national authority or in urgent cases, as defined in the decision. But most important, it introduced the right for Eurojust's College to issue non-binding opinions in cases where: 2 or more national members are unable to resolve conflicts of jurisdiction; competent authorities report recurrent refusals for, or other difficulties relating to, judicial cooperation.

On November 14th 2018, regulation (EU) 2018/1727 of the European Parliament and of the Council was adopted on EUROJUST, replacing and repeaing Council Decision 2002/187/JHA[1]. The Regulation has established Eurojust in its new structure, clarifying that the Eurojust agency replaces and succeeds Eurojust as established by Decision 2002/187/JHA (Article 1 of the Eurojust Regulation).

The Eurojust Regulation "*establishes a new governance system, clarifies the relationship between Eurojust and the EPPO, prescribes a new data protection regime, adopts new rules for Eurojust's external relations and strengthens the role of the European and national parliaments in the democratic oversight of Eurojust's activities*"[2]. According to Article 86(1) TFEU the EPPO must be established from Eurojust. That language seems to leave it open whether Eurojust should be converted into the EPPO or whether both bodies should coexist; however, the latter interpretation is the more reasonable, given that the EPPO has a more limited material scope.

[1] European Parliament and Council of the European Union, (2018). Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, PE/37/2018/REV/1, OJ L 295, 21.11.2018, p. 138–183

[2] European Parliament, 'Annual report 2019 – Relations between the European Parliament and EU national Parliaments', (2020), https://www.europarl.europa.eu/cmsdata/226162/L020206_-_DG_PRES_-_BROCH_A4_-_RelNatParl_annual_report_2019_EN_WEB.pdf

According to Article 4 of regulation (EU) 2018/1727 on operational functions of Eurojust, the latter may issue a written opinion "*where two or more Member States cannot agree as to which of them should undertake an investigation or prosecution*", and "*send the opinion to the Member States concerned immediately*". The written opinions of Eurojust are not binding on Member States but should be responded without undue delay (recital 14). However, "*The competent authorities of Member States may refuse to comply with such requests or to follow the written opinion if doing so would harm essential national security interests, would jeopardise the success of an ongoing investigation or would jeopardise the safety of an individual*" (Article 4 of the Regulation 2018/1727).

Therefore, Eurojust exercises its competence either through its National Members or its acts as the College, whereas we need to point out that Eurojust is not competent to adopt decisions binding for Member States, but it is a *mere* coordinating and recommending authority in the area of international cooperation in criminal matters if the competent authorities of Member States do not accept Eurojust's recommendation. There is thus one sanction only, namely, to release the fact that the Member State refused a request in the Annual Report (form of naming and shaming).

Eurojust may also issue a non-binding opinion in case of recurring refusals or difficulties with execution of requests and decisions concerning judicial cooperation. The increase of the powers of Eurojust to decide in a binding way on which national jurisdiction should be investigated and prosecuted and which should withdraw from the investigation, would have been appreciated while considering a form of control of Eurojust's decisions.

In a strategic seminar, entitled "*Conflicts of Jurisdiction, Transfer of Proceedings and Ne Bis in Idem: Successes, Shortcomings and Solutions*", which was jointly organised by Eurojust and the Latvian Presidency of the EU and took place on 4 June 2015, Katalin Ligeti (Professor, University of Luxembourg) presented a critical assessment of the existing EU legal framework on conflicts of jurisdiction from an academic perspective. She underlined that there is a collection of soft law instruments with modest ambitions and modest outcomes, but no legal instrument setting up a binding mechanism to allocate cases or trigger the jurisdiction of Member States in cases of negative conflict.

Highlighting this issue of conflicts of jurisdiction in the context of cybercrimes is very important because of the phenomena of loss of data and loss of location. In situations such as cloud computing or the dark web, it is often unclear which country has jurisdiction and what legal framework regulates the collection of evidence or the use of special investigative powers. The complexity of the organised criminal groups (OCGs) that are the subject of cybercrime investigations is a relatively common feature in Eurojust's casework. In such context prosecuting authorities struggle, again, with conflicts of jurisdiction and/or ne bis in idem situations, as the same suspect(s)/victim(s) may be the subject of various proceedings in different jurisdictions.

Recognising this power thus elevates Eurojust from being a mere cooperation agency to being able to directly enforce the powers conferred upon it. This significantly strengthens the importance given to the agency, which should be recognised as having the same value as other EU bodies equipped with explicit/de jure powers. The

softness of Eurojust's written opinions and its enforcement mechanism incites me to categorise Eurojust acts as soft law.

2. The European Union Agency for Law Enforcement Cooperation – EUROPOL (88 TFEU)

EUROPOL is the European law enforcement agency whose main aim is to achieve a safer Europe for the benefit of all EU citizens. Founded as an intergovernmental organization in 1999, it has been an EU agency since 2010, making it ultimately accountable to the JHA formation of the Council and to the European Parliament.

If within ten years Europol has become the main European actor in the field of internal security, EUROPOL has gradually increased its ability to shape the European Union's external environment.[1] It influences the EU's foreign policy is via the signature of cooperation agreements with third countries. Since the 2008 agreement establishing a Co-Operation Mechanisms for the Exchange of Personal Data Between Europol and Civilian ESDP Missions increased EUROPOL's capacity to guide the EU's civilian crisis management efforts.[2] At last, EUROPOL is also active in security sector reform (SSR) activities, mainly throughout cooperation agreements with the Western Balkans.

Europol is not a European police force, and it does not have executive powers, but it works closely with the law enforcement agencies of the 27 Member States and with other states outside the EU, such as Australia, Canada, the US and Norway. According to article 88 TFEU, Europol's mission is "*to support and strengthen actions by the Member States' police authorities and other law enforcement services and their cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy*". In order to do so, the service uses its unique information capabilities and the expertise of its staff to identify the most dangerous criminal and terrorist networks in Europe.

Based on a feasibility study commissioned by the European Commission and carried out by RAND Europe,[3] Europol established the European Cyber Crime Centre (hereafter EC3) in 2013. To ensure cybercrime is approached from a holistic perspective, EC3 comprises three different units: Operations, Strategy and Forensic Expertise. EC3 focuses on the following key axes of cybercrime: cybercrime perpetrated by organised crime

[1] See G. Mounier, 'Europol: A New Player in the EU External Policy Field?' 4 *Perspectives on European Politics and Society*, 10

[2] Council of the European Union. Common Considerations by the General Secretariat of the Council (GSC) and Europol in View of the Possible Establishment of Co-Operation Mechanisms for the Exchange of Personal Data Between Europol and Civilian ESDP Missions 31 October 2008, 15063/08

[3] RAND Europe is an independent not-for-profit research institute whose mission is to help improve policy and decision making through research and analysis.

groups, in particular crimes that generate enormous profits such as online fraud; cybercrime that causes serious harm to their victims, such as cyberbullying, and cybercrime affecting key infrastructure and information systems in the Union.

The EC3 should also be able to act, responding to requests from Member States, and address the emergence of new, more sophisticated threats to the Union. The basic functions of EC3 are to serve as a European focal point for cybercrime information; to bring together European expertise in cybercrime to help Member States build capacity; to support Member States' investigations into cybercrime and to make the collective voice of European cybercrime investigators at the judicial and law enforcement level. When officially launched on January 11th 2013, the European Cybercrime Centre was not expected to be fully operational until 2015. The EC3 was tasked with assisting Member States in their efforts to dismantle and disrupt cybercrime networks and developing tools as well as providing training.

In recital 24 of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, it is stated that "*Member States should submit information on the modus operandi of the offenders to Europol and its European Cybercrime Centre for the purpose of conducting threat assessments and strategic analyses of cybercrime (...)*". Europol's missions and operational capacities cannot be therefore related to any sanctioning power, as its role is mainly restrained to the collection and spread of information and best practices among national administrations. The same also applies to EUROJUST for which recital 1 stresses that "*The objectives of this Directive are (...) to improve cooperation between competent authorities, including the police and other specialised law enforcement services of Member States, as well as the competent specialised Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA)*".

3. European Defence Agency – EDA (42 and 45 TEU)

EDA supports its 26 Member States in improving their defence capabilities through European cooperation. Through its actions towards the strengthening of the EU's position as a global actor via cooperation and capability development, EDA also contributes to Smart and Sustainable Growth by fostering innovation in the defence industry, promoting a competitive European Defence Equipment Market, strengthening the European Defence Technological and Industrial Base, and improving energy efficiency and renewable energy in the defence and security sector.

As a Council Agency, the EDA was set up by the Joint Action of the Council of Ministers on July 12th 2004, "*to support Member States and the Council in its efforts to improve European defence capabilities in crisis management and maintain European Security and Defence Policy as defined and further develop it in the future*". Thus, the EDA has become the hub for European defence cooperation. These four main functions shape

the chain for development capacity, from the definition of research and equipment cooperation to industrial procurement. This integrated approach contributes to the coherent development of capabilities, where demand and supply are well integrated to save time and cost for Member States. More partnerships then provide opportunities for the European defence industry. The Agency also supports the Ministries of Defence in their interactions with other European institutions and keeps them informed of wider EU policies with implications for defence. EDA acts as a catalyst, promotes partnerships, launches new initiatives, and introduces solutions to improve defence capabilities. It is the place where Member States that wish to develop competencies in cooperation do so. It is also a key mediator in the development of the capabilities needed to support the European Union's CSDP.

On July 12th 2011 the Council adopted a decision defining the statute, seat and operational rules of the European Defence Agency and repealing Joint Action 2004/551/CFS.[1] In May 2017, Member States agreed to further reinforce the agency's mission as:

> "*the main intergovernmental prioritisation instrument at EU level in support of defence capability development; the preferred cooperation forum and management support structure at EU level for participating Member States to engage in technology and capability development activities; the interface coordinating military views in wider EU policies to the benefit of the defence community and a central operator with regard to EU-funded defence related activities.*"[2]

The Agency works closely with Member States for developing their national capabilities in the field of cyber defence by agreeing on a strategic context case that outlines the capability landscape, and by detailing the programme to be conducted by the Cyber Defence Project Team and the Ad Hoc Working Group (AHWG) for Cyber Defence Research and Technology; as well as by supporting the definition of PESCO projects. PESCO is a generic term for a specific kind of enhanced cooperation defined in the TEU. Article 42(6) TEU allows for the creation of a permanent structured cooperation (PESCO) between willing Member States "*whose military capabilities fulfil higher criteria, and which have made more binding commitments to one another in this area with a view to the most demanding missions*". In December 2017, this paragraph was translated into Council Decision (CFSP) 2017/2315 establishing PESCO.[3] This has not only established the first list of projects but added the "*more binding commitments*" to be undertaken by each PESCO participating state.

[1] Council Decision 2011/411/CFSP of 12 July 2011 defining the statute, seat and operational rules of the European Defence Agency and repealing Joint Action 2004/551/CFSP, 13.07.2011, L 183/16.

[2] EDA, 'Long Term Review Of The Agency – Conclusions And Recommendations', 18 May 2017. Available at https://eda.europa.eu/docs/default-source/documents/ltr-conclusions-and-recommendations.pdf (accessed on January 22nd, 2022)

[3] Council Decision (CFSP) 2017/2315 of 11 December 2017, establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States, L 331/57

The decision being legally binding in nature, states are required to meet certain objectives.[1] These 20 commitments are subdivided into five categories concerning: "*defence investment expenditure; harmonisation, capability specialisation and training/logistics cooperation; force availability, interoperability, flexibility and deployability; Capability Development Mechanism implementation; and equipment programme development through the EDA*"[2]. In the early assessments of PESCO, much attention was however focused on the list of the 46 specific projects, covering training facilities, land formation systems, maritime and air systems, and cyber systems, and enabling joint multiple services or space projects.[3] Equally important, however, are the less discussed binding common commitments to Council conclusions listed in the Annex. In accordance with PESCO's Terms of Reference, commitments will be legally binding, and decisions will be made on the basis of Qualified Majority Voting (hereafter QMV). No instruments for sanctioning non-abiding parties have been indicated, however, apart from the risk of being suspended from a project. After more than 20 years of CSDP, national interests are still prevailing amon Member States in their defence planning, which resulted to a very little discipline in meeting the commitments that they undertook. In the CSDP, Member States take decisions by unanimity with a limited culture of compliance.

B. EU Agencies Established by Secondary Law

The legal basis for European Union agencies is not necessarily contained in the Treaties, nor is there any provision which explicitly governs the capacity of the Commission to delegate powers to them.[4] As a matter of fact, these institutions are created by secondary law (namely Regulations) and their powers are delineated by the case law of the CJEU. In particular, the *Meroni* judgement[5], stated that EU actors can only delegate clearly defined executive powers to the agencies, to the exclusion of discretionary ones. However, more and more agencies are involved in the drafting of various kinds of soft law (such as recommendations, guidelines or opinions) which is general in nature. Since soft law is not formally binding and, thus, does not create any rights or obligations, it seems to escape the limitations established by the *Meroni* judgement. Yet, the importance of soft law must not be underestimated, as it may have considerable practical effects. An important development

[1] See S. Blockmans, 'The EU's modular approach to defence integration: An inclusive, ambitious and legally binding PESCO?', (2018) *Common Market Law Review* 55

[2] S. Blockmans and D. Macchiarini Crosson, 'Differentiated integration within PESCO – clusters and convergence in EU defence', (2019), 4 *CEPS Research Report* 2019

[3] Council of European Union, (2019), Permanent Structured Cooperation (PESCO) Projects: Overview, Available at https://www.consilium.europa.eu/media/41333/pesco-projects-12-nov-2019.pdf (accessed on August 5th, 2021)

[4] See Peter Alexiadis and Caio Mario Da Silva Pereira Neto, 'Competing Architectures For Regulatory And Competition Law Governance,' European University Institute, Research Report, June 2019.

[5] Case 9-56, Judgment of the Court of 13 June 1958. Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community. English special edition 1957-1958 00133. ECLI identifier: ECLI:EU:C:1958:7

that should be mentioned is the recent ESMA-short selling case,[1] in which the CJEU ruled that it is possible to delegate the power to adopt acts of general application to EU agencies if those acts are amenable to judicial review. In the field of cybersecurity two agencies established by secondary law can be cited, among which the ENISA is the most notable.

1. European Network and Information Security Agency – ENISA (Regulation (EU) 2019/881)

Founded by Regulation (EC) No 460/2004[2] of the European Parliament and of the Council on March 10th 2004, ENISA became operational in 2005. Through its work in the field of cybersecurity, ENISA contributes to smart growth via its actions towards an efficient functioning of the DSM. It strives to anticipate and support the EU in facing emerging network and information security challenges; to promote network and information security as an EU policy priority; to support the EU in maintaining state-of-the art network and information security capacities, and to foster the emerging European network and information security community. Through its actions in the field of data protection, ENISA also contributes to the area of justice and to citizens' fundamental rights.

The Agency works closely together with Member States and the private sector to deliver advice and solutions as well as improving their capabilities. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS and assists Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis. However, soon after the adoption of the regulation establishing the ENISA, the UK questioned the use of Article 114 TFEU as the legal basis for the Regulation.[3] The UK argued that "*the purpose of Article 114 TFEU was the approximation of laws and that the Regulation in fact took effect on the institutional level*"[4]. Simply because a measure may benefit the functioning of the internal market does not mean that it thereby constitutes harmonisation within the meaning of Article 114 TFEU. The UK also submitted that none of the provisions in the ENISA Regulation, even indirectly or in a minor way, approximates national legislation.

In its judgement, the Court said that "*Article 114 TFEU could be used to establish an Union body responsible for contributing to the implementation of a process of harmonisation where, for example, the Union body provided services to national authorities and/or operators which affected the homogenous implementation of*

[1] Case C-270/12, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, ECLI:EU:C:2014:18

[2] OJ L 077, 13.03.2004, p. 1–11

[3] Case C-217/04, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, ECLI:EU:C:2006:279

[4] See M. Chamon, *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration* (Oxford University Press, 2016), 12

harmonising instruments and was likely to facilitate their application"[1]. The Court added that the tasks conferred on such a body did, however, have to be closely linked to the subject matter of the harmonisation legislation.[2] Therefore, ENISA could be established on the basis of Article 114 TFEU since its aim was to assist the Commission and Member States with meeting the requirements of network and information security, as part of a wider package of measures,[3] thereby ensuring the smooth functioning of electronic communications services.

In accordance with Regulation (EC) No 460/2004, the Agency aims to enhance the capacity of the Community, the Member States and, as a result, the business community to prevent, and respond to NIS security problems; to assist and advise the Commission and Member States on matters relating to network and information security, which fall within its remit; to develop a high level of specialised knowledge, starting from national and Community efforts and finally; to assist the Commission, when requested, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

To achieve its objectives, the Agency, in accordance with Article 3 of the Regulation, is endowed with the following tasks:

"*(a) the collection of relevant information for the analysis of existing, future, and immediate risks, and in particular at European level, of risks that could affect the robustness and availability of electronic communications networks, as well as the authenticity, integrity and confidentiality of their information that is accessible or transmitted through these networks, and transmission of the results of the analysis to the Member States and the Commission*

(b) advising and, at the request of the European Parliament, European bodies or competent national bodies designated by Member States, within the framework of its objectives

(c) enhancing cooperation between the various actors involved in the field of network and information security, including regular consultations with industry, universities, and other interested parties, and by establishing contact networks for Community bodies, stakeholders public sector designated by Member States, private sector bodies and consumer organisations

(d) facilitating cooperation between the Commission and Member States in developing common methodologies for the prevention and response to network and information security issues

---

[1] Case C-217/04, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, ECLI:EU:C:2006:279, para 44-45

[2] *Ibid*, para 45

[3] Case C-217/04, *United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union*, ECLI:EU:C:2006:279, para 60

(e) contributing to raising awareness and availability of timely, objective and centralised information on network and information security issues for all users, by promoting exchanges of existing best practice, including user alerting methods, as well as; the synergy between public and private initiatives

(f) assisting the Commission and Member States in conducting their dialogue with the industry to address security problems with hardware and software products

(g) monitoring the evolution of standards for network and information security products and services

(h) advising the Commission on research in the field of network and information security, as well as on the effective use of risk prevention technologies

(i) promoting risk assessment activities, interoperable risk management solutions and studies on prevention management solutions within public and private organisations

(j) contributing to the Community's efforts to cooperate with third countries and, where appropriate, with international organisations, with a view to promoting a common global approach to network and information security, thereby contributing to an understanding of network and information security

(k) independent expression of its conclusions, orientations and advice on matters relating to its scope and objectives".

ENISA's priorities now include critical information infrastructure protection and cyber capacity-building activities.[1] ENISA's Management Board defines the Agency's general orientation. It is composed of representatives of Member States and the Commission. The ENISA has also an Executive Board, tasked with preparing decisions for adoption by the Management Board on administrative and budgetary matters. An Executive Director, appointed by the Management Board, manages the Agency, assisted by two heads of department[2]. Thirty-three members appointed from all over Europe compose the ENISA Permanent Stakeholders Group, which is an advisory body to the Executive Director on matters such as the development of the Agency's work program. Every year, ENISA produces reports, position papers, risk assessments, or briefings covering different areas, which are comprehensive documents outlining key information and provide practical recommendations.

Thus, ENISA's mission was principally at launch to provide advice and assistance and enhance cooperation between EU bodies and Member States in the field of cybersecurity.[3] Based inter alia on its findings and on the consultation of various stakeholders, the Commission concluded that ENISA's mandate was not sufficient and

[1] Interview 5

[2] The Core Operations Department and the Resources Department

[3] European Commission Final report on the Evaluation of the European Union Agency for Network a Information Security (ENISA), 2017

adopted the Cybersecurity Act,[1] which provides ENISA with a strengthened and permanent mandate since June 27th 2019.[2] From now on, ENISA will act as the EU's cybersecurity expert, providing advice and expertise to Member States, private stakeholders, European institutions and policymakers,[3] and helping Member States and national authorities to prevent and improve responsiveness to cyber threats and incidents. To accomplish its tasks with efficiency, the financial and human resources allocated to ENISA have also been increased.

The Cybersecurity Act is enhancing the capacity of ENISA for collecting and spreading information and best practices among national administrations,[4] as well as monitoring the implementation of the Union's policy and law regarding cybersecurity, in particular in relation to Directive (EU) 2016/1148. Nevertheless, there is no direct link, legally speaking, to any function of carrying out inspections that might lead to further sanctions issued by other bodies, at either EU or national level; nor a link to any power to propose to the Commission to impose fees. However, the ENISA's capacity for assisting "*the Commission by means of advice, opinions and analyses, (...) to enhance the relevance of Union policies and laws with a cybersecurity dimension and to enable consistency in the implementation of those policies and laws at national level*"[5], can contribute for the activation of the Commission's infringement powers.

2. The European Union Agency for Law Enforcement Training – CEPOL (Regulation (EU) 2015/2219)

CEPOL is an agency of the EU dedicated to developing, implementing, and coordinating training for law enforcement officials. CEPOL was initially founded by Council Decision 200/820/JHA of 22nd December 2000[6] as a body financed directly by Member States of the European Union. But it was upgraded in 2005 to a Union's agency, under the denomination of European Police College (CEPOL).[7] The decision was amended by the European Parliament and the Council on 15 May 2014 establishing that the seat of CEPOL shall be Budapest, Hungary. On November 25th 2015, the Council and the European Parliament adopted Regulation (EU) 2015/2219, establishing the European Union Agency for Law Enforcement Training (CEPOL),[8] which replaced and repealed Council Decision 2005/681/JHA.

[1] OJ L 151, 7.6.2019, p. 15–69

[2] Recital 16 of the Regulation (EU) 2019/881

[3] Article 3 of the Regulation (EU) 2019/881

[4] Interview 5

[5] Recital 22 of the Regulation (EU) 2019/881

[6] Council Decision of 22 December 2000 establishing a European Police College (CEPOL), OJ L 336, 30.12.2000, p. 1–3

[7] OJ L 256, 1.10.2005, p. 63–70

[8] OJ L 319, 4.12.2015, p. 1–20

CEPOL's core business is to provide training courses for senior police officers of the EU Member States, with a focus on spreading information and knowledge and fostering cross-border contacts. CEPOL has identified cybercrime as its key priority for the upcoming years. Developing the necessary knowledge and expertise in law enforcement authorities across Europe is thus important for addressing the evolving challenge of cybercrime. By doing so, CEPOL inaugurated the *CEPOL Cybercrime Academy* in June 2019,[1] which was counting a total of 8,271 enrolments on April 17th 2020, in cyber training activities.[2]

CEPOL has no sanctioning powers and Management Board Decisions are not binding on Member States. Monitoring tasks, such as its Annual Report or Consolidated Annual Activity Report, are principally aimed at overviewing the most relevant developments and achievements of the agency in a year or procuring a comprehensive account of the activities carried out by CEPOL in implementing its mandate and Annual Work Programme.

§4. Third-Party Institutions: Developing External Expertise.

Four third-party institutions are working closely with the EU's institutions and agencies providing them with a high-level of expertise on various policy fields: the European Centre of Excellence for Countering Hybrid Threats (A); the European Security and Defence College (B); EU Institute for Security Studies (C); the European Cybercrime Training and Education Group (D); and European Cybersecurity Centre and Network (E).

A. European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)

In September 2017, the European Centre of Excellence for Countering Hybrid Threats (hereafter Hybrid CoE) was created in Helsinki, Finland. The Centre's aim is mainly to enable building participants' capabilities and to enhance EU-NATO cooperation in countering hybrid threats. The tasks of the new centre of excellence include "*promoting security debates and improving the EU Member States' civil-military capabilities; enhancing resilience against forces that try to polarise societies in ways that undermine democracy and democratic countries' decision-making, improving preparedness for attacks that seek to weaken different alliances and states; finding better ways to build solidarity among nations and share best practices and expertise; as well as seeking to improve coordinated responses*"[3].

[1] Available at https://www.cepol.europa.eu/media/news/cepol-cybercrime-academy-inaugurated (accessed on August 6th, 2021)

[2] Available at https://www.cepol.europa.eu/media/news/cepol-cybercrime-academy-over-8200-enrolments-cyber-training-activities-inception (accessed on August 6th, 2021)

[3] Retrieved from https://www.hybridcoe.fi/

B. The European Security and Defence College

The European Security and Defence College, led by the 27 EU Member States, is a network college consisting of 140 partners within and outside the European Union. During a special meeting on 6 February 2018, the 28 Member States decided to create a Cyber Exercise, Training, Exercise and Evaluation (hereafter ETEE). The Cyber ETEE platform aims :

> "*To address cyber security and defence training among the civilian and military personnel, including the CSDP requirements for all CSDP training levels as identified by the EU Military and Civilian Training Groups, and upscaling the training opportunities for Member States. (…) At a later stage and depending on the further development of such a concept, the Cyber ETEE platform could advance ETEE opportunities for wider cyber defence workforce (the so-called Cyber Reserve).*"[1]

C. EU Institute for Security Studies (EUISS)

The European Union Institute for Security Studies (hereafter EUISS) is an EU's agency dealing with the analysis of foreign, security and defence policy issues. Its core mission is to assist the EU and its Member States in the integration of the CFSP, including the CSDP as well as other external action of the Union. In the area of cybersecurity, the EUISS established the EU Cyber Direct project with two other partners in support of EU cyber diplomacy and cyber resilience. The Institute's three latest publications on cybersecurity include "*Building capacities for cyber defence*", "*Hybrid threats and the EU - State of play and future progress*" and "*The cybridisation of EU defence*".[2]

D. European Cybercrime Training and Education Group (ECTEG)

The European Cybercrime Training and Education Group (hereafter ECTEG) is composed of the EU's and European Economic Area Member States' law enforcement agencies, international bodies, academia, private industry, and experts. Since 2016, the ECTEG officially became an international non-profit association. Funded

[1] Document ESDC 2018/013 Rev 1 - Cyber ETEE Platform.

[2] All publications can be downloaded via the EU ISS homepage www.iss.europa.eu.

by the European Commission and working in close cooperation with Europol's EC3 and CEPOL, both members of the advisory group, the ECTEG's activities aim to "*support international activities to harmonise cybercrime training across international borders; share knowledge and expertise and find training solutions; promote standardisation of methods and procedures for training programmes and cooperation with other international organisations; collaborate with academic partners to establish recognised academic qualifications in the field of cybercrime and work with universities that have already created such awards, making them available across international borders; collaborate with industry partners to establish frameworks whereby their existing and future efforts to support law enforcement by the delivery of training are harmonised into an effective programme that makes the best use of available resources; provide training and education material and reference trainers to international partners, supporting their efforts to train law enforcement on cybercrime issues globally*"[1].

E. European Cybersecurity Centre and Network

In the view of a steady proliferation of *Union bodies*, the proposal for a European Cybersecurity Centre once more raises the question to such agencification. Recognising the significance of cybersecurity in an increasingly inter-connected society, in September 2018 the European Commission proposed to establish on the basis of Articles 173 (3) and 188 TFEU respectively, a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Coordination Centres,[2] with the aim to improve and strengthen the Union's competitiveness, as well as the autonomy of its cybersecurity value chain. The European Centre's main objectives are to strengthen the security of European industries against cyberattacks, to support public-private partnerships (PPPs) in cybersecurity research, and to promote Europe's research projects with funding research and Digital Europe. Through the Horizon Europe and Digital Europe programs, 2.8 billion euros and 1.9 billion euros will be allocated for cybersecurity, respectively.

The European Centre will be one of the three main pillars of the new European system of technology and innovation for cybersecurity. In particular, the European Centre will have the task of a) managing the funds provided for cybersecurity under the Horizon Europe and Digital Europe programs, b) coordinating the National Coordination Centres Network, with the aim of building national skills and connectivity. with existing initiatives, c) support for joint EU, EU and industry investment co-investment in cybersecurity research, d) support for the development of products and solutions in the field of cybersecurity, and e) European Community Competence cybersecurity coordination to promote technological agenda in the cybersecurity sector. The National Coordination Centres will be funding recipients and will be able to distribute financial support to

[1] Retrieved from https://www.ecteg.eu/

[2] European Commission Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, 12 September 2018, COM(2018) 630 final

national entities (e.g., research institutes, universities, etc.), while the European Community Security and Quality Assurance Community will be made up of public sector representatives and private individualsin the field of cybersecurity research.

The European Centre will fund actions related to: (a) the Network of National Coordination Centres and the European Community Cybersecurity Capacity Community, such as funding for the National Coordination Centres from the Digital Europe program in order to financially support groups in their operation, providing secretarial Community work (e.g. organising meetings), mapping the factors involved in cybersecurity research; (b) to research, development and the press poetry in the field of cybersecurity; (c) joint investments by the EU and the EU (if they wish) in new high-tech infrastructure and capabilities; (d) investments at national or regional level in infrastructure or capabilities with a smaller percentage of EU funding; (e) strengthening the development and introduction of cybersecurity solutions and services; (f) actions connecting SMEs with the demand, as well as aligning them with EU investment financing, with the ultimate goal of avoiding the movement or acquisition of European companies in the field of cybersecurity; (g) development of cybersecurity skills by creating a European framework for training programs for cybersecurity designing. The proposal is however characterised by legal uncertainty. This concerns firstly the uncertain status of the Centre within the EU's institutional architecture. Second, and related to this, is the unclear relationship between the Centre and the ENISA. The political debate on the seat allocation of the Centre, which is normally reserved up to decentralised agencies, furthermore blured sits legal nature.

Following a textual interpretation of Articles 188 and 187 TFEU, the Centre could be "*either as a joint undertaking or be established as another structure necessary for the efficient execution of Union research programs*". However, the Commission suggested that the Centre be established as an "*EU body set up under the Treaty*" charged with implementing funding in accordance with Article 70 of the Financial Regulation. This strategy may support the idea that the classification as a non-specified Union body would suffice under primary law, providing the EU legislature almost with a *carte blanche* regarding the establishment of unique legal structure.

The option to confer such tasks to ENISA was discarded on the basis of an apparent mismatch in objectives and governance structure, even if Article 11 of the ENISA founding regulation (EU) 2019/881 (Cybersecurity Act)[1] might have formed the stepping-stone for broadening the scope of ENISA's activities. However, to extend ENISA's attributions to the field of cyber defence industrial policy, the founding regulation (EU) 2019/881 of ENISA would also need to be amended to include Article 173 (3) TFEU as its legal basis. But this could raise certain challenges in this area, since the EDA is already present in everything related to defence, even cyberdefence.

[1] OJ L 151, 7.6.2019, p. 15–69

On March 13th and 20th 2019, two trialogues were held on the legislative proposal for the establishment of the European Centre, but no agreement was reached between participants. The main points of discordance were the issue of fund management by the European Centre and the governance of the European Centre.[1] At the time of this writing[2], the Croatian Presidency issued a revised mandate for negotiations with the European Parliament based on the results of the Horizontal Working Party on Cyber Issues working group meeting on 11 March 2020. The presidency is to draw up a 5th revised version of the bill and then submit the text to COREPER I for approval, whenever possible (delay due to coronary pandemic). As for the planning of the trialogue, there will be no resumption, but the trialogue will continue from the point where it was interrupted during the Romanian presidency. The Croatian presidency intends to start with a political trialogue and then to resolve most disagreements with the European Parliament at a technical level.

As seen from the above developments, the publication of the First European Union (EU) Cybersecurity Strategy in 2013 marked the formal establishment of *cybersecurity* as a new policy area in the EU. The developments highlighted the *hybridity* of the legal framework of the EU, which oscillates between the hard and the soft law across the European cyber policy mix. A limited transfer of competences, the lack of competences for the policy mix and its cross-cutting nature led the EU to apply different modes of governance in cyber policy. While decisions are made according to the ordinary legislative process for issues such as the security of the DSM, any decision having an impact on the national cyberdefence must employ soft institutional governance. This recognition was a long-awaited development acknowledging the blurring of lines in three initially distinct but converging policy areas of network and information security measures, including privacy and data protection issues; cybercrime; and cyber defence. It is now established that the European cybersecurity policy area constitutes a highly fragmented legal framework. In this respect, the adoption of the NIS Directive reflects an evolution towards more hard law, even if it and it does not put an end to fragmentation.

Chapter II. Directive (EU) 2016/1148: A Hard Instrument with a Soft Dimension

All cybersecurity efforts today require protection from a wide range of challenges. New and emerging technologies have put the issue of cyber security not only in the forefront, but also on the number one topic of discussion. But being in the 21st century and seeing the ever-growing cyber-security threats which may become issues of national or even international security threat, it is imperative to act. Thus far, the European Union has

[1] Council Proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres - Examination of possible compromise proposals and preparation for the trilogue, 7616/19 LIMITE

[2] 21 April 2020.

taken more of a passive role in promoting cybersecurity related issues[1]. National security falls within the responsibility of Member States of the EU under Article 4 §2 TEU. By stating that "*national security remains the sole responsibility of each Member State*"[2], the Member States, acting as the heads of the treaties, have insisted that national security is one of their inherent competencies. But cybersecurity is not only an issue of national security, but it also has to do with trusting the digital economy, freedom of speech, free trade, the respect of citizens' rights and their data protection and privacy; in a few words, it is a basic element of the European Single Market.

As stated in the previous chapter, the Commission has adopted multiple *soft* instruments over the last ten years,[3] such as communications aiming at enhancing Network and Information Security in the EU. However, this approach has led to a fragmented cybersecurity legal landscape across the EU. The adoption of Directive (EU) 2016/1148 (NIS Directive) presented thus the first EU-wide cybersecurity legislation, and further hardened the European legal framework in the field after the adoption of the regulatory framework for electronic communications in 2002. But having recourse to a *hard* law's instrument does not necessarily entail *hard* obligation. Obligations depend not only on the source (the nature of the instrument) but also on the content of the instrument.

It is on the basis of the assumption that "*the obligation to achieve a particular result is stronger than a best effort obligation, or that a norm containing a principle is less mandatory than a norm containing a right*"[4], that we will study the content of the NIS Directive a foundational policy instrument for enhancing cyber resilience across the EU. This Directive establishes obligations and assigns tasks to the Member States of the EU, as well as to a considerable number of public and private stakeholders. Therefore, assessing the nature of the obligations provided by Directive NIS becomes relevant for evaluating the hardness of the Directive NIS (**Section I**), which aims to balance two main concerns: the development of national cybersecurity capabilities and cross-border cooperation (**Section II**) and the enhancement of national supervision upon critical market operators' security (**Section III**).

---

[1] See K. R. Sliwinski, 'Moving beyond the European Union's Weakness as a Cyber-Security Agent', (2014) 3 *Contemporary Security Policy* 35, 468-469.

[2] Art. 4 §2 TUE, 3rd sentence.

[3] Communication on "i2010 – A European Information Society for growth and employment" COM(2005) 229 final; Strategy for a Secure Information Society COM(2006)251; Council Resolution on a Strategy for a Secure Information Society in Europe (2007/C 68/01); Communication on Critical Information Infrastructure Protection (CIIP) "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" COM(2009)149; Communication on A Digital Agenda for Europe COM(2010) 245 final; Communication on CIIP 'Achievements and next steps: towards global cyber-security' COM(2011) 163 final; Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013).

[4] F. Terpan, 'Soft Law in the European Union - The Changing Nature of EU Law', (2015) 1 *European Law Journal, Wiley*, 21

Section I. Combining Maximum with Minimum Harmonisation Requirements

Harmonisation of laws is not an end, but a tool for the establishment and functioning of the internal market. The techniques for harmonising legislation vary according to the objective pursued by the Union legislator and to the leeway accorded to the national legislator. Although many categorisations have been advocated, the two main types of harmonisation techniques commonly used are the creation and functioning of the internal market: maximum harmonisation and minimum harmonisation. The NIS directive combines minimum with maximum harmonisation requirements. The procedures by which harmonisation measures are adopted are evolving rapidly. The harmonisation of legislation is not an end, but a tool for the establishment and operation of the internal market. For this reason, the harmonisation techniques of the legislation vary depending on the purpose pursued by the Union legislator and the scope of the facility that allows, if permitted, to the national legislator.

The variation between the various harmonisation methods uses quantitative criteria (e.g., the number of elements of a reference field that are the subject of harmonisation in relation to the total data of the specific field is examined). Therefore, there is a distinction between partial harmonisation, if only certain elements that are subject to harmonisation measures have been selected, and extensive harmonisation, in case the harmonisation rules cover the regulatory field. Given the growing complexity of regulatory fields and the proliferation of stakeholders in the modern globalised environment, the partial harmonisation method is not being used to the same extent today as its widespread use in the early stages of European integration.

The harmonisation methods used in the context of European integration can also be categorised based on the qualitative criterion:the depth of harmonisation promoted through a legislative act. This categorisation examines the depth or intensity of harmonisation, which is not defined objectively, but in relation to the field of reference and the goal pursued. More specifically, the depth and intensity of the harmonisation concern the binding nature of the obligations imposed on Member States and national bodies, as well as the thoroughness of the rules established at the EU level and must be applied at the national level (after transfer to the national legal order), in case the EU legislation is a directive). The depth of harmonisation, therefore, directly influences the relationship that develops between the EU regulatory intervention and the national legislative framework. The main criterion is whether Member States prevent them from maintaining or introducing stricter measures. Thus, the two main types of harmonisation techniques commonly used are the "*complete-overall harmonisation*" and the "*minimal harmonisation*". These two types represent diametrically opposed techniques.

Full harmonisation takes place when the harmonising measure, such as a Directive, exhaustively regulates the area, leaving Member States no opportunity to maintain or take measures different from the harmonising measure. That is, in the case of a fully harmonised Directive, Member States may not maintain or adopt provisions with additional requirements of those Directives covered by this section, even in the case of internal relations. Member States may differ from the provisions of a full harmonisation directive, only if the directive expressly allows it. If the harmonisation is maximal, after the establishment of the EU rules, the European Union

shall acquire exclusive jurisdiction over the specific field or the specific elements subject to the harmonisation measures. The wording of Community / EU provisions is usually clear, as it explicitly and precisely defines products and services allowed to move freely within the internal market and under what conditions. The advantages of a single set of rules, which apply both intra-Community and nationally, are that it creates a level playing field between the various European Union regulators and provides clarity on the rules and procedure for state enforceability modifying them, which in turn contributes to political and economic stability.

On the other hand, a serious disadvantage of full / maximum harmonisation is that it is often not a realistic option. Since the creation of a single market constitutes a concurrent responsibility of the Union, its action to achieve this goal cannot fully comprehend the scope, (e.g., harmonisation cannot be complete except in very exceptional cases). It also does not characterise the heterogeneity of the modern European Union of the 27 Member States in terms of economic structures, social systems, legal traditions, political institutions, and administrative practices. Although it proved effective in tackling the problems of market integration at the beginning of the European Union, the method of full harmonisation was abandoned in the 1970s and was soon overtaken by the European Commission's new approach to completing the internal market which was based on minimal harmonisation.

The minimum harmonisation method has been the most widespread harmonisation method since the 1970s in the European Union and was first formulated in the Internal Market Completion Program. This method is based on the establishment of minimum rules. This method was seen as more realistic, as it limited the data being harmonised with the essential elements of each policy, allowing Member States to introduce or maintain stricter provisions if they do not violate EU law. As pointed out by the CJEU, "*the concept of minimum standards does not limit Community intervention to the lowest common denominator nor, of course, to the lowest level of protection provided for in the various Member States, but it does mean that the States are free to secure greater protection than the potentially high level of protection under Community law*"[1]. Of course, the ability of Member States to add stricter rules than the minimum of the EU Member States often results in over-regulation. It should be noted, however, that the national measure, the requirements of which go beyond those of the harmonising measure, should not violate the provisions of the Treaty relating to free movement.

In this way, minimum harmonisation allows the difference, in contrast to full harmonisation which excludes it. Therefore, the European Union has shown a preference for minimal harmonisation measures, especially when it legislates in areas of social policy. In practice, minimal harmonisation was particularly effective in removing technical barriers (technical specifications for products), which was also the aim of the European Commission's new strategy for establishing a common market by 1992. However, it proved problematic in all areas as they presented more complex regulation either in goods or services that could create security or health problems, for which there were barriers to intra-Community transactions that were legal (e.g., and could discourage economic

[1] Case C-84/94, *United Kingdom of Great Britain, and Northern Ireland v Council of the European Union*, ECLI:EU:C:1996:431

operators from conducting cross-border transactions).[1] The EU adopted the NIS Directive in July 2016, a minimum harmonisation directive establishing common security and co-operation rules for all EU Member States since Member States "*may adopt or maintain provisions with a view to achieving a higher level of security of information networks and systems*" (Art. 3 NIS-D).

August 2016	-	**Entry into force**
February 2017	6 months	**Cooperation Group begins tasks**
August 2017	12 months	**Adoption of implementing on security and notification requirements for DSPs**
February 2018	18 months	**Cooperation Group establishes work programme**
9 May 2018	21 months	**Transposition into national law**
November 2018	27 months	**Member States to identify operators of essential services**
May 2019	33 months (i.e. 1 year after transposition)	**Commission report - consistency of Member States' identification of OES**
May 2021	57 months (i.e. 3 years after transposition)	**Commission review**

Figure 1: *NIS Directive Timeline*

Source: *https://slideplayer.com/slide/13541086/*

The NIS Directive is therefore undoubtedly a founding instrument in the arsenal of legislative measures adopted by the Union legislator to combat cyber threats since it establishes obligations and assigns tasks to Member States as well as to certain economic operators.[2] However, as we can see in the following table, it leaves the Member States a room of maneuver to lay down more stringent provisions, with a view to achieving a higher level of security (minimum harmonisation) since more than half of the obligations (52 out of 91) are obligations of result (**Table 5**). The question arises whether the NIS Directive would not fuel, by the nature of its obligations, the already existing legislative fragmentation than harmonisation. However, it would be more a question of establishing a common base of definitions and principles on the basis of cooperation among Member States.

Actors	Types of Obligations

[1] See K.P. Purnhagen and J.H. Wesseler, 'Maximum vs minimum harmonization: what to expect from the institutional and legal battles in the EU on gene editing technologies', (2019) 9 *Pest Management Science* 75, 2310-2315 ; See also P. Giliker, 'The Transposition of the Consumer Rights Directive into UK Law: Implementing a Maximum Harmonization Directive', (2015), 1 *European Review of Private Law* 23, 5-28 ; R. Lang, 'The EU's New Victims' Rights Directive: Can Minimum Harmonization Work for a Concept Like Vulnerability?', (2013), 22 *Nottingham LJ* 90 ; F. Gomez and J.J. Ganuza, 'An Economic Analysis of Harmonization Regimes: Full Harmonization, Minimum Harmonization or Optional Instrument?', (2011), 2 *European Review of Contract Law* 7, 275-294 ; P. Rott, 'Minimum harmonization for the completion of the internal market? The example of consumer sales law', (2003), 5 *Common Market Law Review* 40, 1107-1135; M. Dougan, 'Minimum Harmonization and the Internal Market', (2000), 4 *Common Market Law Review* 37, 853-885.

[2] Interview 5

	To act		To abstain	Voluntary Obligations
	Of result	*Of means*		
Commission	5	1	-	2
Union	-	1	-	-
Member States	16	13	4	1
National competent authorities and single point of contact	11	6	-	3
Computer security incident response teams (CSIRTs)	7	-	-	1
Cooperation Group	6	1	-	-
CSIRTs network	3	1	-	-
OES	2	2	-	-
DSP	2	3	-	-

Table 5: *NIS Directive 2016/1148 Provisions Typology*

Table made by author and source based on NIS Directive

The digital transformation of society has expanded the threat landscape and is bringing about new challenges which require adapted and innovative responses. Thus, the Union legislator has defined the scope of the NIS directive by seeking to reconcile three distinct concerns: the need for harmonisation in the interest of cybersecurity; the necessary autonomy of Member States in safeguarding the essential interests of national security, public action and security; and a form of subsidiarity with regard to certain sectors where rules of application already apply similar security. Therefore, assessing the nature of obligations provided by Directive NIS becomes relevant for evaluating the hardness of Directive NIS, which aims to balance two main concerns: the development of national cybersecurity capabilities and cross-border cooperation.

Section II. National Capabilities' Development and Cross-Border Cooperation: From Minimum Regulatory Limit Thresholds to 'Soft Governed' Structures

Dependence on digital resources in general leads to vulnerabilities that require urgent attention. Thus, the development of national capabilities becomes an urgent matter. However, by observing the various texts of European law adopted since 2009, there is no precise definition of what is meant by *national capabilities*.

In a 2009 communication from the Commission on Critical Information Infrastructure Protection, we can read that, "*a strong European early warning and incident response capability has to rely on well-functioning National/Governmental Computer Emergency Response Teams (hereafter CERTs), e.g. having a common baseline in terms of capabilities*"[1]. The Commission was inviting Member States and concerned stakeholders to "*define, with the support of ENISA, a minimum level of capabilities and services for National/Governmental*

[1] European Commission Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', 30 March 2009, COM(2009) 149 final

CERTs and incident response operations in support to pan-European cooperation" and to "*make sure National/Governmental CERTs act as the key component of national capability for preparedness, information sharing, coordination and response*".

On 14-15 April 2011, the Presidency of the Council organised in *Balatonfüred*, in collaboration with the Commission, a Ministerial Conference on Critical Information Infrastructure Protection. The Presidency Statement emphasised the need for Member States

> "*to intensify their efforts in reinforcing their national cyber-security capabilities. It also underlined the importance of stimulating and support the development of a high level of preparedness, security and resilience capabilities and to up-grade technical competencies to allow Europe to face the challenge of networks and information infrastructure protection*."[1]

Information sharing is also important for cyber resilience, situation monitoring, and policy development. A general goal is to increase the security of network and information systems against attacks. Competition law of the EU has traditionally viewed information sharing - especially among market competitors - with suspicion. The cross-border nature of cyber threats adds additional wrinkles: in the event of a cyber-event, not only are companies subject to the unclear laws of a single sovereign, but they will also likely face the varying laws of multiple sovereigns. As one can imagine, this clearly complicates matters especially in the context of cross-border information sharing.

The EU's comprehension of national capabilities and cross-border collaboration combines two approaches. While a vertical approach was adopted for setting up Member States capabilities through hard obligation with a minimum regulatory threshold (**§1**), a *soft governed* cross-border cooperation was chosen (**§2**).

§1. Enhancing National Capabilities Through Hard Obligations with A Minimum Regulatory Limit Threshold

Under the NIS Directive, *national capabilities* refers to the "*technical and organisational capabilities, to prevent, detect, respond to, and mitigate network and information system incidents and risks*"[2]. However, Member States have quite different levels of capabilities and preparedness, leading to fragmented approaches to NIS across the EU.[3]

[1] Council of European Union, CIIP – "*Achievements and next steps: towards global cyber-security*", Adoption of Council conclusions, 2011, 10299/11.

[2] Recital 34 of Directive 2016/1148

[3] *Ibid,* Recital 5

Thus, they are required to set national strategies at national level to adopt integrated policies and regulatory measures in order to ensure high levels of security. (**A**) The setting up of National Competent Authorities to monitor the implementation of the Directive (**B**) and Computer Security Incident Response Teams (**C**), form part of the Member States' obligations under the NIS Directive.

A. National Cybersecurity Strategy (Article 7 NIS)

Following Article 7 §1 NIS Directive, Member States are required to adopt a national strategy "*defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems*". In this task, Member States can be assisted by ENISA[1]. Thus, a National CyberSecurity Strategy (hereafter NCSS) is a plan of actions designed to set strategic principles, guidelines, objectives and specific measures to mitigate risks associated with cybersecurity and to foster cyber resilience for a nation. It is addressed among all public and private stakeholders with a specific timeframe application.[2]

Even if the NCSS represents only a soft law instrument without any binding force, the NIS directive sets a limit threshold to the content of the NCSS. In fact, this strategy shall address the following issues:

> "*(a) the objectives and priorities of the national strategy on the security of network and information systems; (b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of government bodies and the other relevant actors; (c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors; (d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems; (e) an indication of the research and development plans relating to the national strategy on the security of network and information systems; (f) a risk assessment plan to identify risks; (g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems*".

[1] Available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies (accessed on March 3rd, 2020)

[2] Art. 7 §3 : *Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption…*

ENISA has already published[1] in 2012 the main points that should be covered by a typical NCSS.[2] Main points which, compared to article 7§1 of the NIS Directive, present similarities (**Table 6**).

2012 ENISA Guidelines	2016 NIS Directive (Art. 7 §1)
To define a governance framework for cyber security	*(b) a **governance framework** to achieve the objectives and priorities of the national strategy on the security of network and information systems, including **roles and responsibilities** of the government bodies and the other relevant actors;*
To outline and define necessary policy and regulatory measures and clearly defined roles, responsibilities, and rights of the private and public sector (e.g., new legal framework for fighting cybercrime, mandatory reporting of incidents, minimum security measures and guidelines, new procurement rules).	
To identify critical information infrastructures (CIIs) including key assets, services and interdependencies.	*(g) a **list of the various actors involved** in the implementation of the national strategy on the security of network and information systems.*
To develop or improve preparedness, response and recovery plans and measures for protecting such CIIs (e.g., national contingency plans, cyber exercises, and situation awareness). This may also mean an integration of existing structures (e.g., national/governmental CERTs).	*(c) the identification of measures relating to **preparedness, response, and recovery**, including cooperation between the public and private sectors;*
To define a systematic and integrated approach to national risk management (e.g., trusted information sharing and national registries of risks).	*(f) a **risk assessment plan** to identify risks;*
To define and set the goals for awareness raising campaigns that instil changes in the behaviour and working patterns of users.	*(d) an indication of the **education, awareness-raising** and **training programmes** relating to the national strategy on the security of network and information systems;*
To define the needs for new curricula with emphasis on cyber security for IT and security professionals and specialists; and also training programs that allow the improvement of skills of users.	
Comprehensive research and development programs that focus on emerging security and resilience issues of current as well future systems and services (e.g., smart devices).	*(e) an indication of the **research and development plans** relating to the national strategy on the security of network and information systems;*
To define an appropriate mechanism (often a public private partnership) that allows all relevant public and private stakeholders to discuss and agree on different policy and regulatory cyber security issues.	-
To set the goals and means to develop national capabilities and the necessary legal framework to engage in the international efforts of diminishing the effects of cybercrime.	-

[1] ENISA, National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace, 2012, available at https://www.enisa.europa.eu/publications/cyber-security-strategies-paper (accessed on March 3rd, 2020)

[2] Interview 5

International co-operation with EU and non-EU Member States (e.g., adoption of international conventions).	-

Table 6: *Article 7§1 NISD Similarities with 2012 ENISA Guidelines*

Table made by author and source based on ENISA publication

Four years later with the adoption of the NIS Directive, ENISA went even further by updating its guide.[1] Indeed, it updated the different steps, objectives and good practices of the original guide and analyses the status of NCSS in the European Union and EFTA area. In addition, fifteen objectives for the implementation of NCSS are described (**Table 7**).

1. **Develop national cyber contingency plans**	**9. Address cyber crime**
2. **Protect critical information infrastructure**	10. Engage in international cooperation
3. **Organise cyber security exercises**	11. Establish a public-private partnership
4. **Establish baseline security measures**	12. Balance security with privacy
5. **Establish incident reporting mechanisms**	13. Institutionalise coop. between public agencies
6. **Raise user awareness**	14. Foster R&D
7. **Strengthen training and educational program.**	15. Provide incentives for the private sector to invest in security measures
8. **Establish an incident response capability**	

Table 7: *2016 ENISA's NCSS Good Practice Guide Objectives*

Table made by author and source based on ENISA publication

Finally, the NCSS must cover at least the energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure sectors and the online marketplace, online search engine, and cloud computing services.

B. National Competent Authorities, a mixed governance approach (Article 8 NIS)

[1] ENISA (2016), NCSS Good Practice Guide.

National Competent authority (hereafter NCA) is the term used in NIS for a regulatory body. According to the NIS Directive, it shall "*monitor the application of this Directive at national level*"[1]. As with most of the obligations included in the NIS Directive, we are here faced with an obligation of result. By dwelling on the term *monitor*, we note that no mention is made of the monitoring tools to be used. However, Member States will have to ensure that "*the competent authorities have sufficient resources to be able to carry out their tasks effectively and efficiently*". Therefore, if the Authorities have all the necessary latitude in the monitoring tools to be implemented, they will have to ensure their effectiveness and efficiency. In this regard, recitals 59 and 61 provide some details, even if they have no binding legal force;

Concerning the NCA's organisation, "*in view of the differences in national governance structures and in order to safeguard already existing sectoral arrangements or Union supervisory and regulatory bodies, and to avoid duplication*"[2]. Thus, each Member State is required to designate one or more national competent authorities for being accountable mainly for the identified sectors and services[3] covered by the NIS Directive, without excluding the option to also cover additional ones.[4] This role can be assigned to an existing authority or authorities. Member States may choose between adequate governance approaches to their national governance they use: (a) the centralised approach; (b) the decentralised approach and (c) the hybrid approach (**Table 8**).

Centralised approach	**This type is characterised by a central cybersecurity authority with wide responsibilities and capabilities within different sectors.**
Decentralised approach	This type is characterised by a strong degree of cooperation between multiple sector-based authorities being responsible for specific sectors and services.
Hybrid approach	This type is characterised by the combination of elements of both centralised and decentralised approaches.

Table 8: *National Competent Authorities Governance Approach*

Table made by author and source based on ENISA publication

[1] Article 8§2 of Directive 2016/1148

[2] Recital 30 of Directive 2016/1148

[3] *Ibid*, Annexes I &II

[4] *Ibid,* Article 8 §1: '*covering at least the sectors referred to in Annex II and the services referred to in Annex III*'.

This is rather regrettable because in my opinion, it is the small countries which should have favoured a centralised approach for saving resources – both human and economic – and for minimising the possible friction between several services. Whereas the decentralised approach would make the industry more confident vis-à-vis the device, since it will make the choice of the NCA most compatible with its sector, but also this will lead to a sectoral specialisation of personnel different to NCA's. However, this diversified approach to NCA's is also found in the implementation of the CERTs.

C. Computer Security Incident Response Teams (Article 9 NIS)

Before presenting NIS Directive provisions relative to Computer Security Incident Response Teams (hereafter CSIRT), it is important to be able to distinguish a Computer Emergency Response Team (CERT) from a CSIRT. Because it these two terms are sometimes confused. Initially, a team that took care of computer and network security incidents was called a CERT. That term was trademarked by Carnegie Mellon University and they give licenses to all legit teams who want to use that word. Thus, all organisations wishing to use CERT in their team's name must request permission through the CERT / CC authorities. It was at that point and in an attempt to circumvent this permission that the term CSIRT was introduced by the NIS Directive.[1]

Early CSIRTs had little authority and could only issue alerts and recommendations in their organisations. The evolution of CSIRTs can be placed within three broader trends:

> "*(1) creation of governmental and national CSIRTs as coordinating bodies and information-sharing platforms for CSIRTs; (2) reformation of overarching cybersecurity structures and revaluation of the role and location of the existing mature national CSIRT; (3) inclusion of references to CSIRTs in international cybersecurity policy discussions encouraging countries to establish CSIRTs*."[2]

There is no one-fits-all answer to the question whether a security team can call itself CERT or CSIRT. Under NIS Directive, each Member State is required to establish an IT security team for responding to cybersecurity incidents, by providing any critical information to the relative stakeholders; and based on certain capabilities and requirements[3] defined in a relative policy document.[4] Thus, according to the national implementation of the

[1] First European research network was created by the French Spatial Physics Analysis Network (SPAN) in 1990. It was followed by the Dutch research network SURFnet CERT, created in 1992 and the DFN-CERT of the network of the German Research Academy in 1993.

[2] See I. Skierka, R. Morgus, M. Hohmann and T. Maurer, 'CSIRT Basics for Policy-Makers - The History, Types & Culture of Computer Security Incident Response Teams, Transatlantic Dialogues on Security and Freedom in the Digital Age', [Paper], *Global Public Policy Institute*, May 2015, available at https://www.gppi.net/media/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf (accessed on March 5th, 2020)

[3] Annex I of Directive 2016/1148

[4] This policy should be communicated to the Commission.

NIS Directive a security team can call itself CSIRT by following formal designation by a national authority. But this may be a potential for misunderstanding here, as not every CSIRT fulfils this criterion, but in some contexts, it might be somehow implied. Perhaps it would have been better to introduce a term like *NIS-CSIRT* for such teams.[1]

There can be a single CSIRTs covering all, or the responsibility can be split over multiple CSIRTs. The only requirement from the NIS Directive is that every identified OES/DSP must have a CSIRT[2] assigned to it.[3] While NIS Directive delimitates the framework of activities of the CSIRT, ENISA may provide a relative guidance in "*developing national CSIRTs*"[4]. The constituency criteria of *national CSIRT* appears here for the first time in the whole directive. Today the roles and responsibilities of CSIRTs vary widely, depending on their funding and expertise.[5] Institutions such as Software Engineering Institute and the ENISA have grouped CSIRTs into different types based on the services they provide or the sectors they serve (**Table 9**).

ENISA (2013)	ENISA (2006)
• National	• National
• National/Governmental	
• De facto National	
• Governmental	• Governmental
• Governmental/Military	
• Research & Education Sector	• CIP/CIIP Sector
• Financial Sector	• Governmental Sector
• Energy Sector	• Military Sector
• Non-commercial organization	• Academic Sector
• Commercial organization	• Internal
	• SME
• ICT Vendor Customer Base	• Vendor
• Service Provider/ISP Customer Base	
• N/A	• Commercial

Table 9: *ENISA 2013/2016 CSIRT Typology*

Table made by author and source based on ENISA publication

According to ENISA's study on CSIRT 2020 landscape, among the 344 CSIRTS identified, there was "*a majority of Commercial Sector, NREN, Governmental sector and financial sector CSIRTs, while entities in*

[1] Available at https://www.cert.at/en/blog/2018/8/blog-20180731155524-2252 (accessed on March 5th, 2020)

[2] Which is qualified according to Annex I.

[3] Recital 34 of Directive 2016/1148

[4] Article 9 §5 of Directive 2016/1148

[5] Interview 5

Military organisations, CIP/CIIP sector, Law enforcement agencies, and non-commercial organisations were less represented"[1]. 15 Member States had less than 8 CSIRTs identified in the inventory. All EU Members States have a national and/or government CSIRT. No EU Member State has CSIRTs for all critical sectors. 3 Member States have a CSIRT for the energy sector (Poland, Italy, and Austria). 13 Member States have a CSIRT for the financial sector (Austria, Belgium, Czech Republic, Estonia, Germany, Italy, Luxembourg, Spain, and the UK). 10 Member States have a CSIRT focusing on Critical Information Protection and / or Critical Information and Infrastructure protection (Belgium, Estonia, Germany, Italy, Luxembourg, Slovakia, Spain, and the UK).

Following analyses of NIS Directive provision on CSIRT, we can understand that the used term of *National CSIRT* is just shorthand for a designated CSIRT in Member States. There is no definition of a national CSIRT in the NIS Directive, nor a reference to an external definition. Thus, the language of the NIS Directive regarding national CSIRTs does not reflect the meaning of the term as it was used in the years prior to the NIS Directive, as a national CERT could be also designated by Member States inside the NIS context (Annex).

The role of the CSIRT shall include: "*the monitoring of incidents*"[2]; "*the provision of early warning, alerts and information sharing to relevant stakeholders in case of incidents reported*"[3]; "*the response to incidents*[4]*; the provision of dynamic*[5] *risk and incident analysis and raising situational awareness*"[6]; "*the participation in a network of the CSIRTs*"[7] within EU. Furthermore, "*Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level*". We are therefore in the presence of an obligation of result and the terms "*appropriate, secure, and resilient*" require some clarifications. In this regard, Annex I of NIS Directive provides some precisions. CSIRTs shall ensure a

[1] ENISA, 'Study on CSIRT landscape and IR capabilities in Europe 2025', (2019), available at https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025 (accessed on March 7th, 2020)

[2] Annex I (2) (a) of Directive 2016/1148

[3] *Ibid,* Annex I (2) (b)

[4] *Ibid,* Annex I (2) (c)

[5] Dynamic in the sense that the data changes as the time passes by and the actions taken to cope with the incident will also change till the succeed respond to the cyber threat.

[6] Annex I (2) (d) of Directive 2016/1148

[7] Through partnerships with public and private area and cooperation with CSIRTs' from different Member States, based on the tasks referred in Annex I(2)(c)(d).

high level of availability of their communications services[1], be in secure sites[2], be capable of preserving business continuity[3], and have the possibility of participating in international cooperation networks.[4]

If the NIS Directive does not in itself entail obligations of means allowing to better specify the tasks which fall to the CSIRTs, it is possible to have recourse to ENISA guidance. In accordance with the ENISA study[5], the nature of the expected function of the CSIRT, should be characterised[6] by pro-activity[7], reactivity[8], artifact handling[9], security and quality management services.[10] Furthermore, the Member States should develop a business plan with "*clearly defined procedures ensuring the security, the quality and the strengthening of the provided services from the CSIRT*"[11]. More specifically, the creation of the CSIRT entity should be complemented by "*a policy document focusing on defining the financial model, defining the organisational structure, hiring the right staff, developing an information security policy and searching for cooperation between other CSIRTs and possible national initiatives*"[12]. CSIRT maturity might influence the effectiveness of a CSIRT in providing the aforementioned services above to its constituency and in cooperating with other teams. CSIRT maturity[13] can be more generally understood as "*a teams' ability to manage (document, perform and*

[1] Annex I (1) (a) of Directive 2016/1148 : '…by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. The communication channels shall be clearly specified and well known to the constituency and cooperative partners.'

[2] *Ibid,* Annex I (1) (b)

[3] *Ibid,* Annex I (1) (c) : '(i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers; (ii) CSIRTs shall be adequately staffed to ensure availability at all times; (iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.'

[4] *Ibid,* Annex I (1) (d)

[5] ENISA, 'CSIRT Setting up Guide in English', (2006), available at https://www.enisa.europa.eu/publications/csirt-setting-up-guide (accessed on March 7th, 2020)

[6] These are implied in the CSIRT tasks in Annex I (2), in accordance with European Commission - Fact Sheet 'Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cyber security'.

[7] In terms of preparedness, through awareness building and training.

[8] In terms of providing incident handling and mitigation treatment activities - Based on the tasks of the Annex I (2).

[9] Performed through analysis of the evidence found - Based on the requirement of Annex I (3).

[10] Provided through clearly defined responding and mitigation plans.

[11] ENISA, 'CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs', (2016), available at https://www.enisa.europa.eu/publications/csirt-capabilities (accessed on March 7th, 2020)

[12] Recital 34 of Directive 2016/1148

[13] In 2015, the National Cyber Security Centre of the Netherlands published a document, 'CSIRT Maturity Kit - A step-by-step guide towards enhancing CSIRT Maturity', which provides good practices for CSIRTs to achieve a higher level of maturity.

measure) CSIRT capabilities and services in particular"[1]. The maturity of an organisation is defined as measurement of its capability in terms of structure, people, processes, and technologies.

It provides a certain level of assurance that the organisation can carry out its activities and functions in a consistent and trustworthy manner, while being able to focus on constant development. Depending on the national context, increasing the level of maturity of a national CSIRT can involve organisational and personnel changes. The CSIRT community's mission and effectiveness can be disrupted intentionally or unintentionally. It is therefore crucial for policymakers to understand CSIRTs, their history and evolution, as well as current trends and challenges, to establish well balanced policies and regulation. The next strategic pillar of the NIS Directive focuses on increasing the EU level cooperation and coordination for building confidence and trust among the Member States.

§2. Establishing Cross-border Cooperation Through Soft Governance Structures

The NIS Directive encourages cross-border collaboration and information sharing to reduce the risk of attack and improve responsiveness, a particular focus on the creation of the Single points of Contact (**A**), the strategic NIS cooperation group (**B**) and the creation of a CSIRT network (**C**).

A. The single points of contact (Article 9 & 10 NIS)

Each Member State shall designate a national Single Point of Contact (hereafter SPOC).[2] The role of the SPOC is to establish a "*trusted cross-border information sharing mechanism in order to facilitate the identification and cooperation of competent authorities, between different Member States*"[3]. The Member States of the EU may assign this role to an existing authority. In case a Member State adopts a centralised governance approach, the designated NCA may also have the role of the SPOC.[4] We will not go back over the different types of approaches, as has been already explained for the NCAs, therefore we will limit ourselves to the only exposure of the SPOCs to centralised approach (**Table 10**).

Austria	Federal Ministry of the Interior	**Ireland**	CSIRT-IE

[1] ENISA, 'CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs', (2016), available at https://www.enisa.europa.eu/publications/csirt-capabilities (accessed on March 7th, 2020)

[2] Article 8 §3 of Directive 2016/1148

[3] Article 8 §4 and recital 31 of Directive 2016/1148

[4] *Ibid,* Article 8 §3

Belgium	Centre for Cybersecurity Belgium	**Lithuania**	National Cyber Security Centre (NCSC/CERT-LT)/
Cyprus	Digital Security Authority (DSA)	**Malta**	Critical Information Infrastructure Protection Unit
Czech Republic	National cyber and information security agency	**Portugal**	Portuguese National Cybersecurity Centre
Estonia	Estonian Information System Authority	**Romania**	Romanian National Computer Security Incident Response Team (CERT-RO)
France	Agence nationale de la sécurité des systèmes d'information (ANSSI)	**Slovakia**	National Security Authority
Germany	Federal Office for Information Security / Bundesamt für Sicherheit in der Informationstechnik	**Slovenia**	Information Security Administration
Greece	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications and Media)	**Spain**	National Security Council, through the National Security Department
Hungary	National Cyber Security Centre		

Table 10: *Member States SPOCs with centralized approach*

Table made by author and source based on the site of the European Commission

Once the SPOC identified and its tasks designated, the Member States shall inform the Commission by the transposition deadline. Afterwards, a list of designated SPOCs is published by the Commission "*for ensuring transparency and effective coordination*"[1], between the relevant authorities at European level. But also, at national level, as SPOC shall also, whenever appropriate and in accordance with national law, "*consult and cooperate with the relevant national law enforcement authorities and national data protection authorities*"[2]. The SPOC of each Member State is required for sending an anonymous[3] summary report every year to the Cooperation Group with the number of incident notifications, the "*nature of the incidents*" [4] and the measures taken by the national authorities. To carry out the tasks assigned to them in an effective and efficient manner, SPOCs[5] must have the adequate technical, financial, and human resources.

[1] Article 8 §7 of Directive 2016/1148

[2] *Ibid,* Article 8 §6

[3] *Ibid,* Recital 33: '…as information on the identity of the notifying entities is not required for the exchange of best practice in the Cooperation Group.'

[4] *Ibid,* '…such as the types of security breaches, their seriousness or their duration.'

[5] As also for competent authorities.

According to article 8§4, the SPOC shall "*exercise a liaison function to ensure cross-border cooperation of Member State authorities*", with Cooperation Group and CSIRTs network.

B. The strategic NIS cooperation group (Article 11 NIS)

A Cooperation Group is established between Member States with the aim of developing cross-border credibility and trust through the exchange of information and best practices and standards, the evaluation of national strategies, the effectiveness of CSIRTs and more.[1] It is composed of representatives from ENISA, Member States, and the Commission, which acts as a secretariat of the Cooperation Group.[2] The Chairmanship is ensured by the Member State holding the Presidency of the Council of the EU.[3]

The role of the Cooperation Group is crucial for assisting the CSIRT network for sharing information and best practice and generally for Member States in their tasks. More specifically, and according to Article 11§3 (a) of Directive 2016/1148, the Cooperation Group's tasks are:

> "*(a) Defining the way CSIRTs network performs its tasks, by providing strategic guidelines to the CSIRT network (b) The provision of guidelines to the CSIRT network for exchanging best practices for handling incidents; (c) The provision of non-binding guidelines to Member States supported by ENI-SA's workshop activities, for exchanging best practice, aiming to assist in building national capacities on the security of networks and information systems; (d) The productive*[4] *provision of consultant support to Member States for evaluating the national capabilities and capacities, on a voluntary basis, and the effectiveness of CSIRTs; (e) The exchanging of information and best practice concerning training and awareness-raising; (f) The exchanging of information and best practice on the security of network and information systems, relative to research and development; (g) Maintaining of communication with relevant Union institutions, bodies, offices and agencies and exchanges experiences on relative security issues; (h) Building on a standardisation approach with the assistance of relevant European standardisation organisations; (i) The concentration of best practice information relative to risks and incidents; (j) The examination, on an annual basis, of the summary reports from the Single Point of Contacts with information relative to the incident notification; (k) Organising cybersecurity exercises, education programmes and training, supported by ENISA; (l) The*

[1] Article 11 §1 of Directive 2016/1148: 'In order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence…'

[2] *Ibid,* Article 11 §2

[3] Croatia's presidency of the Council of the EU: 1 January - 30 June 2020.

[4] Through the discussion process the cooperation group identifies best practices and promotes them accordingly.

establishment of the following processes, supported by ENISA's contribution: the identification process of operators of essential services by Member States and the cross-border affection process for notifying incidents to the neighbouring Member States; (m) The consistent work on defining proper non-binding guidelines on incident notifications."

According to provision 11 §5 NIS Directive, the NIS Cooperation Group functions according to the European Commission Implementing Decision of February 1st, 2017[1] and following its own rules of procedure.[2] The Cooperation Group's decisions are made by consensus. The duration of the work programs is "*two years*"[3] and every fifteen months, "*it is required to provide a report to the Commission, clarifying the positive contribution of the cooperation*"[4]. This report also functions as input to the European Commission's review of the Directive. The Cooperation Group has so far produced the following eleven documents[5]:

- Reference document on security measures for Operators of Essential Services (CG Publication 01/2018)
- Reference document on incident notification for Operators of Essential Services (CG Publication 02/2018)
- Compendium on cyber security of election technology (CG Publication 03/2018)
- Cybersecurity incident taxonomy (CG Publication 04/2018)
- Guidelines on notification of Operators of Essential Services incidents (CG Publication 05/2018)
- Guidelines on notification of Digital Service Providers incidents (CG Publication 06/2018)
- Reference document on the identification of Operators of Essential Services (CG Publication 07/2018)
- Guidelines for the Member States on voluntary information exchange on cross-border dependencies (CG Publication 01/2019)
- Risk assessment of 5G networks (CG Publication 02/2019)
- Sectorial implementation of the NIS Directive in the Energy sector (CG Publication 03/2019)

[1] OJ L 28, 2.2.2017, p. 73–77

[2] Available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51975 (accessed on March 8th, 2020)

[3] Article 11§3 of Directive 2016/1148: 'Every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken'.

[4] *Ibid,* Article 11§4

[5] Available at https://ec.europa.eu/digital-single-market/en/nis-cooperation-group (accessed on March 8th, 2020)

- Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures (CG Publication 01/2020)

While the Cooperation Group promotes strategic cooperation at EU-level, CSIRT network intends fostering effective operational cooperation at EU-level and building trust and confidence between Member States.

C. The CSIRT network (Article 12 NIS)

A network of national intervention teams on computer security incidents across the EU is being set up to quickly respond to cyber threats and incidents. The effectiveness of the networks of these national teams is achieved through the exchange of information on individual events, the definition of forms of operational cooperation related to early warning, the issuance of guidelines and more. For this communication being effective, trust and confidence must be present among the members of the CSIRT network and therefore among Member States.[1]

Article 12 §3 NIS Directive presents a non-limitative list of CSIRT network tasks. By 9 August 2018 and every 18 months thereafter, the CSIRTs Network is required to provide an assessment report of the benefits "*obtained through the operational cooperation, including conclusions and recommendations, to the Commission*"[2]. The CSIRTs network shall lay down its own rules of procedures.[3]

If the NIS Directive aims not only to promote cooperation between nations but also between private entities and governments, by establishing an efficient and effective governance on NIS matters, EU Member States will also have to supervise the cybersecurity of critical market operators in their country.

Section III. NIS Operators' and Providers' Security Obligations and National Enforcement Mechanisms

Article 1 of the NIS Directive establishes three important rules. First, the directive applies without prejudice to the rules of Union law on the protection of critical infrastructure, the fight against sexual abuse and child pornography, as well as attacks against information systems. Then, it applies without prejudice to the national measures taken to preserve the essential state functions of the Member States, in the field of national security and the maintenance of public order as well as research, observation and prosecution offenses. Finally, the sectoral legal acts of the Union which impose on essential service operators or digital service providers security

[1] Article 12 §1 of Directive 2016/1148

[2] This will serve as a contribution to the review of the functioning of the Directive.

[3] Article 12 §5 of Directive 2016/1148

or incident notification rules having an effect at least equivalent to that of the obligations provided for by the NIS Directive, continue to apply[1].

Thus, according to the NIS Directive's provisions, the security architecture of digital networks at Union level has been divided between the Operators of Essential Services (**§1**) and the Digital Providers Services (**§2**).

Member States must implement primary and secondary legislation adopted by the EU legislator. They are oftentimes free to choose which type of enforcement to use to enforce substantive norms. For example, Member States can choose to enforce a substantive norm regarding cybersecurity law by creating an agency or delegating the task to a ministry, also through sanctions derived from administrative, criminal, or private law. A third paragraph will be thus interested in implementation and enforcement provisions of the NIS Directive (**§3**).

§1. Operators of Essential Services' Security Requirements and Incident Notification

According to NIS Directive, an Operator of Essential Services (OES) is defined as a public or private entity established in a member state,[2] which provides an essential service for the maintenance of critical societal and/or economic sectors. A service that depends on the usage of network and information systems and for which, an incident would have significant disruptive effects on the provision of that service.[3] However, the identification criteria's calls for some clarifications (**A**).

Consequently, identified OES are required to implement the NIS Directive. OES should take appropriate and proportionate technical and organisational measures to manage risk, prevent and minimise the impact of incidents and notify without undue delay, the competent authorities, events with a significant impact on the continuity of the key services they provide. A situation which generates some obligations among private stakeholders (**B**).

A. Identification process (Article 5 NIS)

[1] lex specialis clause - Art. 1 §7 of Directive 2016/1148

[2] Recital (21) of Directive 2016/1148: 'For the purposes of identifying operators of essential services, establishment in a Member State implies the effective and real exercise of activity through stable arrangements.'

[3] *Ibid,* Article 4 (4)

The Directive has direct implications for many companies and utilities in the State. A number of these companies and utilities have been designated as *Operators of Essential Services* (OES) by the Department and are subject to security obligations and incident reporting requirements. To correctly transpose the Network and Information Security Directive, there are two parallel processes being conducted in tandem. The first of these is identifying the Operators of Essential Services to whom the Directive will apply (**1**). While a second one refers to the cross-border consultation process (**2**).

1. The identification criteria, absence of common definition

To make sure that all Member States follow the same approach on the identification of the OES, a list of each sector and subsector is provided in Annex II of the Directive to serve as a roadmap (**Appendix 2**: Types of essential entities falling within the scope of the NIS Directive). As regards the public domain, the scope of the Directive does not apply to all public administrations but only to those which have been identified as operators of essential services.[1] In other words, it is the formal identification of an entity as operator of essential services that prevails. Even if an entity meets identification criteria, it will not be considered as OES if not identified as such.

Following *lex specialis* principle of Article 1 §7 NIS Directive, an EU legal act should impose security and/or notification requirements on the OES similar to those imposed by the NIS Directive. This precondition will determine when the NIS Directive requirements should or not be applied to the OESs. In any other case, the identification process of the OESs should proceed.

During the second stage, it will be necessary to establish whether the public or private entity in one of the sectors or sub-sectors described above meets or not the three identification criteria of article 5 §2 NIS Directive, namely: "*the entity provides a service which is essential to the maintenance of critical social and economic activities; the provision of this service is dependent on networks and information systems; an incident would have a significant disruptive effect on the provision of that service*"[2]. Finally, Member States must research if the operator provides basic services to other Member States.[3]

The Directive does not oblige the use of specific technical security products, which may intails a disparity between the Member States on the matter.[4] Thus, when an entity provides an essential service in two or more Member States, those Member States shall "*engage in bilateral or multilateral discussions with each other*

[1] Recital 45 of Directive 2016/1148

[2] *Ibid,* Article 5 §2

[3] *Ibid,* Article 5 §4

[4] Interview 8

before a decision on identification is reached"[1]. This, will ensure that they are dealt with under a common legal framework, to avoid any inconsistency which may jeopardize the effectiveness of the Directive. Member States may however request assistance from the Cooperation Group, if they do not come up with an agreemen.[2]

Once the list of OESs established, it should be communicated to the European Commission that they monitor the correct application of the identification process of the OESs at national level. By 9 November 2018 and every two years after, the Member States are required to submit the following non-limitative information to the Commission:

> "*the national measures allowing for the identification of operators of essential services;*[3] *the list of essential services;*[4] *the number of identified OES for each sector referred to in Annex II and the relevance of those operators for the sector;*[5] *and, thresholds identified for determining the supply level by reference to the number of users relying on that service or to the importance of that particular OES.*"[6]

The criteria for the identification of the operators of essential services, as referred to in point (2) of Article 5, shall be as follows: "*(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service*". Concerning the latter, it is important to remind how the significant disruptive effect is determined. According to Article 6 of the NIS Directive,

> "*when determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors: (a) the number of users relying on the service provided by the entity concerned; (b) the dependency of other sectors referred to in Annex II on the service provided by that entity; (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; (d) the market share of that entity; (e) the geographic spread with regard to the area that could be affected by an incident; (f) the importance of the entity for maintaining a*

[1] Article 5 §4 of Directive 2016/1148

[2] Article 5 §4 and Recital (24) of Directive 2016/1148

[3] *Ibid,* Article 5 §7 (a)

[4] *Ibid,* Article 5 §7 (b)

[5] *Ibid,* Article 5 §7 (c)

[6] *Ibid,* Article 5 §7 (d)

sufficient level of the service, taking into account the availability of alternative means for the provision of that service. 2. To determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors".

Article 5, para. 7 of the NIS Directive provides that Member States should submit to the Commission by 9 November 2018 the information necessary to enable the Commission to assess the consistency of their approaches to the identification of OES. That information shall include at least:

"*(a) national measures allowing for the identification of operators of essential services*

(b) the list of services referred to in paragraph 3

(c) the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector

(d) thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service as referred to in point (a) of Article 6(1) or to the importance of that particular operator of essential services as referred to in point (f) of Article 6(1)".

While the list of services should serve as a reference point[1] for Member States, allowing for identification of operators of essential services, the essentiality and criticality criteria seem somewhat questionable to us. If the adoption of the Directive will make it possible to establish a common definition, through the adoption of this list of sectors / services, it would however remain divergent, as the principle of minimum harmonisation adopted by the Directive allows Member States to go beyond the scope of Annex II and to identify additional sectors and sub-sectors.

Thus, the number of services identified by each Member State as being covered by Annex II to the NIS Directive which has been communicated to the Commission[2] varies considerably from one Member State to another (**Table 11**).

Member States	***OES identified***	***Additional services***
AT	0	0
BE	0	0
BG	185	3

[1] Recital (23) of Directive 2016/1148

[2] European Commission Report to the European Parliament and The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, 28 October 2019, COM(2019) 546 final

CY	20	17
CZ	50	12
DE	573	12
DK	128	0
EE	137	6
EL	67	0
ES	132	18
FI	10 897	0
FR	127	20
HR	85	2
HU	42	0
IE	64	0
IT	553	0
LT	22	0
LU	49	0
LV	66	0
MT	36	2
NL	42	0
PL	142	0
PT	1 250	0
RO	86	0
SE	326	0
SI	0	2
SK	273	7

Table 11: *Number of services identified by each Member State*

Source: *Commission's report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services, COM(2019) 546 final*

As seen in the table above, the correlation between the size of a Member State and the number of services identified does not seem strong. Always according to the Commission data's, the variation of identified services across Member States, sectors and sub-sectors is justified by the lack of constituency between methodological approaches adopted by the countries. For example, in the rail sector, France has adressed a detailed and complete list of services essential to the functioning of rail transport, while Finland, Ireland, Poland have only selected a small subset of services. Thus, the total number of OES communicated to the Commission by Member States ranges from 20 to 10,897 with an average of 633 OES per Member State.

One could then have supposed that to avoid getting lost in long discussions on what should be understood by *essential* and *critical*, the Commission could have simply published a list of sectors/services that it hears as such. Moreover, this is what the Directive mentions in its recital (20): "*When assessing whether an entity provides a service which is essential for the maintenance of critical societal or economic activities, it is sufficient*

to examine whether that entity provides a service that is included in the list of essential services". In other words, it does not matter whether Member States can interpret Article 5 NIS Directive differently, as long as the 7 essential critical sectors / services are adopted as such.

The absence of communication of most data to the public makes it not easy to try to explain the methodological approaches operated by Member States. However, Member States have used different methodologies to identify OES within the acceptable range of NIS Directive. Indeed, following the adoption and transposition of Council Directive 2008/114[1] on the "*identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection*", ENISA published in 2014 a study on methodologies for the "*identification of Critical Information Infrastructure assets and services*"[2]. In that document, four maturity levels with regards to critical infrastructures II activities across Member States have been identified and categorised by an indicative state of the art: a) pure transposition of Directive 114/2008, b) identification of additional critical sectors, c) general methodological framework for identification of critical infrastructures assets, d) detailed methodological approach for identification of critical infrastructures assets with specific criticality criteria.

Reegarding the identification of critical services, two different approaches were assessed by ENISA in different Member States, the *state-driven approach*[3] and the *operator-driven approach*. In the first approach the leading role is assumed by the government agencies[4] that have the mandate to identify and protect critical infrastructures. While in the second one, the Member State identifies a list of operators[5] responsible for identifying the individual critical services and assets.

As a significant number of Member States showed a low level of maturity and lacked a structured approach, ENISA proposed the following reference list of critical sectors / services (**Appendix 3:** Types of essential sectors as defined by ENISA). This list presents important similarities with the list proposed by the NIS Directive.[6] Even if the additional sectors considered by certain Member States are not included in Annex II of the NIS directive, they certainly appear in the list proposed by ENISA in 2014. This reinforces -to a certain extent -the advisory role of ENISA on NIS. "*11 of the 28 Member States have identified essential services in sectors which do not fall within the scope of Annex II to the directive*", which represents close to 50% of Member

[1] OJ L 345, 23.12.2008, p. 75–82

[2] ENISA, Methodologies for the identification of Critical Information Infrastructure assets and services Guidelines for charting electronic data communication networks, (2014), available at https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport (accessed on March 11th, 2020)

[3] Estonia or Czech Republic.

[4] In most of the cases the responsible ministries.

[5] Called also 'vital operators.'

[6] Interview 5

States. For example, France has been able to identify the insurance, restoration and education services as essential sectors,[1] while Germany has included the nutrition sector.[2] Information infrastructures, financial services provided by entities not listed in Annex II and public services are the most widespread categories.

However, this seems to justify that, the adoption of Annex II was the subject of several debates at Council level during the adoption of the directive. Debates after which the national policies of Member States are likely to impact this list. Indeed, if the NIS Directive seems to leave to the Commission all the latitude regarding the definition of essential / critical sectors / activity, the key national role played by Member States in the definition of critical infrastructure sectors, as well as the existing classification for these sectors should be more considered. It seems therefore that a definition of these criteria to be able to justify the choice of these sectors / activities would have been welcomed. The same situation is met on the definition of the third and last criterion the *significant disruptive effect*, for which an entire article is dedicated.

Article 6 NIS Directive defines an incident as having a significant disruptive effect when "*the continuity of the provided operations and services are negatively affected*". According to then to Article6 §1 of the NIS Directive, the severity of the incidents should be judged by:

> "*(a) the number of users relying on the service provided by the entity concerned; (b) The dependency of other sectors referred to in Annex II on the service provided by that entity; (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; (d) the market share of that entity; (e) the geographic spread with regard to the area that could be affected by an incident; and (f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service*."

Further to the above-mentioned general criteria, Member States should also define sector-specific factors. For accomplishing their task, Member States may also consult with stakeholders of the sectors indicated by Annex II of the Directive in order to consider sector-specific factors. Examples of such criteria like the volume and number and types of users supplied are given in NIS Directive preamble[3].

Coherent approach on the application of the OES definition criteria's falls under the Member States' responsibility.[4] Coherent application among Member States imports, as it should help to reduce the risks of cross-border dependencies, guarantee fair conditions of competition for operators on the internal market, reduce

[1] Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique

[2] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)

[3] Recital (28) of Directive 2016/1148

[4] *Ibid,* Recital (19): 'In order to ensure a consistent approach, the definition of operator of essential services should be coherently applied by all Member States.'

the risk of divergent interpretations of the directive and finally and develop a global overview of the degree of cyber resilience across the Union.[1] The consistent approach criterion doesn't appear in the body of the directive but in a recital to its preamble. However, in a CJEU judgement *Meta Fackler KG v Bundesrepublik Deutschland*[2] of May 12th 2005, the Court was able to confirm that it is settled case-law that "*the preamble to a directive would not have binding legal force (…)*"[3]. The recitals have thus the purpose of concisely motivating the essential provisions of the directive and they do not have any normative nature or formulate political vows.

The voluntary extension of the application of the NIS Directive to other sectors raised concerns among the Commission[4] on whether the scope of its Annex II is well suited to fulfil the objective of protecting all Union operators which are of critical importance to society and the economy. Member States used their prior experience as a point of reference and incorporated specificities related to the NIS Directive into existing methodologies, with differences falling in the following main categories[5] : (a) use of thresholds; (b) degree of centralisation; and (c) authorities in charge of the identification and assessment of network and information systems dependence (**Table 12**).

Categories	*Criteria*
Use of thresholds[6]	• a single quantitative factor (e.g., number of users relying on a service) to determine whether an entity is to be considered an OES within a certain service • a larger set of quantitative factors (e.g., number of users relying on a service plus market share), • a combination of quantitative and qualitative factors.[7]
Degree of centralization	• delegation of the decision making as regards various elements of the identification process to sectoral authorities (ministries, agencies etc.) • sectoral authorities usually have a deeper understanding of the sectors than the lead authorities.

[1] European Commission Report to the European Parliament and The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, 28 October 2019, COM(2019) 546 final

[2] Case C-444/03, *Meta Fackler KG v Bundesrepublik Deutschland*, ECLI:EU:C:2005:288

[3] Case C-162/97, *Criminal proceedings v Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn*, ECLI:EU:C:1998:554

[4] European Commission Report to the European Parliament and The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, 28 October 2019, COM(2019) 546 final

[5] *Ibid*.

[6] Thresholds of the BSI-Kritis Ordinance, (2018), available at https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/bsi-kritis-ordiance-poster.html (accessed on March 11th, 2020)

[7] Complex mix of thresholds, which can have negative impact on overall OES identification consistency.

Authorities in charge of identification	• **Top-down**: public authorities conduct the identification process (*state-driven approach*) • **Bottom-up**: market operators are called upon to verify by themselves whether they meet the requirements as operators of essential services (*operator-driven approach*) • In most cases the identification process is top-down. However, in practice authorities often partly rely on certain self-assessment elements, such as questionnaires to be filled out by potential OES (e.g., UK[1])
Assessment of NIS dependence	• Considering dependence on network and information systems to be a given in today's digital economy. • Some authorities chose more elaborate practices, for example by conducting detailed assessments or by asking operators to self-evaluate the degree of their dependence

Table 12: *OES identification criteria used by Member States*

Table made by author based on Commission's report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services, COM(2019) 546 final

Thus, we might understand that the existence of variable identification methodologies across the EU might lead to a fragmented approach on the Directive's scope. This therefore reinforces the idea that setting minimum identification criteria and leaving thus more freedom of movement to Member States may jeopardise the harmonising outcome of the NIS Directive. The criteria for identifying essential service operators set out in Article 5 of the NIS Directive may leave room for subjectivity in our view, except perhaps for the significant disruptive effect. It is therefore logical that divergent national policies can be asserted in the absence of a precise common definition. Moreover, uneven application of article 5 §2 NIS Directive provision could lead, regarding the application of the lex specialis principle, to the identification of OES where sector-specific rules apply. As the requirement of *lex specialis derogat legi* has been the subject of several debates in the Council of the Union, it might be interesting to devote a few words to this.

[1] UK Department for Digital, Culture, Media and Sport, Security of Network and Information Systems: Government response to public consultation(2018), available at https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive (accessed on March 15th, 2020)

2. Cross-border consultation

There is no formally established process to facilitate the dialogue among the Member States for the purposes of article 5 §4 NIS Directive. While Member States without any prior experience in the same matter might face difficulties in implementing this article, other EU procedures with similar objectives e.g., the ECI Directive[1] might also be considered. To provide Member States with comprehensive guidelines, relating to the identification of OES providing service in more than one Member State, NIS Cooperation Group published a reference document on modalities of the consultation process in cases with cross-border impact (**Figure 2**).[2]

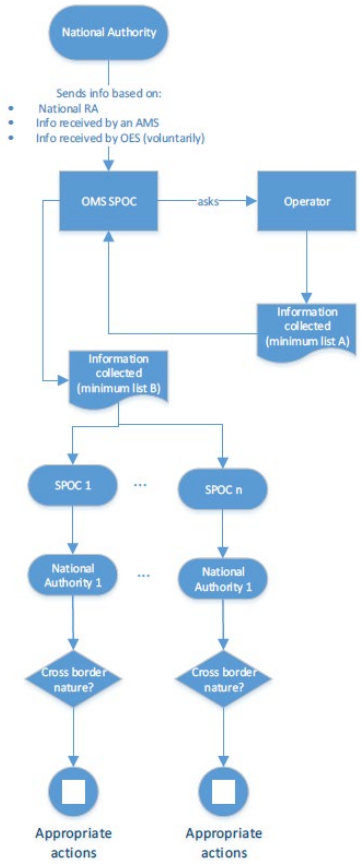


Figure 2: *Cross-border consultation flow diagram*

Source: *Cooperation Group (2018), Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact.*[3]

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance), OJ L 345, 23.12.2008, p. 75–82

[2] Cooperation Group, Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact, CG Publication 07/2018, available at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53661 (accessed on March 11th, 2020)

[3] Available at https://www.europeansources.info/corporate-author/nis-cooperation-group-nis-cg/ (accessed on January 3rd, 2022).

Thus, the risk that operators will be forced to face a multitude of different regulatory requirements or to disadvantage themselves compared to other less regulated operators on the market, seems obvious to us. However, the Commission has identified five reasons justifying why the consultation procedure is so far not being used as intended: (a) a longer identification time than expected, (b) the lack of secure channels to transfer information, (c) the considerable number of existing cross-border dependencies, (d) the lack of a common understanding of goals and scope of the cross-border consultation exercise, (e) absence of multilateral dialogue.

The considerable number of existing cross-border dependencies (and interdependencies) is of particular importance, as cross-border impact may have a cascading effect on different sectors as well as on services across Member States.[1] Cross-border (inter)dependencies refers to "*services' (inter)dependencies between OES themselves, between DSPs themselves, and between OES and DSPs operating in two or more different Member States*"[2]. Thus, connectivity of sectors/services operating in different countries underlies attacks infecting ICT systems and propagating by infecting connected resources or systems. The *Trans-European Networks (T-EN)* case may be an interesting example.

The Lisbon Treaty seek to give the EU a better capacity to act in priority areas for the EU and marked a great expansion in its internal policies.[3] One of these was the energy sector for which, a separate chapter on energy has been included in the text of the Union Treaty for the first time since the founding treaties. We can then say that this is a real qualitative upgrade of the importance of energy policy within the EU. Furthermore, the Lisbon Treaty has strengthened the EU's presence on the international scene by pooling available foreign policy instruments and giving it "*the capacity to be a subject of international law, which has rights and international obligations*", such as "*the ability to invoke or not to invoke rules of international law*". However, the right of each Member State to determine the conditions for the exploitation of its energy resources, its choice between different sources of energy and the general structure of its energy supply cannot be taken away and no specific mechanism of aligning national interests to those of the EU in energy are foreseen. Therefore, Member States and more particularly, those which depend on energy resources from third countries, adopt an interpretation of energy security according to their own energy situation and their degree of vulnerability to possible supply disruptions.

However, the last decades of the 21st century marked an important development of international trade in the energy sector and a transition from the oil era to a more diversified energy mix. Energy security is no longer connected only with the fluidity of oil supplies. More specifically, the increased use of natural gas links energy security with the issue of managing complex natural gas transportation and storage infrastructure. However, the

[1] Interview 8

[2] ENISA, Good practices on interdependencies between OES and DSPs, 30 November 2018, available at https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps (accessed on September 9th, 2021)

[3] See L. V. Langenhove and D. Marchesi, Lisbon Treaty, and the emergence of Third Generation Regional Integration, (2008) 9 *Jean Monnet/Robert Shuman Paper Series* 8, 12

management and protection of infrastructure networks is the main characteristic of the modern concept of energy security, and it does not only concern gas pipeline networks but also nuclear energy networks, hydroelectric dams, and electrical networks emanating from renewable energy resources (solar farms, wind energy).[1] The establishment of trans-European networks in the energy sector (TEN-E), in addition to those in the transport and communications sectors, was contained in the provisions of the Amsterdam Treaty to contribute to the completion of the internal market and sustainable development.

The Community concept of trans-European networks (TENs) appeared at the end of the 1980s with a view to the completion of the single market. The TENs were created in the fields of transport, energy and telecommunications, networks necessary to ensure the free movement of goods and people, as well as European cohesion. It was the Maastricht Treaty which enshrined in Community law Community competence for "*the encouragement of the establishment and development of trans-European networks*" and devoted a Title XII to it,[2] the provisions of which were taken up by the Treaty of Lisbon in its Title XVI.[3]

To achieve these objectives, the Union decides, by the ordinary legislative procedure of the guidelines covering the objectives, the priorities as well as the broad outlines of actions and projects of common interest, implements actions to ensure the interoperability of networks, in particular in the field of harmonisation of technical standards and supports projects of common interest of the Member States, in particular by feasibility studies, loan guarantees or interest rate subsidies or by financing from Cohesion fund (**Figure 3**). Union action must consider the potential economic viability of projects.[4]

[1] Interview 6

[2] Articles 129B and 129C of the Maastricht Treaty.

[3] Article 170 TFEU (ex-Article 154 TEC): '1. To help achieve the objectives referred to in Articles 26 and 174 and to enable citizens of the Union, economic operators and regional and local communities to derive full benefit from the setting-up of an area without internal frontiers, the Union shall contribute to the establishment and development of trans-European networks in the areas of transport, telecommunications and energy infrastructures.

2. Within the framework of a system of open and competitive markets, action by the Union shall aim at promoting the interconnection and interoperability of national networks as well as access to such networks. It shall take account in particular of the need to link island, landlocked and peripheral regions with the central regions of the Union.'

[4] Art. 171 TFEU.

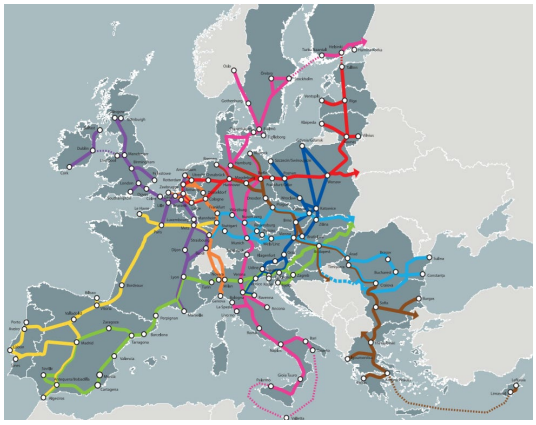


Figure 3: *Ten-T Core Networks Corridors*

Source: *European Commission*[1]

In terms of transport, the implementation of the current policy is based on the new TEN-T infrastructure guidelines, which define 30 priority projects. Current European actions focus on nine multimodal transport corridors, considered to be the most strategic networks, and two horizontal priorities.[2] Each must include at least three Member States and cross at least two borders. Investments are directed in priority for the construction of cross-border links (including with third countries: Switzerland, Norway, Turkey, countries of the Western Balkans) and multimodal connections, the elimination of bottlenecks and the setting up of interoperability. In addition to this basic network, the completion of which is planned for 2030, the creation of a wider European network enabling all European regions to be connected by 2050 has also been planned.

In terms of energy, the European Council adopted the objective of an integrated European network enabling electricity and gas to be supplied in the event of a supply crisis in a country and in the event of intermittent supply by renewable energies (wind and solar), as well as the storage of gas and liquefied natural gas and the transport, extraction and conservation of coal and the transport of oil in certain regions of the CEECs. Thus, the interconnection of the grid systems plays a key role in all the subsectors of the energy sector.[3] According to the European Network of Electricity Transmission Operators, Europe must build more than 45,000 km of new lines only to meet the development objectives of renewable energies and 40,000 km of new lines to integrate the internal market and ensure security of supply. The list of projects of common interest is revised every two years and each has three and a half years to prepare the planning. These projects must also comply with environmental requirements. Projects can be financed even if their commercial viability is not guaranteed provided that the social externalities are significant, for example in terms of security of supply. Thus, the energy sector may have

[1] Retrieved from https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/site/en/maps.html (accessed on March 17th, 2020)

[2] The European rail traffic management system and motorways of the sea.

[3] Interview 6

dependencies with financial market infrastructures and digital infrastructures even across multiple Member States. Even so, unlike the transport and communications sectors, the energy sector has made no significant progress.

In the face of such a degree of interconnectivity, the NIS Directive requires only minimum technical harmonisation in NIS security issues across the Union, just like a railway company which travels between two or three Member States and interacts with various infrastructures (e.g., approach beacons). Its appointment as an OES by two, or even three different Member States would imply a submission to a divergent degree of obligations, since Member States are forced to impose only a threshold of security requirements and incident notification obligations retaining the right to go further beyond it.

B. Security and notification obligations (Article14 NIS)

The security requirements for OESs are achieved by focusing on the adoption of appropriate and proportionate security measures by the OES (**1**); as well as on the notification of incidents with a significant impact on the provision of the essential services by the Member States (**2**).

1. The adoption of appropriate and proportionate security measures

Following article 14 §1 NIS Directive, OESs are required "*to assess the effectiveness of the existing technical and organisational controls in order to evaluate the level of their preparedness, regarding the security of the networks and information systems they use for the provided services*"[1]. Bearing in mind "*the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed*"[2]. However, the Directive does not indicate what type of methodology to adopt when performing relevant risk assessments, nor the form of technology to be used. Thus, their content is discussed at EU level within the NIS Cooperation Group. In its 2018 Reference document on security measures for OES[3], the Cooperation Group agreed therefore that, a common consensual basis should be identified as Member States may wish either to use

[1] Article 14 §1 of Directive 2016/1148

[2] *Ibid*

[3] NIS Cooperation Group, 'Reference document on security measures for OES', CG Publication 01/2018, available at https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf (accessed on March 18th, 2020)

"*different sources or control frameworks for security measures from European or International standards (e.g., ISO 27.000)*[1] *to existing or new sets of security measures*[2]*; or aim at different levels of granularity and prescription regarding specific cybersecurity requirements, objectives and controls; or lastly, aim to only establish cross-sectoral measures or choose to address individual sector specificities as well (with sector-specific measures).*"

The appropriateness and the proportionality of technical and organisational security measures are hard to define, even more so when this condition applies to Member States. Let us recall that proportionality is a general principle of the Union's law under which,

"*the content and the form of Union action do not go beyond what is necessary to achieve the objectives of the Treaties".*[3] *According to settled case law of the CJEU, "the principle of proportionality requires that the acts of the institutions of the Union are capable of achieving the legitimate objectives pursued by the legislation in question and do not go beyond the limits of what is appropriate and necessary to achieving these goals.*"[4]

Consequently, it "*limits the authorities in the exercise of their powers by requiring them to strike a balance between the means used and the objective sought (or the result achieved)*"[5]. The term of proportionality must be clearly distinguished from that of appropriateness, which requires carrying out a combined factual assessment of the effectiveness of the measure for the purposes pursued and to determine whether this measure is less intrusive compared to other means of achieving the same goal. It is, however, interesting to note that while the Directive uses the term *appropriateness*, it is however translated into French by the term 'necessity'. This will eventually allow the French domestic judge to easily appreciate the limits of what is *necessary and proportionate* to the objective set, while in German or Italian the term seems to have been correctly translated. This therefore makes one wonder about the uniform application of the requirements of the NIS Directive vis-à-vis the terminological differences used.

It is therefore possible that the Union judge will be asked about the limits of measures to be taken by the OES. To what extent will a security measure be considered appropriate and proportional to the risk posed? It is difficult to precisely depict. If 14§1 and 14§2 NIS Directive provisions leave enough legroom for Member

[1] Article 19 of Directive 2016/1148: *Encourage the use of European and internationally accepted standards and specifications relevant to the security of Network and Information Systems*

[2] E.g., France's cybersecurity measures for OES, Germany's IT-Grundschutz, Spain's National Security Framework, etc.)

[3] Article 5 §4 TUE.

[4] Case C-62/14, *Peter Gauweiler and Others v Deutscher Bundestag*, OJ C 279, 24.8.2015, p. 12–13

[5] Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen*, ECLI:EU:C:2010:662

States to adopt different security approaches, it is possible to set the following principles following Cooperation Group guidelines (**Table 13**).[1]

Effective	*In view significantly increasing the cybersecurity of OES, in relation to the current and foreseen threat landscape.*
Tailored	*In view of putting OES' efforts on measures having the most impact on their cybersecurity and avoid unnecessary effort and duplication.*
Compatible	*In view of addressing, in the short term, basic and common security vulnerabilities of OES despite their sectors, which may in the meantime be complemented with sector specific security measures*
Concrete	*To ensure that the security measures are actually implemented by OES and actually contribute to reinforcing their cybersecurity.*
Verifiable	*To ensure that operators may provide their national NIS competent authority(ies) with "evidence of the effective implementation of security policies, such as results of a security audit carried out by the competent authority or a qualified auditor"[2].*
Inclusive	*To encompass all security domains which may contribute to reinforcing the cybersecurity of OES, including physical security of information systems.*
Cost-benefit balanced	*To ensure efficient security measures, with respect to the security of essential services to the economy and the society, while taking into account their cost for OES'.*

Table 13: *Security measures' general principles*

Table made by author based on NIS Cooperation Group's ' reference document on security measures for Operators of Essential Services'

Thus, a culture of risk management should be "*promoted and developed through appropriate regulatory requirements and voluntary industry practices*"[3]. The selected management risk approach should maintain "*the character of prevention, reaction and limitation of impact over the disruption of the provided essential, to the society and economy, services*"[4]. Therefore, the proposed security measures adopted by the OES should consider the following five functions: Identify; Protect; Detect; Respond; and Recover (**Figure 4**); in the following four domains: (a) Governance and Ecosystem, (b) Protection, (c) Defence and (d) Resilience. A summarised checklist is proposed in **Appendix 4**: OES Security measures Checklist**.**

[1] NIS Cooperation Group, 'Reference document on security measures for Operators of Essential Services', CG Publication 01/2018, available at https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf (accessed on September 9th, 2021)

[2] Article 15 §1 and §2 of Directive 2016/1148

[3] *Ibid,* Recital 44

[4] Interview 6

Figure 4: *OES security measures framework infographic*

Source: *https://www.ncsc.gov.ie/*

2. Notification of incidents with a significant impact

Following article 14 §3 NIS Directive, OESs are obliged to report incidents that fall under the scope of the NIS Directive. Any incident having a *significant impact* on the continuity of the service provided, must be notified "*without undue delay*" to the NCA or national CSIRT. For a clear understanding of this provision, two notions need clarifications: the incident significant impact and the undue delay notification.

Within the meaning of Article 4 NIS Directive, an incident represents "*any event having an actual adverse effect on the security of network and information systems*". If the term 'adverse reaction' is not defined among the provisions of the NIS Directive, it is however possible to interpret the general meaning of the words as an impediment, a nuisance, and an unfavourable development. In order to determine the significance of the impact of an incident, NIS Directive establishes the following non-limitative parameters to be taken into account: "*(a) the number of users affected by the disruption of the essential service; (b) the duration of the incident and (c) the geographical spread with regard to the area affected by the incident*"[1]. Such a list of relevant parameters might be completed by the provisions of art. 6 §1 NIS Directive, referring to factors to be used when determining the *significance of a disruptive effect* (**Table 14**).

PARAMETERS	DEFINITION

[1] Article 14 §4 of Directive 2016/1148

The number of users affected by the disruption of the essential service	*The number of affected natural persons and legal entities with whom a contract for the provision of the service has been concluded.*[1]
The duration of the incident (NIS downtime)	*The period of time when an essential service offered by OES is unavailable due to impairment affecting the confidentiality, integrity, availability, or authenticity of the underlying computer system that supports the provision of the service.*[2]
The geographical spread	*Member States or regions within the EU where users were affected by impairments of the essential service affected.*[3]
The dependency of other oes sectors on the service provided by the affected entity	*The level of reliance of other OES on essential service provided by one OES.)*
The impact that incidents have, in terms of degree and duration, on economic and societal activities or public safety	*The detrimental effects of an incident on the activities of users that generate either economic or social damages or endanger public safety.*[4]
The market share of that entity	*The percentage of a market (defined in terms of either units or revenue) accounted for by a specific entity.*

Table 14: *Parameters used to measure impact of incidents*

Table made by author

Concerning the notification timeline, the 'undue delay' condition might be considered as the "sooner" the operator is aware of the triggering event of the significant incident. However, most of the Member States seem to use a two phase or three phase reporting[5]. Even if the NIS Directive is not laid out in Article 14, as proposed by the European Data Protection Supervisor, "*the format of the notification, including the types of personal data that should be notified and whether, and to which extent, the notification and its supporting documents will include details of personal data affected by a specific security incident (such as IP addresses)*" [6].

Following Cooperation group survey[7], the OES is invited to notify in, as soon as possible, using one of the following methods: phone call (e.g., POTS or IP-based voice/video calls), plain email, email with a form as an attachment (e.g., PDF), online form (e.g., HTML over SSL/TLS), web service API (e.g., XML) or plain paper.

[1] Particularities per industry type should be considered (e.g., Health sector: number of patients treated within the affected clinic/hospital during the time of the incident, or the number of population served within the region).

[2] The duration of the incident should be measured (and consequently reported) as starting from the moment when the provision of the service was affected up until the time of full recovery.

[3] Reporting geographical spread has to be adapted to specificities within the sectors.

[4] Measuring the real impact on economic and societal activities requires many resources and has high probability of failing due to inconsistent or incomplete data.

[5] A preliminary reporting, an intermediate reporting, and a full reporting.

[6] OJ C 32, 4.2.2014, p. 19–22

[7] NIS Cooperation Group, Reference document on security measures for Operators of Essential Services, CG Publication 01/2018, available at https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf (accessed on September 9th, 2021)

Member States may also apply following technical and security measures on different methods of notification (**Table 15**).

Encryption	Protecting confidentiality of the notification.
Authentication	Avoiding fake notifications.
Confirmation	Confirming that the notification was received by the national competent authority and/or CSIRT

Table 15: *Technical and security measures applied on notification methods*

Table made by author based on NIS Cooperation Group'w reference document on security measures for Operators of Essential Services

After submitting the information, the OES receives a ticket/case number, confirming that the notification was processed properly. The national authority forwards the notification to the CSIRT alerting them that that there is a situation where their support might be needed. The national SPOC also notifies SPOCs abroad if needed. The CSIRT assesses the situation and engages with the operator asking if support is needed in handling the incident. The CSIRT identifies useful threat information for sharing with peers and/or constituents. Ex-post, after the incident is resolved, the operator must send a complete incident report to the national authority, a longer, more complete, online form. This must be done within 3 weeks. A part of this report is used for annual summary reporting to the NIS Cooperation group. Every year the national authority uses these reports to publish a full overview of common root causes, total number of incidents, their nature, their impact, etc.

There is the possibility the same services of OESs are also provided to the other Member States. Thus, notifications shall include information enabling the competent authority or the CSIRT to determine any large-scale incidents. However, in its 2016 Communication on "*Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*"[1] the European Commission encouraged Member States to make the most out of the NIS Directive cooperation mechanisms and to enhance cross-border cooperation related to preparedness for a large-scale cyber incident. The Commission's Recommendation of September 13th, 2017, also known as the "*blueprint*", invited Member States to "*cooperate in establishing a common taxonomy and template for situational reports*" to describe the technical causes and impacts of cybersecurity incidents during crises[2]. On June 26th, 2018, the General Affairs Council in its conclusions on "*EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises*" welcomed a common

[1] European Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, 5 July 2016, COM/2016/0410 final

[2] OJ L 239, 19.9.2017

taxonomy for cybersecurity incidents developed by NIS Cooperation Group (**Appendix 5:** Common taxonomy for cybersecurity incidents' notification).[1]

Sometimes the extent of the cyber-attack may require communicating the incident to the public (**Figure 5**). In such a situation, Member States may choose either the NCA either the CSIRT, "*after having consulted the notifying operator of essential services, to communicate the individual incident to the public, or the notifying operator itself, in order to raise public awareness on preventing or dealing with an ongoing incident*"[2]. The secretariat of the CSIRTs network may publish general information on major incidents that have occurred across the Union where it is made available to the public[3] and; "*where information is considered to be confidential in accordance with Union and national rules on business confidentiality, such confidentiality should be ensured when carrying out the activities and fulfilling the objectives set by this Directive*"[4].

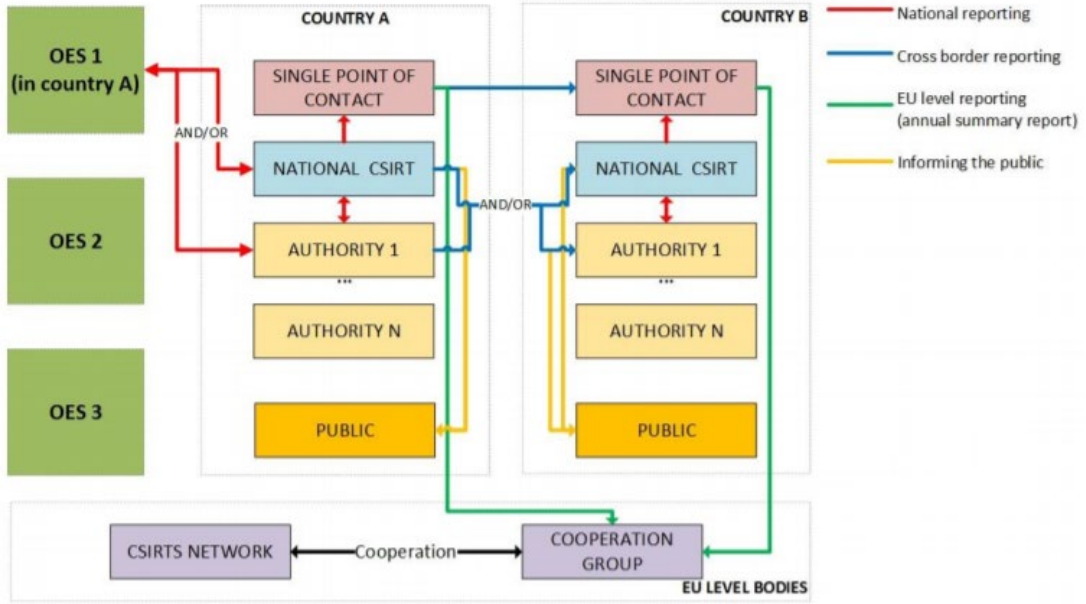


Figure 5: *Overview of the incident reporting process for OESs*

Source: *NIS Cooperation Group*[5]

[1] Council Conclusions on 'EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises', 26 June 2018, 10086/18

[2] *Ibid*, Article 14 §6

[3] *Ibid*, Recital 40

[4] *Ibid*, Recital 41

[5] NIS Cooperation Group, 'Reference document on Incident Notification for Operators of Essential Services, Circumstances of notification', CG Publication, February 2018, available at https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_incident_reporting_00A3C6D5-9BDB-23AA-240AF504DA77F0A6_53644.pdf (accessed on March 19th, 2020)

§2. Digital Service Providers' Security Requirements and Incident Notification

Digital service providers are the second category of entities falling within the scope of the NIS Directive. DSPs include any legal person that provides a digital service and more specifically an online marketplace, an online search engine, or a cloud computing service. Their regulation is justified since many businesses depend on these providers for the provision of their own services. Consequently, a disruption of the digital service could have an impact on key economic and societal activities in the Union.

In the WP TELE document 12126/15 of September 21st, 2015, Council Presidency stressed that "*there seems to be a general understanding that the approach to DSPs should be 'lighter' than the one on operators providing essential services*". Thus, Member States should be not allowed 'to impose any further security or notification requirements on DSPs, besides the ones foreseen in the directive'[1] and jurisdiction should be based "*on the criteria of main establishment of a DSP within only one Member State*"[2]. When provided with evidence that a digital service provider does not meet the requirements laid down in Article 16, an ex-post supervision is allowed from the competent authority[3]. However, the minimum-security requirements for DSPs "*should be lighter than those of the OES, and they should remain free to take the measures that they deem appropriate*"[4].

In the Presidency's view, there were two elements to the *light touch approach* that should be analysed separately: which DSPs within the types of DSPs retained in Annex III should be covered (**A**) and which requirements should be applicable to those DSPs that are covered (**B**). We will adopt the same presentation on treating the requirements for Member States concerning the DSP notification (**C**).

A. Identification process, adopting a differentiated approach

In its 2017 consultation[5] on how the Security of the NIS Directive will apply to DSPs in the UK, under half (45%) of the respondents to the Government's DSP consultation said they were not "*readily able*" to identify themselves as DSPs, the main area of difficulty being related to the definition of cloud service providers. As mentioned above, the NIS Directive adopted a differentiated approach to the OES and DSP's identification (**1**),

[1] Article 16 §10 of Directive 2016/1148

[2] Article 18 of Directive 2016/1148

[3] *Ibid,* Article 17 §1

[4] This interpretation of the light-touch approach was presented by Commission's representatives, during ENISA's Network and Information Security Workshop in Bratislava, 17-18.10.2016.

[5] Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785375/DSP_Targeted_Consultation__Final_.pdf (accessed on March 20th, 2020)

by applying to all digital service providers within its scope due to their cross-border nature to treat them "*in a uniform way across the Union, in a manner proportionate to their nature and the degree of risk which they might face*"[1] (**2**).

1. DSPs identification elements, defining a differentiated approach

The NIS directive does not explicitly define what should be understood as a DSP.[2] It is possible however to find a definition of what should be understood as a service in the context of an Information Society, throughout Article 1 §1 (b) of Directive 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification)[3]:

> "*Service refers to a service provided from a distance and by using electronic means; at the request of the person concerned, to receive the service; against remuneration. For the purposes of this definition: (i) 'at a distance' means that the service is provided without the parties being simultaneously present; (ii) 'by electronic means' means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means; (iii) 'at the individual request of a recipient of services' means that the service is provided through the transmission of data on individual request*."

The question that seems interesting to examine at this point is how the Directive links the definition of Directive 2015/1535 to "*information society services*" and digital services provider. However, this link finds its justification in trialogues between the Commission, the Council, and the European Parliament. Initially the Commission proposal on the NIS Directive mentioned in recital 24 that, I quote,

> "*Those obligations should be extended beyond the electronic communications sector to key providers of information society services, (...), which underpin downstream information society services or on-line activities, such as e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, application stores. Disruption of these enabling information society services prevents the provision of other information society services which rely on them as key inputs. Software developers and hardware manufacturers are not providers of information society services and are therefore excluded*."

[1] Recital 57 of Directive 2016/1148

[2] *Ibid,* Article 4 §5

[3] OJ L 241, 17.9.2015, p. 1–15

However, some Member States argued in favour of excluding *internet enablers* and *internet services*,[1] while others proposed deleting Annex II from the Commission's initial proposal. Within the framework of the WP TELE of 05 May 2015, the Presidency of the Union reported on the results of the third trialogue, stating that the EP had clearly indicated that it could accept the extension of the scope to *internet enablers* only under the following conditions:

- At least one sector in Annex II has been indicated to be covered in its entirety as the EP outlined
- The 5 outstanding issues related to the inclusion of internet enablers are resolved:
- A differing justification for inclusion of internet enablers as they lack criticality in a stricter sense
- definitions of terms involved (apart from on-line marketplace as defined in the ODR regulation)
- Legal certainty on the question of territoriality and enforcement,
- Practical concerns related to the intrinsically cross-border nature of services (e.g., notification)
- Possible overlap on the obligations imposed on internet enablers and stemming from other pieces of legislation coming under possible review, so called telecoms framework.

It should be noted that the Legal Service of the Council had expressed strong reservations as to the justification for the selection of a sector, while the Commission had supported the European Parliament's proposal for *internet enablers*, mentioning that it would present its respective proposals in the second week of May 2015. Following the understanding reached with the European Parliament at the fourth informal trilogue of 29 June 2015, the Luxembourg Presidency intends to proceed to reflect the agreed principles in relation to the NIS Directive, into concrete legal provisions. The European Parliament has repeatedly confirmed its preference for such a differentiated treatment of digital service platforms including through a separate chapter and Annex dedicated to those service providers. In view of this, the Presidency proposed the following drafting:

> Article 3(8)(a)(new) : "*Digital Service Platform" means any natural or legal person that provides an information society service within the meaning of point (2) of Article 1 of Directive 98/34/EC and the type of which is listed in Annex III (…).*"[2]

[1] UK, Sweden, Denmark, Poland, Netherlands, Czechia, and Latvia.

[2] Council, 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - Proposed approach to digital service platforms, 31 July 2015, 11244/15 LIMITE.

All platforms meeting the definition would be covered by the Directive thus ensuring a harmonised approach to those platforms across the Union. Under this approach it is therefore fundamentally important that the definitions of digital service platforms are set out clearly in the Directive. However, on 21 September 2015 during a meeting of the Working Party on Telecommunications and Information Society (WP-TELE)[1] some delegations pointed out the possible confusion of the term "digital service platform". To avoid any confusion, the Presidency suggested replacing the term "*digital service platform*" with "*digital service provider*". Some delegations suggested that natural persons should be excluded from the definition of DSP and other delegations proposed to stress the *enabling* element of DSPs.

Sweden proposed the deletion of the definition of "*Cloud computing service provider*", while in the definition of "*social network*", it supported Spain's proposal to add the term *enabling* this network. The UK says it will send written comments on all definitions, although it supports the definition of *Cloud computing service provider* because, as the footnote indicates, it comes from the corresponding chat with the United States. Estonia opposed the addition of *social networks*, while Germany and Spain requested that the term *individual profile* be deleted from this definition as limitative, since it excludes companies. The Czech Republic thanked the Presidency for excluding, according to its own interpretation, the term *application stores*. Greece, Spain, and Slovenia objected to the Czech Republic's interpretation and pointed out that this was wrong, because in the Presidency text it is stated that "*the definition of application stores has been removed as the Presidency considers that it is covered by the definition of online marketplace and requested that this be clarified in a recital*". France has requested the addition of "*web hosts*", a proposal supported by Germany and Austria. The UK, Sweden, the Czech Republic, Ireland, and Poland were radically opposed to the French proposal. The Commission supported the Presidency's proposals as they stood, although it agreed to add a recital on the application stores. The following definitions were thus removed from the consolidated Council proposal:

- Information society service mean service within the meaning of point (2) of Article 1 of Directive 98/34/EC;'

- Provider of information society services which enable the provision of other information society services, a non-exhaustive list of which is set out in Annex II;

[1] Council of the European Union (2015), Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - drafting suggestions on 'internet enablers', 12126/15 LIMITE.

But it was after the 6th trialogue of February 7th 2015, that the presidency published a final consolidated proposal[1] in which we find the definition of DSP and the categories falling within its scope as it appears today in the NIS directive:

> • '"digital service ~~provider~~" means ~~any legal person that provides an information society~~ a service within the meaning of point ~~2~~ (b) of Article 1 of Directive ~~98/34/EC~~ 2015/1535 ~~offered to the public at large or to businesses at large~~ which is of a type listed in Annex III.1
>
> • "Online marketplace" is a digital service that allows consumers and/or traders as defined respectively in Article 4(1)(a) and 4(1)(b) of Directive 2013/11/EU to conclude online sales and service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace.
>
> • "Online search engine" is a digital service that allows users to perform searches of in principle all websites or ~~a geographical subset thereof~~, <u>websites in a particular language</u> on the basis of a query on any subject in the form of a keyword, phrase, or other input; and returns links in which information related to the requested content can be found.
>
> • "Cloud computing service" is a digital service that enables access to a scalable and elastic pool of shareable computing resources.'

We can therefore understand that national domestic policies can strongly influence the debate on the content of the directive, by attaching an interest on the wording used. The same applies to the scope of the directive to DSP's as well.

2. NIS Directive scope and mandatory categories

Although the NIS Directive does not require Member States to identify[2] which DSPs should be set under its scope, it defines nevertheless certain categories[3] of DSPs: (a) Online marketplace, (b) Online search engine provider and (c) cloud computing service provider.

[1] Council of the European Union (2015), Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - Examination of the final compromise text in view to agreement, 15229/15 LIMITE.

[2] Recital 57 of Directive 2016/1148

[3] *Ibid,* Annex III

Article 4§17 NIS Directive defines online marketplaces as services that "*allow consumers and traders to conclude online sales or service contracts with traders and is the final destination for the conclusion of those contracts*"[1]. Intermediaries and price comparison services are excluded.[2] The term online market service provider the Directive refers therefore to the services that facilitate the economic activity of an entity with the use of electronic means, such as "*the state of processing transactions and aggregation of information regarding buyers, suppliers and products; the provision of a searching facility for appropriate products; the provision of products; the provision of special knowledge of transactions; and the provision of a matching capability between buyers and sellers*"[3]. Concerning the Online search engine provider, it allows "*users to search on all websites, independent of content and language*"[4]. However, provided services related to "*search and price comparisons are excluded*"[5].

Lastly, article 4 §19 NIS Directive defines cloud computing service as meaning "*a digital service that enables access to a scalable and elastic pool of shareable computing re-sources*". The following three main types of cloud computing provided are covered by the NIS Directive: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a service (SaaS).[6] However, micro-, and small enterprises[7] in these sectors were exempted from the NIS Directive's scope. Indeed, different suggestions were made within the Council's debates on excluding following services from the application of the Directive: services not offered to public, natural persons, micro-enterprises, small enterprises, and medium-sized enterprises. It seems that most delegations favoured the exclusion of micro-enterprises, while the issue of small and medium-sized enterprises (hereafter SME's) sparked debate. The UK, Sweden, Denmark, Poland, Ireland, and Latvia proposed the exclusion of SMEs, while France, the Commission and Germany were opposed. France declared that except for SMEs, 97% of the market would be excluded. Greece has formulated a positive scrutiny reserve for their exclusion and highlighted the issue of *start-up's*, which should not be included in the scope of the directive. The Greek proposal was supported by Estonia. Finally, reservations were expressed regarding natural persons,

[1] OJ L 165, 18.6.2013, p. 63–79, Article 4 §1 (b): 'trader' means any natural persons, or any legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession

[2] Recital 15 of Directive 2016/1148

[3] European Commission, 'Communication to the European Parliament and the Council, Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', 13 September 2017, COM(2017) 476/2 final.

[4] Article 4 § 18 of Directive 2016/1148

[5] *Ibid,* Recital 16

[6] European Commission, 'Communication to the European Parliament and the Council, Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', 13 September 2017, COM(2017) 476/2 final.

[7] Article 16 §11 of Directive 2016/1148: 'Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC (19).'

although the majority of Member States expressed themselves in favour of their exclusion or the addition of a recital which would clarify the relevant categories.

Finally, while Presidency stressed that in the case of the exclusion of small enterprises, those employing less than 50 people but having a turnover of more than 10 million € would still be covered. The Commission supported the maintenance of SMEs, was in favour of excluding *micro-enterprises*[1] and declared that it would return to the subject of *start-ups* and individuals later. Finally, it added that it could accept the exception to the SME, only on a case-by-case basis, but it admitted that this process required additional costs in time and resources. It is then possible to understand that once again the weight of national policies is such that it is possible to quite significantly modify any normative proposal; in order to come up with a proposal tailored to the objectives pursued by Member States.

Furthermore, the NIS Directive also requires DSPs to identify and take appropriate and proportionate technical and organisational measures to manage their risks and prevent and minimise the impact of security incidents.

B. Security and notification obligations: Commission's implementing power in action

As mentioned several times, European Directive 2016/1148 imposes new regulatory requirements on a set of players whose information technologies support fundamental societal functions. If the NIS Directive obligations are less burdensome for OES, the same does not apply for DSP's which are submitted to identify "*the risks which threaten the security of networks and information systems*" that they use to offer their services in the Union, and to take "*the necessary and proportionate technical and organisational measures to manage them*" (**1**). DSPs must also report to their OES customers any incident having a significant impact on the continuity of essential services, in accordance with the requirements of European Implementing Regulation 2018/151 specifying the parameters making it possible to determine whether an incident has significant impact (**2**).

1. Security requirements (Art. 16 §1 and §2 NIS Directive)

NIS Directive stresses that DSPs should "*identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems*"[2], and prevent and minimise the impact of incidents affecting the security of their network and information systems,

[1] Article 16 §11 of Directive 2016/1148

[2] *Ibid*, Article 16 §1

with a view to ensuring the continuity of those services.[1] Thus, article 16 §1 NIS Directive lists the elements that need to be considered by a DSP upon identification and adoption of security measures for its network. Which are (a) the security of the systems and facilities, (b) incident handling, (c) business continuity management, (d) monitoring, auditing, and testing and (e) compliance with international standards.

While one would have expected that the security specifications / standards would be announced / modified only by ENISA, as had been proposed by many Member States (the UK,the Czech Republic, Sweden, Ireland, Denmark, etc.) during discussions in the Council, the possibility of the Commission having recourse to an implementing act in order to specify them further was finally envisaged.[2] It should be noted that the responsibility for implementing binding EU legal acts rests primarily with EU Member States. However, certain binding legal acts require uniform conditions of execution. In these cases, the Commission or, in specific duly justified cases and in the cases provided for in Articles 24 and 26 of the Treaty on European Union, the Council is empowered to adopt implementing acts.[3]

Nevertheless, the NIS directive stresses that any DSP security requirement related to implementing acts is adopted by applying Article 5 provision of Regulation (EU) No 182/2011.[4] Regulation (EU) No 182/2011 of the European Parliament and of the Council establishes the general rules and principles relating to the procedures for the control by EU countries of the exercise of implementing powers by the Commission.[5] This is done through so-called *comitology procedures*, that is, the Commission is assisted by committees made up of representatives of EU countries and chaired by a representative of the Commission. Any draft implementing act is submitted to the committee by its chairman. Thus, Article 2 §1 of the Commission's implementing regulation (EU) 2018/151[6] of January 30th 2018, laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be considered by DSPs for managing the risks posed to the security of NIS and of the parameters for determining whether an incident has a substantial impact, stresses the following precisions on article 16 NIS Directive provisions (**Appendix 6:** Further elements to be considered by DSPs for managing the risks posed to the security of NIS (Article 2 §1 of Commission's implementing regulation (EU) 2018/151). Except for the security requirements mentioned above, for a digital service provider to safeguard the security of its network and information system, an incident notification procedure should be followed.

[1] Article 16 §2 of Directive 2016/1148

[2] *Ibid,* Article 16 §8

[3] Article 291 TFEU.

[4] Article 22 §2 of Directive 2016/1148

[5] OJ L 55, 28.2.2011, p. 13–18

[6] OJ L 26, 31.1.2018, p. 48–51

2. Notification requirements (Art. 16 §3 and §4 NIS Directive)

This softer regulation of digital service providers in terms of security and notification requirements is also evident in their obligation to notify an incident only in those cases where they have access to the information needed to assess the impact of such incident.[1] The light-touch approach aims at "*avoiding overburdening"* the DSPs while not "*hampering the capacity of the EU, to react to cybersecurity incidents in a swift and efficient manner*"[2]. Therefore, there are reasons to be concerned that a significant lowering of the requirements of incident notification (types of incidents, parameters to be used) could result in hindering the capacity (at EU or national level) to follow up on specific incidents threatening the functioning of the internal market at various levels.

The DSPs are required to notify to the national competent authorities or the CSIRT any incident having a substantial impact on the provision of their services, only in the following situations: "*the provider has access to all this information required to report an incident so that the reporting can be done properly*"[3]; "*The provider is not considered a micro and small digital service provider*"[4], otherwise, it will be excluded from implementing the incident notification provisions.

Article 16 §4 NIS Directive mentions the parameters to be taken into account in order to determine whether the impact of an incident is substantial, namely: "*(a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident; (d) the extent of the disruption of the functioning of the service; (e) the extent of the impact on economic and societal activities*". These parameters are further specified in the Implementing Regulation (**Table 16**).

Elements	Details
number of users	(a) Number of affected natural and legal persons with whom a contract for the provision of the service has been concluded; or (b) Number of affected users having used the service based in particular on previous traffic data.
duration of the incident	Time period from the disruption of the proper provision of the service in terms of availability, authenticity, integrity, or confidentiality until the time of recovery.
geographical spread	Digital service provider shall be in a position to identify whether the incident affects the provision of its services in specific Member States

[1] Article 16 §4 of Directive 2016/1148

[2] ENISA, 'Incident notification for DSPs in the context of the NIS Directive, A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive', 27 February 2017, available at https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive (accessed on September 9th, 2021)

[3] Article 16 §4 of Directive 2016/1148 and Article 3 §6 Implementing Regulation 2018/151

[4] Article 16 §11 of Directive 2016/1148

extent of the disruption	Measured as regards one or more of the following characteristics impaired by an incident: the availability, authenticity, integrity or confidentiality of data or related services.
extent of the impact	shall be able to conclude, based on indications such as the nature of its contractual relations with the customer or, where appropriate, the potential number of affected users, whether the incident has caused significant material or non-material losses for the users such as in relation to health, safety or damage to property.

Table 16: *Impact substantiality evaluation criteria*

Table made by author

The Council's Presidency considered[1] that it was difficult to determine objective criteria related to the *criticality* of a specific DSP. However, in view of the proposed harmonised approach towards DSPs, any threshold needs to be based on objective criteria, to avoid the risk of fragmentation that such subjective criteria would entail. In order to foster commons threshold at EU-level, Article 4 of the Implementing Regulation 2018/51 establishes a set of incident notification provisions for adopting common thresholds parameters, as follow:

> *"(a) The incident caused an unavailability of the core service more than 5 000 000 user hours, whereby the term user hour refers to the number of affected users in the EU for a duration of sixty minutes. (b) The incident caused a loss of confidentiality, integrity or authenticity of data or services affecting more than 100 000 users. (c) The incident created risks for public safety, public security or of loss of life. (d) The incident caused damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000000.*"

It should be reminded here that any disruption on DSPs' operations may affect the cybersecurity of essential sectors and have either a cross-sector (or even a cross-border) impact on the provided services. Article 16 §5 NIS Directive requires from DSPs to manage a documented security policy, for ensuring that third parties are trained and aware of security issues. But mentioning thresholds to cover such case will have been welcomed. Maybe we should expect that future NIS II Directive will establish a compatible framework taking in considerations (inter)dependencies.

To sum up, the NIS directive contains three mandatory notification and reporting requirements (**Figure 6**). At first, DSP must notify incidents with substantial impact, without undue delay, to the national authority and/or

[1] Council, 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - drafting suggestions on "*internet enablers*"', 23 September 2015, 12126/15 REV 2 LIMITE.

the national CSIRT of the Member State of main establishment. Then, if the notified incident concerns two or more EU Member States, then the Single Point of Contact of the Member State of main establishment shall inform the SPOC in that other Member State.[1] Finally, the NCA's of the Member States of the main establishment, send an annual summary report to the NIS Cooperation group each year, about the notification received from DSP's.[2] Apart from that, the CSIRTs share information with the EU CSIRT network on a voluntary basis.[3] For example, information sharing about Indicators of Compromise (IOCs) between CSIRTs happens continuously, on a daily basis, even when there are no incidents.

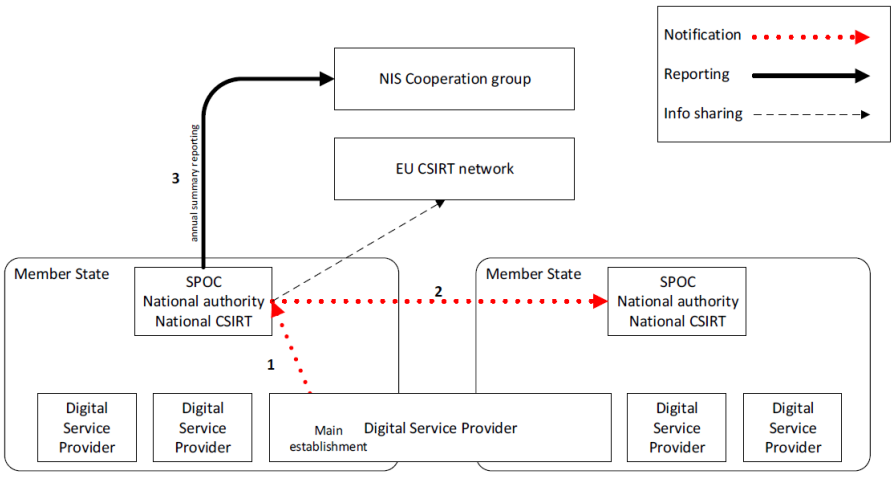


Figure 6: *Notification procedure diagram*

Source: *NIS Cooperation Group publications*[4]

If the public shall be advised due to the nature of the incidents' impact, Member States should provide that the public would "*be informed either from the provider or from the competent authority, within the meaning of preventing or responding to an on-going incident*"[5]. The focus of communication should be on the impact of the incident, for example the impact on the essential services, or the impact on the economy/society. Practically speaking, it is often best if the operator itself reaches out to its customers, or the public in general, because it

[1] Article 16 §6 of Directive 2016/1148

[2] Recital 33 of Directive 2016/1148

[3] *Ibid*, Recital 40

[4] Available at https://www.europeansources.info/corporate-author/nis-cooperation-group-nis-cg/ (accessed on Jnauary 3rd, 2022).

[5] Article 16 §7 of Directive 2016/1148 : 'After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest.'

has appropriate channels for such communications, for example a customer website, a helpdesk, etc. However, there may be situations when the authority or CSIRT must inform the public,

> "*if public awareness is needed to mitigate the impact of ongoing or future incidents; if people outside the current customer base are impacted; if the current customer base is very different from the customers originally affected by the incident; if the operator is no longer able to inform the public, e.g. when the company ceased operating and if the operator did not properly, or will not, inform the public, but there is a critical need to do so*."[1]

It is important that before informing the public about an incident, there is a consultation with the organisation affected by the incident, the national CSIRT and, if relevant, the CSIRTs and/or competent authorities of other Member States involved, to avoid jeopardising ongoing incident response efforts, to avoid hampering ongoing investigations, and to avoid unnecessary impact on the security or commercial interests of the organisation affected by the incident. Additionally, a light-touch approach is provided to DSPs in case of jurisdiction issues. While notifications methods, when it concerns the means, the timing, or the approach, remain the same for OES, there is an important difference: the DSP must notify the incident to the national competent authority or the CSIRT of the relevant Member State where it is established.[2] This also means that the authority receiving the notification must cooperate with the authorities in EU countries where the incident has an impact.

There is, however, the possibility that the DSP offers services in the EU without having the infrastructure established in the EU territory. In that case, the DSP should designate "*a representative in the Union*", without prejudice to legal actions which could be initiated against the DSP itself. The representative may be chosen among one of those Member States where its services are offered. In that case, the DSP shall be deemed "*to be under the jurisdiction of the Member State where the representative is established*"[3]. But Member States are also deemed to some requirement following OES and DSP notification.

§3. Penalties and Enhancement: A Shared Enforcement

[1] NIS Cooperation Group, 'Guidelines on notification of Digital Service Providers incidents, Formats and procedures', CG Publication 06/2018, available at https://ec.europa.eu/digital-single-market/en/nis-cooperation-group (accessed on March 27th, 2020)

[2] Article 18 §1 of Directive 2016/1148

[3] *Ibid*, Article 18 §2 and §3

A. Implementation and Enforcement Powers (Articles 15 & 17 NIS)

When enforcement is entrusted to national authorities, the EU executive actors, such as the Commission, EU agencies and networks, largely monitor the implementation of EU laws through national governments and private actors. In other words, they identify if the policy goals and core values are adhered to (1).

1. The Role of the National Competent Authorities

The NCA's assert that the OESs are compliant with their obligations as they are provided in Article 14, "*for taking the appropriate and proportionate security and operational measures*[1]*, including documented security policies, for ensuring the state-of-the-art security level of the networks and information systems used for the provision of their essential services*"[2].

The role of national competent authorities, or of a "*qualified auditor*"[3], is to serve as an external auditor to OESs with the responsibility of monitoring their compliance with the NIS Directive's notification objectives. To facilitate NCA's audits and to assist OES across all EU Member States to comply with the requirements of the NIS Directive, ENISA proposes in its 2018 guideline document: "*an information security audit and self-assessment/management frameworks (…); a framework mapping per domain of applicability; and presents recommendations to the NCA on how to handle, manage and process the information collected during audits performed on OES*" [4].

An information systems security audit (ISS audit) is "*an independent review and examination of system records, activities and related documents, which intends to improve the level of information security, avoid improper information security designs, and optimise the efficiency of the security safeguards and security processes*"[5]. There are three main forms of ISS audit, depending on the relationship between the auditor and the auditee parties. Following the assessment of information or results of security audits, "*the competent authority may issue binding instructions to the operators of essential services to remedy the deficiencies identified*"[6].

---

[1] Article 15 §1 of Directive 2016/1148

[2] *Ibid,* Article 15 §2

[3] *Ibid,* Article 15 §2 (b)

[4] ENISA, 'Guidelines on assessing DSP and OES compliance to the NIS Directive security requirements', 28 November 2018, available at https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements (accessed on March 20th, 2020)

[5] *Ibid*

[6] Article 15 §3 of Directive 2016/1148

This auditing team should additionally "*be equipped with appropriately qualified personnel complemented by the necessary capacity in numbers and facilities*".[1] It is possible however for the Member States to determine the assessment types the competent authorities may follow when performing their tasks. Finally, the competent authority shall work "*in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches*"[2].

The NCAs are also responsible for ensuring that the DSPs comply with their obligations provided under Article 16 of the NIS Directive, "*for taking the appropriate and proportionate security and operational measures*", including documented security policies for ensuring the state-of-the-art security level of the networks and information systems used for the provision of their services.

2. The Lex specialis clause and the 'Costanzo' obligation

There are two ways according to which law considers the relationship between a particular rule and a general rule, the latter often termed as a principle or a standard. A particular rule may firstly be considered as an application of the general rule in each circumstance. While a particular rule may next be conceived as an exception to the general rule, *lex specialis derogat lex generali.* The lex specialis clause may be thus expressly authorised by the relevant general rule (either as a specific application of or exception to it). It may be expressly prohibited by the relevant general rule. Otherwise, the relevant general rule remains silent on the question. The NIS Directive's preamble expressly authorises lex specialis as an exception to it. [3]

The lex specialis principle is often used to solve redundancy in law, rather than legal antinomies, and so it is a tool to prevent the simultaneous application of special and general compatible rules. One of the difficulties in the lex specialis rule follows from the relative unclarity of the distinction between *general* and *special*. Generality and speciality are thus relational. The *lex specialis* principle is part of the established interpretative repertory found in CJEU's judgements.[4] The CJEU has held that a measure may not be regarded as a *lex specialis* vis-a-vis another rule drafted in too general terms and which contains "*specific rules for particular instances or supplementary rules*"[5]. The CJEU qualifies or overrides therefore a provision of national or Union

[1] Article 15 §1

[2] Article 15 §4 of Directive 2016/1148

[3] *Ibid,* Recitals (9)-(12)

[4] Case C-27/02, *Petra Engler v Janus Versand GmbH*, ECLI:EU:C:2005:33; Case C-582/08, *European Commission v United Kingdom of Great Britain and Northern Ireland*, ECLI:EU:C:2010:429

[5] Case C-444/00, *The Queen, on the application of Mayer Parry Recycling Ltd, v Environment Agency and Secretary of State for the Environment, Transport and the Regions, and Corus (UK) Ltd and Allied Steel and Wire Ltd (ASW)*, ECLI:EU:C:2003:356; Case C -252/05, *The Queen on the application of Thames Water Utilities Ltd v South East London Division, Bromley Magistrates' Court (District Judge Carr)*, ECLI:EU:C:2007:276

law by reference to a hierarchically higher, often treaty-based, norm or a general principle of Union law. [1] It is implied, rather than made explicit that it operates as lex superior compared to a measure of secondary Union legislation.

Initially, no mention of the principle *lex specialis* appeared in the proposal for the directive made by the Commission on February 7th 2013. It was the COREPER meeting of November 7th 2014 which added this provision to the proposal by mentioning that: "*If a sector specific Union legal act contains security and notification requirements covering network and information security, the provisions of that sector specific Union legal act shall apply instead of Article 14 of this Directive*"[2]. Since then, the recurrent mention of a sector specific Union legal act in the field of maritime transport has led to several modifications to Article 1 §7 NIS Directive, as can be seen below (**Table 17**)

10041/15 REV 1 COR1	**12485/15**	**13717/1/15**
Amended by COREPER mandate 23 June 2015	*Council Proposal 06 October 2015*	*Council Proposal 11 November 2015*
If a sector specific Union legal act contains explicit obligations for operators to ensure either the ~~requirements for~~ security of networks and information systems and/or for the notification of incidents, the provisions of that sector specific Union legal act shall apply instead of Article 14 of this Directive.	If a sector specific Union legal act contains explicit obligations for operators **or digital service providers** to ensure either the security of networks and information systems or the notification of incidents, the provisions of that sector specific Union legal act shall apply instead of Article 14 **and 15a** of this Directive.	If a sector specific Union legal act ~~**contains**~~ **requires** ~~explicit obligations~~ ~~for~~ operators **of essential services or digital service providers** to ensure either the security of networks and information systems or the notification of incidents, the provisions of that sector specific Union legal act shall apply **in relation to** ~~those obligations~~ **such requirements** instead of ~~Article 14 and or 15a of~~ this Directive.

Table 17: *Article 1 §7 NIS Directive discussion work 2015 (Part 1)*

(Table made by author)

Source: *https://data.consilium.europa.eu/*

However, as the Council of the Union has been able to recognise, the use of this principle "*should not lead to lower requirements […] it believes that clearer language should be used to avoid legal uncertainty*"[3] and to a fragmented market of course. Therefore, it has been suggested to replace the word *comparable* with *equivalent*[4] and to provide three clarifying recitals (**Table 18 and 19**).

[1] Case 169/80, *Administration des douanes v Société anonyme Gondrand Frères and Société anonyme Garancini*, ECLI:EU:C:1981:171; Case C-439/01, *Libor Cipra and Vlastimil Kvasnicka v Bezirkshauptmannschaft Mistelbach*, ECLI:EU:C:2003:31; Case C-352/09 P, *ThyssenKrupp Nirosta GmbH v European Commission*, ECLI:EU:C:2011:191; Case C-54/16, *Vinyls Italia SpA v Mediterranea di Navigazione SpA*, ECLI:EU:C:2017:433

[2] Council, 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - State of play and work ahead', 14 January 2015, 5257/15 LIMITE.

[3] Council of European Union, 01 December 2015, 14606/15 REV 1.

[4] Council of European Union, 01 December 2015, 14606/15 REV 2.

14606/2/15 REV 2	Directive (EU) 2016/1148
Council Proposal 03 December 2015	6 July 2016
~~If~~ Where a sector specific Union legal act ~~contains~~ requires ~~explicit obligations~~ for operators of essential services or digital service providers to ensure either the security of their networks and information systems or the notification of incidents, provided that such requirements are at least ~~comparable~~ equivalent in effect to the obligations contained in this Directive, ~~the~~ those provisions of that sector specific Union legal act shall apply ~~in relation to those obligations such requirements instead of Article 14 and or 15a~~ the corresponding provisions of this Directive.	~~If~~ Where a sector-specific Union legal act requires operators of essential services or digital service providers **either** to ensure the security of **their** network and information systems or ~~the notification of~~ **to notify** incidents, the provisions ~~of that sector specific Union legal act shall apply in relation to~~ **provided that** such requirements **are at least equivalent in effect to the obligations laid down in this Directive, those provisions of that sector-specific Union legal act shall apply.**

Table 18: *Article 1 §7 NIS Directive discussion work 2015 (Part 2)*

Source: *https://data.consilium.europa.eu/doc/document/ST-14606-2015-REV-2/en/pdf*

(Table made by author)

14606/2/15 REV 2	15229/2/15 REV 2	Directive (EU) 2016/1148
(x) Certain sectors of the economy, including some of those referred to in Annex II, are already regulated or may be regulated in the future by sector specific Union legal acts that include rules related to the security of networks and information systems. Whenever those Union legal acts impose requirements concerning the security of networks and information systems or notifications of incidents, then these provisions should apply instead of the corresponding provisions of this Directive. In order for the sectoral Union legal acts to prevail they should contain requirements which are at least equivalent in effect to the obligations contained in this Directive. Such legal acts should thus impose higher or more complex and specific obligations than those referred to in this Directive.	(x) Certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of networks and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of networks and information systems or notifications of incidents, these provisions should apply instead of the corresponding provisions of this Directive if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive.	Recital (9): *Certain sectors of the economy are already regulated or may be regulated in the future by sector-specific Union legal acts that include rules related to the security of network and information systems. Whenever those Union legal acts contain provisions imposing requirements concerning the security of network and information systems or notifications of incidents, those provisions should apply if they contain requirements which are at least equivalent in effect to the obligations contained in this Directive. Member States should then apply the provisions of such sector-specific Union legal acts, including those relating to jurisdiction, and should not carry out the identification process for operators of essential services as defined by this Directive. In this context, Member States should provide information to the Commission on the application of such lex specialis provisions. In determining whether the requirements on the security of network and information systems and*
(x) Where a sector specific Union legal act defines the scope of entities subject to requirements concerning the security of networks and information systems or notification of incidents, then where this scope includes entities listed in sectors and subsectors as referred to in Annex II, the Member States should apply the provisions of this sector specific Union legal act, instead of carrying out the identification process for operators of essential services as defined by this Directive.	(x) Member States should then apply the provisions of such sector-specific Union legal act, including those relating to jurisdiction, and should not carry out the identification process for operators of essential services as defined by this Directive. In this context, Member States should provide information to the Commission on the application of the provision on lex specialis.	

(x) Where the provisions of a sector specific Union legal act concerning the security of networks and information systems, or notification of incidents apply instead of the corresponding provisions of this Directive it follows that the provisions concerning jurisdiction and supervision as set out in that sector specific Union legal act apply instead of the corresponding provisions of this Directive.		*the notification of incidents contained in sector-specific Union legal acts are equivalent to those contained in this Directive, regard should only be had to the provisions of relevant Union legal acts and their application in the Member States.*

Table 19: *Article 1 §7 NIS Directive discussion work 2015 (Part 3)*

Source: *https://data.consilium.europa.eu/*

(Table made by author)

Although the interpretation of EU law has no legal binding value, it does often have a strong impact.[1] Following European Commission assessment on the application of Article 1§7 NIS Directive to the banking and financial market sectors in its 2017 Communication "*Making the Most of NIS*", it seems to be slightly more assertive than the NIS Directive; without being prolific in clarifying the methodology to be followed in interpreting Article 1§7 NIS Directive. Consequently, while most Member States have identified OES in the banking and financial markets sectors, a few Member States have not identified OES, "*claiming that operators are providing services covered by leges speciales*"[2].

In the context of the NIS Directive, the specific situation is defined by the following conditionality: "*(...)if they contain requirements which are at least of equivalent effect to the obligations contained in this Directive (...)*"[3]. However, there is no definition in the Treaties of what should be understood as a measure of equivalent effect between two norms of the same level and Member States barriers to the free movement of goods by measures, thus having equivalent effects to these quantitative restrictions, isn't applicable here. It is mentioned in the NIS Directive that measures of equivalent effect contained in sector-specific Union legal acts should only be regarded "*to the provisions of relevant Union legal acts and their application in the Member States*". While recitals 10 and 11 of the NIS Directive discuss the water transport sector, recitals 12 to 14 the banking and financial market infrastructure sectors, unfortunately they do not provide clear-cut answers. There is debate whether such EU sector-specific legislations should be considered as lex specialis – and if so to what extent -

[1] European Commission, Communication on 'Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', 4 October 2017, COM(2017) 476 final/2, section on 'the relationship between the NIS Directive and other legislation'

[2] European Commission, 'Report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems', 28 October 2019, COM(2019) 546 final

[3] Recital 9 of Directive 2016/1148

they should prevail over the NIS Directive provisions. These ambiguities will likely prompt the intervention of the CJEU in the assessment of this *equivalence effect*.

Article 1 §7 NIS Directive, followed by related recitals 9, 10 and 13, also lack clarity and even to some extent inconsistency. It is therefore especially unclear whether the NIS Directive shall apply to some extent in excess of *lex specialis* provisions found in other EU sector-specific legislation. While article 1 §3 NIS Directive stipulates, for example, that the Directive does not apply to undertakings subject to the requirements of the Telecom Framework Directive,[1] some Member States[2] "*appear to have identified OES providing services that should actually be regulated under the Telecom Framework Directive, such as internet access and telephone services*"[3]. This entails however some risks for the NIS Directive's provisions implementation if we take into consideration the obligation made by the CJEU's *Fratelli Costanzo* case-law[4] for national administrative authorities for cases, in which a conflict arises between provisions of national law and provisions of EU law.

In case 103/88, concerning a request addressed to the Court, in application of Article 177 of the EEC Treaty, by the *Tribunale Amministrativo Regionale per la Lombardia* (Italy) and seeking to obtain, in the dispute pending before this jurisdiction between Société *Fratelli Costanzo SpA*, a company incorporated under Italian law, with its registered office in *Misterbianco*. The Court of Justice judged that, when a provision of national law is, for instance, incompatible with the freedom of establishment, national administrative authorities are no longer allowed to apply the national provision concerned.[5]

Should the *lex specialis* provisions prevail, the NIS Directive does consequently not apply, including the process of identification of the operators of essential services.[6] But identification process doesn't end with *lex specialis* assessment. For the purposes of the identification process, where an entity provides an essential service in two or more Member States, those Member States should engage in bilateral or multilateral discussions with each other.

B. Penalties (Article 21 NIS), Limiting Member States' Institutional Autonomy

[1] European Parliament and Council, Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, p. 33–50

[2] Germany might serve as example (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI).

[3] European Commission, 'Report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems', 28 October 2019, COM(2019) 546 final.

[4] Case 103/88, *Fratelli Costanzo SpA v Comune di Milano*, ECLI identifier: ECLI:EU:C:1989:256

[5] *Ibid*, p. 31-33

[6] Recital 9 of Directive 2016/1148

The Member States are considered as the traditional enforcers of EU law following the interpretation of the Article 4(3) TEU. In vairous policy areas, the broad obligation incumbent on Member States to adopt all necessary measures for the implementation and the application of EU law. From a national perspective, this multi-level dynamic of compliance could be seen as "*a much-needed self-restraint of the Union, on the deeply held assumption that all aspects of the sanctioning cycle touch upon the noyau dur of national sovereignty*"[1]. The persisting reference of the Court to effective, proportionate[2] and dissuasive sanctions very often takes the shape of specific legal contours within which the domestic authorities must contextualise at their (now more limited) discretion.[3]

According to article 21 of the NIS Directive, "*Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented*". The Member States are often free to choose which type of enforcement to use to enforce substantive norms. In most cases, it is up to Member States to choose a sanction or combination of sanctions. This derives from the principle of "*national institutional autonomy*"[4], according to which each Member State is free to determine its own internal organisation, including the division of powers and duties among its administrative authorities. The autonomy may jeopardize the requirement of a uniform application of EU law. Therefore, enforcement sanctions must be equivalent, effective, proportional, and dissuasive. The fact that penalties must be effective and dissuasive can ensure that the goal of enforcement is achieved in practice and the principle of proportionality ensures that the sanction does not go beyond what is reasonable given the gravity of the offence.

According always to article 21 of the NIS Directive, "*The penalties provided for shall be effective, proportionate and dissuasive*". In this respect, the identification of the essential elements of the sanctions to be transposed into national law "*pre-determines the forms and severity of sanctions that are likely to be considered as effective, proportionate and dissuasive*"[5]. While it contributes to securing the implementation of EU policies, this approach also contributes to preventing these measures from being cancelled following a judicial review at national and European levels, unless the EU normative choices are per se disproportionate, or a Member State

[1] S. Montaldo, F. Costamagna and A. Miglio, *EU Law Enforcement: The Evolution of Sanctioning Powers* (Routledge, 2021).

[2] In the 1970s, the Court of Justice qualified proportionality as a general principle stemming from the rule of law,3 requiring that individual freedom (of action) cannot be limited beyond what is necessary in the public interest.4 Since then, proportionality has gradually developed from a supranational emanation of some domestic legal traditions — especially that of Germany — to a fully-fledged general principle of EU law encompassing any aspect of the Union's action: Case 11/70, *Internationale Handelsgesellschaft mbH contre Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, ECLI:EU:C:1970:114

[3] Case 68/88, *Commission of the European Communities v Hellenic Republic*, ECLI identifier: ECLI:EU:C:1989:339

[4] Article 4(2) TUE

[5] S. Montaldo, F. Costamagna and A. Miglio, *EU Law Enforcement: The Evolution of Sanctioning Powers* (Routledge, 2021).

departs from the EU-pattern when transposing them. Leaving aside situations of erroneous implementation, the actual sanctioning scales may be influenced by other branches or aspects of national legislation falling outside the scope of EU competences, thereby leading to the imposition of excessively harsh measures.

Although it is within the national authorities' duty to punish certain conduct under Article 4(3) TEU, the Union's *jus puniendi* is blurred by the allocation of the choice regarding the type and extent of a sanctioning measure at domestic level. Meanwhile, recent practice indicates that "*the margin of discretion left to Member States is gradually decreasing, as the European legislature increasingly dictates the nature of the sanctions to be enacted at domestic level and the basic criteria of their intensity*"[1]. Article 21 of the NIS Directive does not provide any further indication on the matter. However, the jurisprudence of the Court of Justice brings some elements for assessing the proportionality of the penalties.

The proportionality test developed by the Court of Justice requires a measure to be appropriate to the aim pursued, necessary to achieve it — meaning that no more desirable or less restrictive alternatives are reasonably available — and proportionate in a strict sense.[2] In fact, the review of national measures through the lens of proportionality does not only cover the formal legality of a sanction, but also the merits of its adoption, substance and effects, both on the individual concerned and on the objectives pursued by EU law. This assessment covers all steps of the sanctioning cycle, as the "*Member States are required to comply with the principle of proportionality not only as regards the determination of factors constituting an infringement and the determination of the rules concerning the severity of fines, but also as regards the assessment of the factors which may be taken into account in the fixing of a fine*"[3].

Therefore, Member States must exercise their reserved powers in a manner that does not affect the general principles of the EU legal order.[4] Proportionality plays a major role here, as the Member State is caught between two potentially competing obligations. The duty of loyal cooperation requires it to sanction infringements of EU law and to do so effectively, whereas the general principles place limits on the national authorities' discretion to sanction those breaches. In addition, the national implementing provisions usually embody further national policy goals, which might not be fully in line with the EU objectives. Even if the NIS Directive is better coordinating and saferguarding the cyberspace across the EU, it will take years before its effectiveness can be

[1] S. Montaldo, F. Costamagna and A. Miglio, *EU Law Enforcement: The Evolution of Sanctioning Powers* (Routledge, 2021).

[2] Case 66/82, *Fromançais SA v Fonds d'orientation et de régularisation des marchés agricoles (FORMA)*, ECLI:EU:C:1983:42.

[3] Case C-210/10, *Márton Urbán v Vám- és Pénzügyőrség Észak-alföldi Regionális Parancsnoksága*, ECLI:EU:C:2012:64, para. 54. This is the only judgment in which the Court uses this description. Usually, case law refers to a more nuanced formula, which basically identifies the key components of the proportionality review of a sanction and leaves the door open for possible further assessment criteria: "In order to assess whether a penalty is consistent with the principle of proportionality, account must be taken of, inter alia, the nature and the degree of seriousness of the infringement which that penalty seeks to sanction, and of the means of establishing the amount of that penalty". See C-712/17, *EN.SA. Srl contre Agenzia delle Entrate – Direzione Regionale Lombardia Ufficio Contenzioso*, ECLI:EU:C:2019:374, para. 40

[4] Case C-378/97, *Criminal proceedings against Florus Ariël Wijsenbeek*, ECLI:EU:C:1999:439

proved. There are always going to be zero-day vulnerabilities to be exploited by security agencies and/or criminals. This chapter has examined then whether the nature of the NIS Directive's provisions may limit the regulatory effectiveness of the NIS Directive.

***

The publication of the first EU-CSS in 2013 marked the formal establishment of cybersecurity as a new policy area in the EU. It is important to highlight the fact that the EU plays a coordinating role on cybersecurity by building a cyber-resilient regulatory framework. This outcome resulted from the acknowledgment of the blurring of lines in three initially distinct but converging policy areas of (1) NIS protection, including privacy and data protection issues; (2) cybercrime; and (3) cyberdefence. The EU cybersecurity landscape is continuously evolving thanks to the ambiguity embedded in the term of *cybersecurity*. For the above development it has been now proven that, the EU's legal framework in the cybersecurity domain is a highly fragmented legal framework, scattered across multiple documents from different policies. Areas in which the EU does not have the same level of competences and it should be noted also that the area is bound to develop further given the EU's digital dependency.

The developments highlighted the *hybridity* of the legal framework of the EU, which oscillates between the hard and soft law across the European cyber policy mix. A limited transfer of competences, the lack of competences for the policy mix and its cross-cutting nature let the EU apply different modes of governance in cyber policy. While decisions are made according to the ordinary legislative process for issues such as the security of the DSM, any decision having an impact on the national cyberdefence must employ soft institutional governance. It is now established that a highly fragmented legal framework constitutes the European cybersecurity policy area. The adoption of the NIS Directive hardened the EU's legal framework on cybersecurity issues by seeking the harmonisation the national legal framewoks of the Member States of the EU on network and information systems security. However, it the soft dimension of the NIS Directive also leaves to them -in most cases- the choice of *weapon* to be used. A situation which does not guarantee that the desired result will be achieved.

By exceeding the scope of the NIS Directive on essential sectors, for example, Member States (of the EU) may end up imposing significant financial burdens on certain national operators, especially when they are already subject to other EU policies (e.g., insurance companies). This situation thus entails substantial risks of non-compliance. When it comes to the identification of essential sectors, a maximum harmonisation rule might be preferable, prioritising EU interests over those of individual Member States (of the EU). In its report of 28 October 2019 assessing the "*consistency of the approaches taken by Member States (of the EU) on the identification of OES*" the Commission concluded that "*although the NIS Directive has initiated a crucial process of increasing and improving operator risk management practices in critical sectors, the identification*

of OES is still significantly fragmented across the EU" [1]. Although the NIS Directive was deemed to have harmonised the European DSM, it is also clearly linked to national interests.

Member States' interests are delimitating the extent of the application of the obligations undertaken by the Member States of the EU. Institutional governance in the field of cybersecurity is furthermore fragmented at the EU level, and there is a clear lack of trust that prevents effective cooperation among stakeholders on crucial aspects of the process. The cybersecurity policy mix in the EU involves various modes of institutional governance. Over the past decade, the EU has set up several institutions that aim to provide its Member States with the necessary cybersecurity and cyber defence capabilities. Meanwhile, the EU practice of *agencification* has resulted in an expediential development of the EU's cybersecurity *soft* networked governance, with horizontal cooperation and information exchange between the various agencies being often limited. The next part introduces a research approach for the interpretation and the analysis of legal developments from an angle that brings the legal dimension of the membership of States in the European Union closer to its practical reality. By choosing Member States' interests as a frame for analysis of the NIS Directive compliance, the next part aims to further explore the application of Member State obligations, at the national level.

[1] European Commission. 2019. 'Report to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems COM/2019/546 final'.

Part II. The Impact of Domestic Factors on the Transposition of the NIS Directive

Despite the absence of express competencies in relation to cybersecurity, the establishment of a European legal framework in the field of the cybersecurity triggered a series of important changes due mostly to the cross-border and cross-sectoral dimension of cyber threats. The boundaries between the European Single Digital Market, the Justice and Home Affairs policy and the Foreign policy became increasingly blurred, while institutional roles became untraditional followed by an intensification of the *agencification* practice in cybersecurity matters. Therefore, Member States were obliged to work with the EU in harmonising their national legislation. However, the "*legislation made at the EU level (...) is only effective if implementation of that legislation takes place*"[1].

Effectiveness is a precondition and a guarantee for the success of any legal system. This is particularly true in relation to the Union's law, which is largely dependent on effective implementation in the Member States. The overall effectiveness of the Union regulatory regime – including rights and benefits it is intended to confer – may in practice be shadowed in various ways. For instance, Members States may fail to implement efficiently Union's law instruments. As *Treib* puts it, "*we have yet comparatively little evidence on the extent to which there is non-compliance beyond transposition and on the factors that are conducive to effective application and enforcement*"[2]. Thus, the limits of EU Law should be set within domestic policies.[3]

Following *Fabien Terpan* interpretation, "*there is a continuum running from non-legal positions to legally binding and judicially controlled commitments with, in between these two opposite types of norms, commitments that can be described as soft law*"[4]. While soft law involves the use of non-binding rules, hard law in the EU involves rules stemming from treaties, directives and regulations.[5] European hard law is defined then as having legally binding force and as having a legal basis in the Treaty.[6]

Regarding EU's Directives, article 288 TFEU defines them as a legal act binding on any recipient Member State as to the result to be achieved, while leaving the competence as to form and means to national authorities.

---

[1] European Commission, 'Communication from the Commission, Completing the Better Regulation Agenda: Better solutions for better results', 24 October 2017, COM (2017) 651 final.

[2] Treib, O. (2014), Implementing and complying with EU governance outputs, Living Reviews in European Governance 9(1), 1–46.

[3] See P.J. Cardwell, 'Governance as the meeting place of EU law and politics'. In Cardwell, P.J. and Granger, M.-P. (Eds.), *Research Handbook on the Politics of EU Law* (Edward Elgar Publishing, 2020).

[4] See F. Terpan, 'Soft Law in the European Union - The Changing Nature of EU Law', (2015) 1 *European Law Journal, Wiley*, 21

[5] See D. Trubek, M. Cottrell and M. Nance, "Soft Law", "Hard Law", and European Integration: Toward a Theory of Hybridity, (2005) *University of Wisconsin Legal Studies Research Paper*, No. 1002.

[6] See L. Senden, *Soft Law in European Community Law*, (Hart Publishing, 2004), p. 45

Thus, by allowing for the approximation of national laws the directive plays a preponderant role in the integration of the European community. Unlike the EU regulation which, according to the letter of Article 288, is directly applicable in all Member States, the directive requires transposition. The State's obligation of result implies that it uses its internal law to fulfil it. Thus, the obligation of transposition incumbent on the States is a condition of the effectiveness of EU law. However. Compliance between EU law and Member State's legal obligations remains still an actual issue.[1]

Compliance is the "*(...) behaviour which conforms to a predetermined set of regulatory measures*"[2] and thus refers to the extent to which "*agents act in accordance with, and fulfilment of the prescriptions contained in (...) rules and norms*"[3]. Regarding EU law, compliance refers then to the extent to which Member States behaviour is conform with the fullfiment of prescriptions contained in the EU law. Effectiveness may implicate either compliance or transposition, enforcement, and impact. Unlike European environmental policy, which has been the subject of several analyses on the phenomena of effectiveness, compliance or customisation, European cybersecurity policy does not benefit from a similar interest from Europeanisation research.

In a top-down relationship, the implementation of EU law is part of a hierarchical relationship in which the EU would handle changes at national level through EU law primacy. While in a bottom-up relationship, state actors are seen as *decentralised problem-solvers*, trying to adapt EU law on existing national policies to resolve potential conflicts with national interests. Defined as "*a process of problem-solving by the politico-administrative system*", *Krislov, Ehlermann and Weiler* differenciate three steps within the political process: adoption, implementation, and enforcement[4]. The implementation process relates to the transposition and application phase. For the purposes of the present study, I will only focus on the transposition outcome of the NIS Directive across 6 countries. The first chapter will therefore highlight the way domestic factors may influence the transposition outcome of European directives (**Chapter I**). While the second chapter will assess the transposition outcome of the NIS Directive throughout an empirical analysis (**Chapter II**).

[1] Complaints by citizens and businesses, infringement proceedings by the Commission and rulings of the CJEU are all evidence of these shortcomings in the implementation of EU law.

[2] See D. Matthews, 'Enforcement of Health and Safety Law in the UK, Germany, France and Italy', (1993) *Economic & Social Research Council Working Paper* 18, London: National Institute of Economic and Social Research.

[3] J.T. Checkel, 'Why Comply? Constructivism, Social Norms, and the Study of International Institutions', (1999) *ARENA Working Papers*, 99/24, Oslo: Advanced Research on the Europeanisation of the Nation-State.

[4] See S. Krislov, C. Ehlermann and J.H. Weiler, 'The Political Organs and the Decision-Making Process in the United States and the European Community', in M. Cappelletti, M. Secombe and J. Weiler (eds), *Integration through Law, Volume 1: Methods, Tools and Institutions, Book 2: Political Organs, Integration Techniques and Judicial Process* (Walter de Gruyter, 1986), at 61

Chapter I. Domestic Factors: Moving from Legal to Practical Compliance

EU law operates within "*a self-determined and rather closed conceptual and doctrinal space where formalism dominates the understanding of the rights guaranteed and undertaken by Member States*".[1] Nevertheless, the Member States' interests constitutes a challenge that legal scholarship must not avoid when framing its analysis of EU law issues.

In the case of EU directives confusion can arise on what should be understood as *implementation*. Often a differentiation is made between *legal* implementation and *practical* implementation on the other.[2] By legal implementation is meant the transposition of European directives into domestic law. Practical implementation on the other hand refers to the setting up by national regulators of necessary instruments of monitoring and inspection (e.g., enforcement) and the actual adherence to the law by the regulated (e.g., application). The present thesis focuses on the legal implementation and more specifically on the transposition outcome of EU directives.

Early legal implementation studies[3] depicted the transposition of EU directives as a rather apolitical process in a top-down relationship: the transposition of EU law is part of a hierarchical relationship in which the EU would be responsible for changes at national level. In this way, they drew their attention to the role of various factors, such as the legal quality of the directives. But academics turned later their attention more directly to how domestic norms and political behaviour affect the transposition process of EU directives.

The first section focuses on the theoretical debates upon the limiting impact of the domestic factors on the transposition result (**Section I**). While the second section presents the methodoly retained, the selection of the case studies and the operationalisation assessed variables (**Section II**).

[1] G. Davies, 'Subsidiarity: The wrong idea, in the wrong place, at the wrong time', (2006), 43 *Common Market Law Review* 1

[2] See G. Pridham and M. Cini, 'Enforcing Environmental Standards in the European Union: Is There a Southern Problem', in M. Faure, J. Vervaele and A. Weale (eds), *Environmental Standards in the European Union in an Interdisciplinary Framework* (MAKLU, 1994), at 251

[3] See G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States* (Cambridge University Press, 2005)

Section I. The Impact of Member States' Domestic Factors on Transposition Outcome: A Theoretical Framework

The EU is highlighted by the existence of a decentralised structure since it does not have its own administration to implement locally its legislation. It must rely then on the Member States' cooperation to fulfil this task. The European directives is one of the major legal instruments for this forementioned task. The rules set by those directives must be transposed into national law by Member States within a deadline. Once this transposition is completed. The rules steming from the transposition of the European directive may be applied by domestic actors (e.g., administrations, societal target groups), as well as enforced by administrations and the legal system at the domestic level.

Member States have the primary responsibility for the correct and timely transposition of the Treaties and secondary EU law (regulations, directives, decisions). The process is monitored by the European Commission. If the Commission suspects a Member State not fulfilling its obligations when transposing EU law, it is empowered under the Treaty of Lisbon "*to launch infringement proceedings*"[1]. Transposition problems, especially about the directives, start as soon as the integration deadline has passed, and an infringement has been identified. In this context, there is a preliminary stage which precedes the infringement procedure under Article 258 TFEU, and which consists of a structured dialogue between the Commission and the Member State concerned to identify and resolve problems in a timely manner and to avoid possible appeal to the CJEU.

Transposition is an important tool for assessing the phenomenon, since compliance with European law involves political and institutional changes in the national domain. However, the EU has an implementation *deficit*. Since the directive's measures are not always transposed correctly by all Member States. It is possible indeed to go beyond the minimum rules contained in a directive and thus, create a non-harmonized landscape across the Member States. The multitude of actors involved at the various levels and stages of an EU Directive's life cycle offers also numerous possibilities for shortcomings in transposition and application. As it has been expressed by the European Commission in its Strategic Objectives for 2005-2009, "*failure to apply European legislation on the ground, damages the effectiveness of Union policy and undermines the trust on which the Union depends*".

In Europeanisation research, the state's discretion in transposition has mainly been studied in terms of legal compliance (**§1**). However, adjustment to European policies may also depend on domestic factors such as the stage of liberalisation already present in a Member State, the capacity for national reform, the costs of adaptation or the dominant belief system or the approach to problem solving (**§2**).

[1] K. Davies, *Understanding European Union Law* (Cavendish Publishing, 2001), 87

§1. The 'Pathology of Non-Compliance'

The transposition of directives are clearly related to the literature on Europeanisation[1] What is Europeanisation? As Bulmer points out, "*Europeanisation is not in itself a theory*", but "*a phenomenon that needs to be interpreted*"[2] and, to that end, the support of a theory as well as the appropriate methodological assurance is required. Also, as *Radaelli* states, "*Europeanisation is not a new theory ... It is a process, despite the final state. Europeanisation should be seen as a problem, not as a solution*"[3]. In this sense, the term of *Europeanisation* is a conceptual construction that serves the analysis of a phenomenon (e.g., the dynamics that develop between the different levels of the European system of government). This multilevel dynamic takes different manifestations, based on which different causal relations are formulated. These causal relationships are the subject of investigation and interpretation of various theoretical approaches.

Europeanisation must be conceived as a phenomenon (and not a theory), which each scholar approaches differently, to interpret specific causal relationships. To this end, they employ the conceptual tools of a theory that can produce verifiable hypotheses.[4] However, one of the main problems of the literature upon *Europeanisation* relates to the fact that it overestimates the domestic factors when considering changes at the national level.[5] Not all changes in the internal field can be justified as "*a response to the pressures exerted by Brussels*"[6]. Internal changes may also result from endogenous processes within the national political system.[7]

Another important problem of *Europeanisation* is also related to how its results can be measured.[8] This is a particularly difficult task, as *Europeanisation* is an evolving process, not a static one, where both external

[1] See A. Heritier, 'Differential Europe: The European Union impact on national policymaking', in A. Heritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A.-C. Douillet (eds.), *Differential Europe: The European Union Impact on National Policy Making* (Rowman and Littlefield, 2001), at 1

[2] S. Bulmer, 'Theorizing Europeanization', in P. Graziano and M. P. Vink, *Europeanization: New Research Agendas* (Palgrave Macmillan, 2008), at 46, 47

[3] C.M. Radaelli, 'Europeanization: Solution or problem?', (2004) 4 *European Integration online Papers* 8, 5

[4] S. Bulmer, 'Theorizing Europeanization', in P. Graziano and M. P. Vink, *Europeanization: New Research Agendas* (Palgrave Macmillan, 2008), at 46, 51

[5] M. Vink and P. Graziano, 'Challenges of a new research agenda', in P. Graziano and M. Vink (eds), *Europeanization: New Research Agendas* (Palgrave Macmillan, 2008), at 3, 16

[6] See A. Bradford, *The Brussels Effect – How the European Union rules the world*, (Oxford University Press, 2020).

[7] M. Vink and P. Graziano, 'Challenges of a new research agenda', in P. Graziano and M. Vink (eds), *Europeanization: New Research Agendas* (Palgrave Macmillan, 2008), at 3, 16

[8] See M. Giuliani, 'Europeanization in Comparative Perspective: Institutional Fit and National Adaptation', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanization* (Oxford University Press, 2003), at 134; See also M. Haverland, 'Methodology', in P. Graziano and M. P. Vink (eds), *Europeanization: New Research Agendas* (Palgrave Macmillan, 2007), at 59; C. Radaelli and R. Pasquier, 'Conceptual issues', in P. Graziano and M. P. Vink (eds), *Europeanization: New Research Agendas* (Palgrave Macmillan, 2007), at 35

pressures and internal responses change according to "*time, timing and pace*"[1]. Therefore, its effects can be "*temporary and reversible*"[2]. The process of transposition is being shaken by a *pathology of non-compliance*. A phenomenon to which the effect of Member States' internal forces and more specifically the domestic factors may constitute the *pathology* when explaining transposition outcome.

Inaction is a situation where there is no change. It can take the form of backwardness, delays in transposition and strong resistance to change coming from the EU. It is, in essence, an attachment of European claims to national systems, without a real change in basic structures and political behaviour. Change is the most positive outcome of *Europeanisation*, which essentially implies a *change of model*.[3] In other words, change is not limited to official institutions and national political-administrative structures, but also affects the informal institutions, the beliefs, and preferences of the actors, transmitting new logic and completely changing the political behaviour. On the opposite bank of change, lies the paradoxical result of shrinkage, where national policy becomes less Europeanised than it was before.[4]

The implementation of European cybersecurity legislation is a critical parameter for the success of the policy itself. If Member States do not fully comply with supranational commitments, European cybersecurity policy risks being turned into a paper exercise, with limited cybersecure effects. In addition, under-implementation is a threat to the EU's wider goals, as it calls into question the process of European integration itself.

Several scholars argue that the process of European integration is being shaken by a *pathology of non-compliance*.[5] The real problem is the insufficient amount of data available to calculate the extent of this pathology. The choices, perceptions and reactions of national actors to European pressures and stimuli cannot be interpreted without understanding the creation and evolution of national rules, practices and restrictions that constitute a complex of formal and informal institutions. The adaptation of identities and institutions to an external environment is shaped and limited by internal forces.[6] Therefore, the outcome of actions and policies is determined not only by external pressures, but also by internal factors such as the domestic factors.

---

[1] C. Radaelli and R. Pasquier, 'Conceptual issues', in P. Graziano and M. P. Vink (eds), *Europeanization: New Research Agendas* (Palgrave Macmillan, 2007), at 35, 48

[2] K. Featherstone and D. Papadimitriou, *The Limits of Europeanization: Reform Capacity and Policy Conflict in Greece*, (Palgrave Macmillan, 2008), 55

[3] See P. Hall, 'Policy Paradigms, Social Learning and the State. The case of economic policy making in Britain', (1993) 3 *Comparative Politics* 25, at 275

[4] C. Radaelli, 'The Europeanization of Public Policy', in K. Featherstone and C. Radaelli, *The Politics of Europeanization* (Oxford University Press, 2003), at 27, 37–38

[5] See S. Krislov, C. Ehlermann and J.H. Weiler, 'The Political Organs and the Decision-Making Process in the United States and the European Community', in M. Cappelletti, M. Secombe and J. H. Weiler (eds), *Integration through Law, Volume 1: Methods, Tools and Institutions, Book 2: Political Organs, Integration Techniques and Judicial Process* (Walter de Gruyter, 1986), at 3

[6] See J. March and J. Olsen, 'The Institutional Dynamics of International Political Orders', (1998) 4 *International Organization* 52

The EU has an extremely decentralised system. It lacks its own administrative mechanisms to enforce its legislation and is therefore left to Member States. This particularity makes the EU an extremely interesting field of research. Despite the initial delay, studies on how EU policies are implemented at national level have increased so significantly. Since the mid-1980s, the literature on the europeanization has not only multiplied but has also been upgraded theoretically and methodologically.[1]

Three main different research waves may be diffrenciated.[2] *Siedentopf* and *Ziller* raised firstly the question of whether Member States are really making efforts to make European policies work. In their empirical research, which attempted to analyse the implementation of 17 directives in 12 countries. They argued that the capacity of national administrations plays a key role in implementing Community law.[3] This study, which relied on legal and administrative variables to explain the Member States' compliance with European directives, was followed by others. Coordination capacity and policy-making culture at the national level,[4] as well as issues of pluralism, legislative culture and interpretation of European directives,[5] have been used as the main explanatory factors by their lack of implementation.

In studies based on legal explanatory factors, the complexity and poor quality of directives,[6] the characteristics of national constitutions,[7] as well as the extent and diversity of existing national legislation,[8] were classified as the main reasons for the Members States' non-compliance with the EU's legislation. The specific research focuses mainly on the stage of transposition of the directives and ignores its practical implementation. Consequently, they fail to capture the dynamics of informal processes, such as informal

[1] M. Haverland, 'The Impact of the European Union on Environmental Policies', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanization* (Oxford University Press, 2003), at 203, 207

[2] See E. Mastenbroek, 'EU compliance: Still a "black hole" ?', (2005) 6 *Journal of European Public Policy* 12; See also O. Treib, 'Implementing and complying with EU governance outputs', (2014) 1 *Living Reviews in European Governance* 9

[3] H. Siedentopf and J. Ziller, *Making European policies work: The implementation of community legislation in the Member States* (Sage, 1988), 61–62

[4] See H. Siedentopf and J. Ziller, *Making European policies work: The implementation of community legislation in the Member States* (Sage, 1988); See also J. Richardson, 'Eroding EU politics: Implementation gaps, cheating and re-steering', in J. Richardson (ed), *European Union: Power and Policymaking* (Routledge, 1996), at 278

[5] See K. Collins and D. Earnshaw, 'The implementation and enforcement of European Community legislation', (1992) 4 *Environmental Politics* 1

[6] See H. Collins, 'The constitutionalization of European private law as a path to social justice?', in H.-W. Micklitz, (ed), *The Many Concepts of Social Justice in European Private Law* (Edward Elgar Publishing Ltd, 2011), at 133

[7] S. Krislov, C. Ehlermann, and J.-H. Weiler, 'The Political Organs and the Decision-Making Process in the United States and the European Community', in M. Cappelletti, M. Secombe and J. Weiler (eds), *Integration through Law, Volume 1: Methods, Tools and Institutions, Book 2: Political Organs, Integration Techniques and Judicial Process*, (Walter de Gruyter, 1986), at 3, 80

[8] See H. Collins, 'The constitutionalization of European private law as a path to social justice?', in H.-W. Micklitz, (ed), *The Many Concepts of Social Justice in European Private Law* (Edward Elgar Publishing Ltd, 2011), at 133

practices and the non-institutional dimensions of the interaction between state-society and administration-politics.

From the point of view of administrative science, research has highlighted issues that greatly affect the outcome of implementation, such as: problematic coordination within Member States;[1] style and bargaining standards of national administrations;[2] as well as organisational and technical weaknesses.[3] *Lampinen* and *Uusikyla* emphasised the value of national institutions, where effective and efficient political-administrative institutions - combined with political stability and a public opinion that supports the EU perspective - make implementation easier.[4] Other studies have highlighted the importance of *systemic pathologies* in the implementation process,[5] where structural pathogenesis of bureaucracy, such as corruption in the public sector, can lead to non-compliance.[6] According to *Kaeding*, states with high levels of corruption will experience serious delays in integration, as when a process does not involve personal motivation for those involved, they will be indifferent.[7] Patronage creates systems where obligations are settled only when there is personal motivation for bureaucrats.

The criticism levelled at most of the above studies is that they approach implementation as an apolitical process,[8] where governments fail to respond effectively to European challenges not out of intent but out of weakness due to internal legal and administrative factors. However, *Richardson* also tried to give a political dimension to the role played by governments, as on the one hand, at the European level, Member States appear to be good Europeans to reap benefits, while on the other, they are aware of the real difficulties encountered in implementing policies at home. In any case, the above literature highlighted the role that national administrative

[1] S. Krislov, C. Ehlermann, and J.-H. Weiler, 'The Political Organs and the Decision-Making Process in the United States and the European Community', in M. Cappelletti, M. Secombe and J. Weiler (eds), *Integration through Law, Volume 1: Methods, Tools and Institutions, Book 2: Political Organs, Integration Techniques and Judicial Process*, (Walter de Gruyter, 1986), at 3, 79

[2] See J. Richardson, 'Eroding EU politics: Implementation gaps, cheating andresteering', in J. Richardson (ed), *European Union: Power and Policy-making* (Routledge, 1996), at 278

[3] C. Demmke, 'Towards effective environmental regulation: innovative approaches in implementing and enforcing European environmental law and policy', (2001) *Harvard Jean Monnet Working Paper* 5/01, 15

[4] See R. Lampinen and P. Uusikylä, 'Implementation Deficit — Why Member States do not Comply with EU directives?', (1998) *Scandinavian Political Studies* 21

[5] See M. Kaeding, 'Determinants of transposition delay in the European Union', (2006) 3 *Journal of Public Policy* 26; See also D.H.A. Mbaye, 'Why National States Comply with Supranational Law: Explaining Implementation Infringements in the European Union, 1972-1993', (2001) 3 *European Union Politics* 2; G. Pridham, 'Environmental policies and problems of European legislation in Southern Europe', (1996) 1 *South European Society & Politics* 1

[6] D.H.A. Mbaye, 'Why National States Comply with Supranational Law: Explaining Implementation Infringements in the European Union, 1972-1993', (2001) 3 *European Union Politics* 2, 262

[7] M. Kaeding, 'Determinants of transposition delay in the European Union', (2006) 3 *Journal of Public Policy* 26, 241

[8] E. Mastenbroek, 'EU compliance: Still a "black hole" ?', (2005) 6 *Journal of European Public Policy* 12, 1104; O. Treib, 'Implementing and complying with EU governance outputs', (2014) 1 *Living Reviews in European Governance* 9, 7

culture plays in the implementation process and gave rise to further studies, focusing on the importance of national administrative traditions.

European regulations often reflect however policy problems and experiences that differ from one state to another. Therefore, the analysis should not be one-dimensional, approaching all countries in the same way, as their administrative systems - since they have been formed in different historical, social, economic, and political context - show significant differences in response. Across the years, the process of European integration demanded a greater degree of compliance by Member States, the divergence between the political systems of southern and northern Europe became more pronounced. Respectively, the inability of the countries of the European periphery to follow the dynamics developing in the core of the EU became obvious. Some scholars spoke of the "*Mediterranean syndrome*"[1] and "*paradoxes' of the South*"[2], where the main features of the political culture of the countries of southern Europe were in stark contrast to those of the northern partners. According to this approach, poor implementation and non-compliance was mainly a problem of the South. Four Member States[3] of the Sout Europe were unable to implement environmental policy effectively for three main reasons: significant horizontal and vertical fragmentation of administrative structures and lack of coordination;[4] administrative shortcomings, as the style of policy is defensive and comes in contrary to the proactive approach required by EU environmental policies. In addition, a lack of qualified staff and the necessary infrastructure to implement the policy[5] as well as lax rules and outdated political values stand in the way of defending public matters, such as the environment. After all, political activism and environmental concern have emerged late in southern European societies.[6]

However, *Börzel* disputed the *Mediterranean syndrome* case, as it does not prove that lack of implementation is just a *disease* that afflicts the southern countries.[7] Without ignoring the particular problems of these states, she emphasises that they are not common in all four cases.[8] After all, comparative research between Germany

[1] See A. La Spina and G. Sciortino, 'Common agenda, Southern rules: European integration and environmental change in the Mediterranean states', in J.D. Liefferink, P.D. Lowe, and A.P.J. Mol (eds), *European Integration and Environmental Policy* (Belhaven, 1993), at 217

[2] See G. Pridham, 'Environmental policies and problems of European legislation in Southern Europe', (1996) 1 *South European Society & Politics*, 1

[3] Italy, Greece, Portugal, Spain.

[4] G. Pridham, 'Environmental policies and problems of European legislation in Southern Europe', (1996) 1 *South European Society & Politics*, 1, 52

[5] G. Pridham, 'Environmental policies and problems of European legislation in Southern Europe', (1996) 1 *South European Society & Politics*, 1, 53

[6] G. Pridham and M. Cini, 'Enforcing Environmental Standards in the European Union: Is There a Southern Problem', in M. Faure, J. Vervaele and A. Weale (eds), *Environmental Standards in the European Union in an Interdisciplinary Framework* (MAKLU, 1994), at 251

[7] See T. A. Börzel, 'Why there is no 'southern problem': On environmental leaders and laggards in the European Union', (2000) 1 *Journal of European Public Policy* 7

[8] *Ibid*, 144

and Spain has shown that compliance may differ between different sectoral policies, even within the same country.[1] Therefore, what is most valuable and determines the success of compliance is the degree of compatibility between European and national policy.

In the late 1990s, a second stream emerged from researchers studying Europeanisation. In an attempt to explain the different influences that the EU has on Member States,[2] most scholars have focused mainly on the implementation of environmental policy and have advanced the hypothesis that, the degree of compatibility between EU law and the existing institutional and regulatory traditions may influence EU law's effectiveness.[3] The general idea is that transposition and application are more difficult - if not impossible - if European policies and their impact on governance differ significantly from national institutional structures and acceptable operating standards.[4]

As *Knill*[5] and *Lenschow*[6] have argued, the compatibility of European and national structures depends not only on the nature of Community claims but also on the degree of consolidation of national administrative practices, such as and the capacity of Member States for administrative reform. Effective implementation is likely to occur when adaptation moves within the framework of "*rationality of appropriateness*"[7] (e.g., when European policy does not demand changes in the core of national administrative systems). There are three categories of adjustment pressure depending on the degree of compatibility: high, medium, and low. In the first case, implementation is likely to be ineffective, while when there is little or no pressure, effective implementation occurs, as European claims are in line with existing national practices. In cases of moderate pressure - where European demands call for change but do not challenge the core of national tradition - the

[1] *Ibid*, 141

[2] See A. Heritier, 'Differential Europe: The European Union impact on national policymaking', in A. Heritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A.-C. Douillet (eds), *Differential Europe: The European Union Impact on National Policy Making* (Rowman and Littlefield, 2001), at 1

[3] See T. A. Börzel, 'Why there is no 'southern problem': On environmental leaders and laggards in the European Union', (2000) 1 *Journal of European Public Policy* 7; See also T. Börzel and T. Risse, 'Conceptualizing the Domestic Impact of Europe', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanisation* (Oxford University Press, 2003), at 57; C. Knill, 'European Policies: The Impact of National Administrative Traditions', (1998) 1 *Journal of Public Policy* 18; C. Knill and A. Lenschow, 'Coping with Europe: The Impact of British and German Administrations on the Implementation of EU Environmental Policy', (1998) 4 *Journal of European Public Policy* 5; M. G. Cowles, J. Caporaso and T. Risse (eds.), *Transforming Europe: Europeanization and Domestic Change*, (Cornell University Press, 1998)

[4] O. Treib, 'Implementing and complying with EU governance outputs', (2014) 1 *Living Reviews in European Governance* 9, 8

[5] C. Knill, 'European Policies: The Impact of National Administrative Traditions', (1998) 1 *Journal of Public Policy* 18, 2

[6] See Knill and A. Lenschow, 'Coping with Europe: The Impact of British and German Administrations on the Implementation of EU Environmental Policy', (1998) 4 *Journal of European Public Policy* 5

[7] C. Knill, 'European Policies: The Impact of National Administrative Traditions', (1998) 1 *Journal of Public Policy* 18, 3-4.

implementation process is complicated, and the outcome depends on other factors, such as the preferences and resources of internal alliances, mediated by structures such as *signs of veto*.[1]

However, comparative studies have highlighted the *gap* between theory and reality, as the results of this case have been disappointing.[2] Several researchers have concluded that a good fit is either needless or inadequate for satisfactory compliance and conversely high incompatibility does not necessarily lead to negative results.[3] The main problem with this approach was that, in fact, few cases could be explained by focusing exclusively on compatibility between European requirements and national structures and practices. The findings of the empirical research of *Knill* and *Lenschow*, which examined the implementation of four directives in Germany and the United Kingdom, showed that only 3 out of 8 cases confirm their hypotheses.[4] For the rest of the cases, we need to include other explanatory factors in the analysis, such as: the structure of interests and the interaction of internal actors;[5] social mobilisation within[6] and points of veto;[7] the reform capacity of a country, which depends on consensus and supportive alliances;[8] consensual political culture and the learning factor;[9] the

[1] *Ibid*, 25

[2] E. Mastenbroek, 'EU compliance: Still a "black hole" ?', (2005) 6 *Journal of European Public Policy* 12, 1109

[3] See Knill and A. Lenschow, 'Coping with Europe: The Impact of British and German Administrations on the Implementation of EU Environmental Policy', (1998) 4 *Journal of European Public Policy* 5; See also A. Héritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A.-C. Douillet, *Differential Europe: New opportunities and restrictions for policymaking in the Member States* (Rowman and Littlefield, 2001); M. Haverland, 'National adaptation to European integration: The importance of institutional veto points', (2000) 1 *Journal of Public Policy* 20; G. Falkner, M. Hartlapp, and O. Treib, 'Worlds of compliance: Why leading approaches to European Union implementation are only "sometimes-true theories"', (2007) 3 *European Journal of Political Research*, 46; E. Mastenbroek, and M. Van Keulen, 'Beyond the goodness of fit. A preference-based account of Europeanization', in M. Haverland and R. Holzhacker (eds), *European Research Reloaded - Cooperation and Integration among Europeanized States* (Deventer, 2005), at 19

[4] C. Knill and A. Lenschow, 'Coping with Europe: The Impact of British and German Administrations on the Implementation of EU Environmental Policy', (1998) 4 *Journal of European Public Policy* 5, 600–602

[5] C. Knill and A. Lenschow, 'Modes of regulation in the governance of the European Union: Towards a comprehensive framework', (2003) 1 *European Integration online Papers (EIoP)* 7, 126

[6] See T. A. Börzel, 'Why there is no 'southern problem': On environmental leaders and laggards in the European Union', (2000) 1 *Journal of European Public Policy* 7

[7] See M. Haverland, 'National adaptation to European integration: The importance of institutional veto points', (2000) 1 *Journal of Public Policy* 20

[8] A. Héritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A.-C. Douillet, *Differential Europe: New opportunities and restrictions for policymaking in the Member States* (Rowman and Littlefield, 2001), 288

[9] M. G. Cowles, J. Caporaso, and T. Risse, *Transforming Europe: Europeanization and Domestic Change*,(Cornell University Press, 2001), 1

political will of governments and parliaments;[1] administrative inadequacy; as well as other variables related to the temperament of states.[2]

An earlier study by *Heritier* argued that Member States were trying to reduce adjustment costs by attempting to transpose their national model at European level.[3] Therefore, for governments that are unable to export their policies to Brussels, the cost of implementation is higher, and they are therefore reluctant to implement the policy. Relying on the rational approach, several scholars have highlighted the political will of governments, which is determined by the cost of adaptation as the main cause of delayed integration.[4] The problems arise because the implementation of European policies imposes significant costs on Member States.[5] Therefore, the greater the gap between European environmental policy and the corresponding national one, the higher the cost of adaptation and the lower the willingness of actors to comply.

According then to the pull-and-push model developed by *Börzel,* EU's law ineffectiveness is more likely to occur when EU policy causes a large *gap* and there is no mobilisation by internal actors to pressure public authorities to bear the cost of implementing the policy.[6] In particular, the greater the external pressure and the lower the degree of internal mobilisation, the more likely it is that Member States will not comply with supranational commitments.[7] However, government reluctance can be overcome if pressured from below (internal actors) and from above (European Commission and CJEU). That is to say, the attitude of the national government can change when there is a pull by internal actors who turn against the principles that do not comply with European commitments and a *push* by the Commission when it opens infringement proceedings.[8]

---

[1] E. Mastenbroek, and M. Van Keulen, 'Beyond the goodness of fit. A preference-based account of Europeanization', in M. Haverland and R. Holzhacker (eds), *European Research Reloaded - Cooperation and Integration among Europeanized States* (Deventer, 2005), at 19

[2] See G. Falkner, M. Hartlapp and O. Treib, 'Worlds of compliance: Why leading approaches to European Union implementation are only "sometimes-true theories"', (2007) 3 *European Journal of Political Research* 46

[3] See A. Héritier, '"Leaders" and "laggards" in European clean air policy', in F. van Waarden and B. Unger (eds), *Convergence or Diversity? Internationalization and Economic Policy* (Avebury, 1995), at 278

[4] See T. A. Börzel, 'Shaping and Taking EU Policies: Member States Responses to Europeanization', (2003) *Queen's Papers on Europeanization* 2; A. Héritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A.-C. Douillet, *Differential Europe: New opportunities and restrictions for policymaking in the Member States* (Rowman and Littlefield, 2001)

[5] T. A. Börzel, 'Shaping and Taking EU Policies: Member States Responses to Europeanization', (2003) *Queen's Papers on Europeanization* 2, 35

[6] T. A. Börzel, 'Why there is no "southern problem": On environmental leaders and laggards in the European Union', (2000) 1 *Journal of European Public Policy* 7, 141

[7] T. A. Börzel, 'Why there is no "southern problem": On environmental leaders and laggards in the European Union', (2000) 1 *Journal of European Public Policy* 7, 148–149

[8] T. A. Börzel, 'Shaping and Taking EU Policies: Member States Responses to Europeanization', (2003) *Queen's Papers on Europeanization* 2, 36

A research conducted by *Haverland*,[1] which examined the implementation of the Packaging Waste Directive in the Netherlands, Germany, and the United Kingdom, has shown that compliance depends on the number of institutional vetting points that allow domestic actors to favour or cancel the application. United Kingdom, the country with the widest gap between national practice and European requirements, has successfully implemented the directive, while Germany, where adjustment pressure has been relatively low, has encountered huge problems. Like *Börzel*,[2] *Haverland* attaches great importance to internal mobilisation.[3] However, he does not argue that governments are reluctant to implement the directives in the event of a policy gap. Regarding the role of mobilisation, reluctant governments may be forced to comply, while governments with the political will may be blocked by domineering actors.[4] While the case of veto players is presented as competing with that of compatibility, it essentially tries to combine them. The basic idea is that the *policy gap* is an important parameter for the effects of adjustment, as divergent policies generate huge internal reactions.[5] In contrast to other research,[6] *Haverland* argues that resistance does not come exclusively from governments and administrations, but from interests that are adversely affected.[7] Therefore, the number of vetoes determines whether or not opposition social actors can block implementation.[8]

According to the analysis of *Haverland*,[9] we should expect that Member States with a small number of institutional vetoes will perform well as regards compliance. Nevertheless, subsequent investigations have shown that the evidence does not confirm this hypothesis.[10] For example, Greece has as few vetoes as United

---

[1] See M. Haverland, 'The Impact of the European Union on Environmental Policies', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanization* (Oxford University Press, 2003), at 203; See also M. Haverland, 'National adaptation to European integration: The importance of institutional veto points', (2000) 1 *Journal of Public Policy* 20

[2] T. A. Börzel, 'Why there is no "southern problem": On environmental leaders and laggards in the European Union', (2000) 1 *Journal of European Public Policy* 7

[3] M. Haverland, 'The Impact of the European Union on Environmental Policies', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanization* (Oxford University Press, 2003), 203, 212

[4] M. Haverland, 'The Impact of the European Union on Environmental Policies', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanization* (Oxford University Press, 2003), 203

[5] O. Treib, 'Implementing and Complying with EU Governance Outputs', (2008) 5 *Living Reviews in European Governance* 3, 9

[6] T. A. Börzel, 'Why there is no "southern problem": On environmental leaders and laggards in the European Union', (2000) 1 *Journal of European Public Policy* 7; C. Knill and A. Lenschow, 'Coping with Europe: The Impact of British and German Administrations on the Implementation of EU Environmental Policy', (1998) 5 *Journal of European Public Policy* 4

[7] See M. Haverland, 'The Impact of the European Union on Environmental Policies', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanization* (Oxford University Press, 2003), at 203; See also M. Haverland, 'National adaptation to European integration: The importance of institutional veto points', (2000) 1 *Journal of Public Policy* 20

[8] M. Haverland, 'The Impact of the European Union on Environmental Policies', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanization* (Oxford University Press, 2003), at 203, 212

[9] *Ibid*

[10] See G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States*, (Cambridge University Press, 2005)

Kingdom, but its performance is much worse. In the Greek case, social mobilisation plays an important role, but from the point of view of informal vetoes,[1] which several times try to cancel the implementation in practice.

The conceptual weaknesses of the second stream gave rise to the third stream of literature on the implementation of European policies.[2] The complexity of the phenomenon, as well as the diversity of national implementation standards, requires pluralism in approaches and the integration of more explanatory factors in the analyses. Since one recipe does not cure all diseases, models that seek universality fail to offer solutions to all problems. The third current is characterised by the pluralism of theoretical and methodological approaches. The key feature that classifies all these different approaches in the same category is the attempt for a broader theoretical and empirical investigation to present a more complete picture of the conditions that determine the implementation processes.[3]

A new element, reintroduced by the third stream, is the impact of the the internal political game in terms of timing and correctness of adaptation to European demands.[4] *Treib* argued that it is not a rule "*that national actors always seek to maintain the status quo, as they often seek to change national structures and policies by using European pressure as an external constraint*"[5]. Therefore, we need in consideration the internal political situation in order to explain the Member States' compliance with the EU law.[6] In this context, *Treib* showed that the political preferences of the parties in government have a decisive influence on integration. *Mastenbroek* and *Kaeding* argued that research into the implementation of European policies should focus primarily on the preferences of key players in the domestic political arena,[7] while *Mastenbroek* and van *Keulen* emphasised that, if directives strengthen the preferences of governments, then they can remarkably bridge the policy gap.[8] The

[1] A. Heritier and C. Knill, 'Differential responses European policies: A comparison', in A. Héritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A.-C. Douillet (eds), *Differential Europe: The European Union Impact on National Policy Making* (Rowman and Littlefield, 2001), at 257

[2] O. Treib, 'Implementing and Complying with EU Governance Outputs', (2008) 5 *Living Reviews in European Governance* 3, 10

[3] O. Treib, 'Implementing and Complying with EU Governance Outputs', (2008) 5 *Living Reviews in European Governance* 3, 10

[4] See E. Mastenbroek, 'EU compliance: Still a "black hole" ?', (2005) 6 *Journal of European Public Policy* 12; See also O. Treib, 'EU governance, misfit and the partisan logic of domestic adaptation: an actor-centred perspective on the transposition of EU directives', (2003) *Paper presented at the EUSA 8th International Biennial Conference*, Nashville Tennessee, 27 – 29 March 2003.

[5] O. Treib, 'EU governance, misfit and the partisan logic of domestic adaptation: an actor-centred perspective on the transposition of EU directives', *Paper presented at the EUSA 8th International Biennial Conference*, Nashville Tennessee, 27 – 29 March 2003.

[6] G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States*, (Cambridge University Press, 2005), 329

[7] See E. Mastenbroek, E. and M. Kaeding, 'Europeanization beyond the goodness of fit: domestic politics in the forefront', (2006) 4 *Comparative European Politics* 4

[8] E. Mastenbroek, and M. Van Keulen, 'Beyond the goodness of fit. A preference-based account of Europeanization', in M. Haverland and R. Holzhacker (eds), *European Research Reloaded - Cooperation and Integration among Europeanized States* (Deventer, 2005), at 19, 38

above analyses focus mainly on the role of the actors, considering their preferences as a determining motivating or deterrent factor for compliance, and therefore it is a process that is shaped by their voluntary intentions.

Some researchers,[1] based on sociological institution, have emphasised the importance of existing national norms and beliefs. So, when external rules do not comply with national norms, then compliance takes more time, as it depends on a process of internalisation, through socialisation, persuasion and learning.[2] Therefore, delays in integration are explained by the time-consuming process of changing norms.[3] Drawing their arguments from theories of international relations, several studies have attempted to explain whether non-compliance is a strategic choice or a random uncontrollable situation stemming from structural weaknesses.

The first school,[4] known as the *enforcement approach*, considers that non-compliance is a conscious choice of states and therefore effective monitoring and severe punishment by supranational authorities can force reluctant countries to comply. On the other hand, the *management approach* argues that administrative deficiencies and lack of resources in Member States are the main causes for non-compliance.[5] Therefore, international organisations must help their members, through financial subsidies and educational programs, to become more effective. To bridge the two approaches, Beach argues that both strategic and regulatory factors influence compliance.[6] He therefore proposes a unifying compliance model, which will include both strategic calculations and other constraints.[7]

In one of the most comprehensive studies, Falkner *et al.* attempted to enrich the literature following a multifactorial approach.[8] Their model incorporates many variables, such as: administrative inadequacy, internal opposition, degree of compatibility, culture of compliance, as well as other temperamental elements.[9] According to this analysis, the degree of harmonisation of a country with the EU is determined by differences in domestic culture. These scholars argue that there are *three worlds of compliance*: the world of law compliance; the world

[1] See J.T. Checkel, 'Why comply? Social learning and European identity change', (2001) 3 *International Organization* 55; See also A.L. Dimitrova and M. Rhinard, 'The power of norms in the transposition of EU directives', (2005) 16 *European Integration Online Papers* 9

[2] See J.T. Checkel, 'Why comply? Social learning and European identity change', (2001) 3 *International Organization* 55

[3] See A.L. Dimitrova and M. Rhinard, 'The power of norms in the transposition of EU directives', (2005) 16 *European Integration Online Papers* 9

[4] See J. Tallberg, 'Paths to compliance: enforcement, management and the European Union', (2002) 3 *International Organization* 56; See also G. W. Downs, D. M. Rocke, and P. N. Barsoom, 'Is the good news about compliance also good news about cooperation ?', (1996) 3 *International Organization* 50

[5] See A. Chayes and A. Handler Chayes, 'On Compliance', (1993) 2 *International Organization* 47

[6] D. Beach, 'Why governments comply: An integrative compliance model that bridges the gap between instrumental and normative models of compliance', (2005) 1 *Journal of European Public Policy* 12, 113

[7] *Ibid*, 123

[8] See G. Falkner, M. Hartlapp and O. Treib, 'Worlds of compliance: Why leading approaches to European Union implementation are only "sometimes-true theories"', (2007) 3 *European Journal of Political Research* 46

[9] *Ibid*, pp. 401–404

of domestic politics and the world of neglect. In the first case, compliance with the law is a priority despite any concerns, as Member States are guided by a sense of duty. In the second case, in which internal concerns often prevail, compliance with European rules is one goal, among others. In the third case, compliance with the EU is not an objective. In the world of law enforcement, culture is the key factor, while in the other two worlds interests play a dominant role.[1]

§2. Domestic Factors Explaining the Transposition of Directives

Going further from general to specific, this paragraph presents the concepts, that will be used to analyse the transposition of the NIS directive. To explain the gaps in the levels of harmonization and compliance among the Member States of the EU, the present thesis retains the concept of misfit combined with a number of facilitating factors. Thus, I consider that a combination of the EU's regulatory leeway embedded in the content of the NIS directive with policy-specific factors, administrative factors, and political factors (**A**) under the approach of the *Goodness of fit* (**B**), is needed in order to explain the variation in transposition outcomes.

A. The Goodness of fit approach

Two dimensions should be considered when conceptualizing the goodness of fit approach. Regarding the first dimension, a differentiation is made between institutional and policy misfit.[2] The policy misfit refers to the content of the policies, while the institutional misfit refers to the "*regulatory style and structure of a particular policy sector*"[3]. Another distinction would relate to the legal and the practical *status quo*, since "*certain rules while being not laid down in law exist informally*"[4]. The particularity of the (mis-)fit approach is thus its consequent theoretical implications. The existence of a misfit is therefore considered by *Börzel* as a necessary condition for change. Since a misfit can be "*overcome by adaptational pressure from above such as infringement proceedings, or from below, in the form of domestic mobilisation*" [5].

---

[1] *Ibid*, p. 404

[2] T. A. Börzel and T. Risse, 'Conceptualising the domestic impact of Europe', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanization* (Oxford University Press, 2003), at 57–80

[3] C. Knill and A. Lenschow, 'Coping with Europe: The Impact of British and German Administrations on the Implementation of EU Environmental Policy', (1998) 4 *Journal of European Public Policy* 5, 597

[4] G. Falkner, 'Comparing Europeanization effects: from metaphor to operationalization', (2003) 13 *European Integration online Papers* 7, 3

[5] T. A. Börzel, *Environmental Leaders and Laggards in Europe: Why there is (not) a 'Southern Problem'* (Ashgate, 2003), 3

As already mentioned, Member States have the primary responsibility for the correct and timely transposition of the secondary EU law (regulations, directives, decisions), which is monitored by the European Commission. Where the Commission suspects a state of not fulfilling its obligations to implement EU law, it is "*empowered under the Treaty of Rome to launch infringement proceedings*"[1]. Transposition problems, especially regarding the directives, start as soon as the integration deadline has passed, and an infringement has been identified. In this context, there is a preliminary stage which precedes the infringement procedure under Article 258 TFEU, and which consists of a structured dialogue between the Commission and the Member State concerned, to identify and resolve problems in a timely manner and to avoid possible appeal to the CJEU.

If it is not possible to find a solution at an early stage through the speedy dispute resolution procedures, the Commission may initiate formal infringement proceedings and, where appropriate, refer the Member State to the CJEU in accordance with Article 258 TFEU. Infringement proceedings may also be initiated under other provisions of Union law, such as Article 106 in conjunction with Article 101 or 102 TFEU. The Commission shall bring an action before the CJEU against a Member State accused of violating an article of the Treaties, failing to transpose a directive, failing to implement a Regulation or a Decision, infringing the general principles of Union law or international agreements signed by the Union.

Infringement cases have been used by various studies as indicators for Member State's non-compliance with EU law.[2] Due to limited resources, the Commission cannot however lanch an infringement procedure in every case of non-compliance. Therefore, the result may underestimate the amount of non-compliance.[3] The availability of reliable data may also affect the detection of non-compliance with European Law. Since EU's Member States may not have a sufficient administrative capacity to control whether there is compliance with European legislation. Yet, Member States with high monitoring capacities show "*a low number of complaints and infringement proceedings opened while those with weaker administrative and scientific infrastructures, like Greece and Spain, find themselves at the upper end of the list*"[4]. The Commission has also strategic incentives

[1] See K. Davies, *Understanding European Union Law*, (Cavendish Publishing, 2001)

[2] See J. Tallberg, 'Paths to Compliance: Enforcement, Management and the European Union', (2002) *International Organization* 56, 609–643; See also T. A. Börzel, M. Dudziak, T. Hoffman, D. Panke and C. Sprungk, 'Recalcitrance, Inefficiency, and Support for European Integration: Why Member States Do (Not) Comply with European Law', (2007), *Harvard University Working Paper*; U. Sverdrup, 'Compliance and Conflict Management in the European Union: Nordic Exceptionalism', (2004) 1 *Scandinavian Political Studies*, 27

[3] See G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States*, (Cambridge University Press, 2005)

[4] T. A. Börzel, T. Hofmann and C. Sprungk, 'Why do states not obey the law? Non-compliance in the European Union', (2004) *Paper presented at the workshop 'Transposition and Compliance in the European Union'*, June11–13, Leiden, the Netherlands

to bring some cases and not others before the CJEU. Since Court's rulings may, in some cases, be more "*sensitive to the objections of powerful Member State's governments*"[1].

In order to provide explanations upon the compliances's deviations among EU's Member States, the misfit framework has become popular. *Börzel* and *Risse* consider the degree of (mis-)fit as the "*incompatibility between European-level processes, policies and institutions […] and domestic-level processes, policies and institutions*"[2]. The level of misfit then affects the compliance behaviour of Member States when transposing the EU rules. *Börzel* and *Risse* have therefore gauged the degree of misfit as the necessary condition on whether to expect or not a domestic change. When it comes to the operationalisation of the misfit, the authors are differenciating two kind of misfits. The institutional misfit, which "*describes the discrepancy between EU rules, procedures and the collective understandings attached to them, and the domestic ones*"[3] and the policy misfit, which refers to "*equal compliance problems*"[4]. I will therefore investifage the impact of those two types of misfits.

The goodness of fit approach seems not to be convicing. Many studies assert that a good fit is neither a reason for non-compliance nor a required condition for domestic adaptation.[5] The reason for this outcome may rely on the fact that the hypothesis is rather "*static in nature*[6]". Most proponents of the (mis-)fit thoery have tried preserving the latter while introducing secondary hypotheses allowing to take in consideration the domestic changes. For instance, *Héritier et al.* proposed a revised framework by considering the impact of Europe dependency, both, "*on the Member States pre-existing policies and on the dynamics of political processes*[7]". Specifically, they claim that variables such as the stage of liberalisation already present in a Member State or the national reform capacity and thirdly may affect the adjustment to European policies.[8]

[1] G. Garrett, R. D. Keleman and H. Schulz, 'The European Court of Justice, National Governments, and Legal Integration in the European Union', (1998) 1 *International Organization* 52

[2] T. Börzel and T. Risse, 'When Europe Hits Home: Europeanization and Domestic Change', (2000) 15 *European Integration online Papers* 4, 1

[3] T. Börzel and T. Risse, 'When Europe Hits Home: Europeanization and Domestic Change', (2000) 15 *European Integration online Papers* 4, 1

[4] *Ibid*, p. 5

[5] E. Mastenbroek, and M. Van Keulen, 'Beyond the goodness of fit. A preference-based account of Europeanization', in M. Haverland and R. Holzhacker (eds), *European Research Reloaded - Cooperation and Integration among Europeanized States* (Deventer, 2005), at 19

[6] E. Mastenbroek, *The politics of compliance: explaining the transposition of EC directives in the Netherlands*, Doctoral Thesis, Department of Public Administration, Faculty of Social and Behavioural Sciences (Leiden University, 2007)

[7] A. Héritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A.-C. Douillet, *Differential Europe: New opportunities and restrictions for policymaking in the Member States* (Rowman and Littlefield, 2001), 9

[8] *Ibid,* pp. 257–259

Based on formal competences of factual consensus capacity, *George Tsebelis* [1] assumed that "*the capacity for reform of a political system increases as the number of distinct actors whose agreement is necessary to pass such a reform decrease*". According to that model, three points explains the potential for political change: "*the number of veto players, the lack of congruence (dissimilarity of policy positions among veto players) and the cohesion (similarity of policy positions among the constituent units of each veto player) of these players*". A veto player is an individual or collective subject, whose consent is necessary for a change of policy, either because of his role in the Constitution or because of the position that this player has in the political game of government. Thus, the veto players of a country are divided into institutional ones, which arise from the Constitution (e.g., the Prime Minister, the Ministers) and party members, which arise from the political system (e.g., the different parties that participate in a governing coalition). Another distinction of veto player is in individual and collective. Individuals are players who are individuals such as the President in a presidential system, while collective players are referred to when collective actors, such as a committee, a party, or a parliament, are involved in the decision-making process. Contrary to the basic (mis-)fit argument, this approach is laying more on the political contestation between national reform promoters and opponents. However, the (mis-)fit argument is not sufficiently explained by the veto players approach.[2] While veto players were commonly used in opposition to the (mis-)fit approach,[3] I will disqualify this argument within my research design, since it could lead away from the perspective opted for my research approach. The level of regulatory leeway laid down in an EU provision may also influence the compliance deficit.

B. The influence of EU's Regulatory Leeway: Policy and Institutional Factors and Administrative Effectiveness

While more regulatory leeway may facilitate the adaptation of the European requirements to domestic gaps by a local policy actor. The regulatory leeway may become more complicate through a more political approach. Provisions that allow for several transposition strategies are expected then easing the transposition. Since the domestic implementers may operate few or no changes and thus, maintaining the national regulatory *status quo*. A situation that may lead to a delayed transposition by Member States and for which, scholars predict a negative relation between discretion granted and delayed transposition.[4] Therefore, higher are the levels of discretionary

[1] See G. Tsebelis, 'Decision- Making in Political Systems!: Veto Players in Presidentialism, Parliamentarism, Multicameralism and Multipartyism', (1995) 3 *British Journal of Political Science* 25, n°3

[2] See G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States* (Cambridge University Press, 2005)

[3] See M. Haverland, 'National adaptation to European integration: The importance of institutional veto points', (2000) 1 *Journal of Public Policy* 20

[4] See B. Steunenberg and D. Toshkov, 'Comparing transposition in the 27 Member States of the EU: the impact of discretion and legal fit', (2009) 7 *Journal of European Public Policy* 16

transposition allowed to Member States, the higher will be the domestic conflict and subsequently, the delays in the transposition process.[1] However, the observed delays in the transposition process are not necessarily related to the correctness of the transposition. Administrative bodies may also affect the period of transposition.

Domestic administration may conduct as policymakers an important part of the transposition outcome.[2] They may then (re)interpret "*the overarching norm to ensure that it fits their identities*"[3]. *Mastenbroek* and *Kaeding* argue that "*when following a logic of appropriateness, Member States conform to habits, i.e. patterns of behaviour acquired by frequent repetition*"[4]. What matters is thus "*not the fit [of EU policies] with the status quo, but the fit with the domestic belief system underlying that status quo*"[5]. Cases of non-compliance will occur if administrative resources are not sufficient or coordinated enough.

The three important streams of the new institutionalism delineated and the diversity of approaches for conceptually assessing compliance with EU directives illustrated, the next section presents the methodology retained, the selection of the case studies and the operationalisation of the three independent variables and the dependent variable as well.

Section II. Domestic Factors' Impact: An Analytical Framework

In the previous section, the effects of the domestic factors for legal compliance upon transposing process have been highlighted. In order to study these effects, a combination of the concept of Goodness of fit with facilitating factors such as political administrative and policy-specific factors was retained as an explicative framework on the variation in transposition outcomes. Following a deductive approach, I present the dependent variable and the three independent variables (**§1**), for which I express the hypotheses that will be measured in the Chapter II. Lastly, I outline also the methodological approach and explain the criteria upon cases studies selection (**§2**).

[1] See D. Epstein and S. O'Halloran, *Delegating Powers. A Transaction Costs Politics Approach to Policy Making under Separate Powers* (Cambridge University Press, 1999)

[2] See A. E. Töller, 'Measuring and comparing the Europeanization of national legislation: a research note', (2010) 2 *JCMS: Journal of Common Market Studies* 48

[3] See T. A. Börzel and T. Risse, 'From Europeanisation to diffusion: introduction', (2012) 1 *West European Politics* 35

[4] See E. Mastenbroek and M. Kaeding, 'Europeanization beyond the goodness of fit: domestic politics in the forefront', (2006) 4 *Comparative European Politics* 4

[5] See E. Mastenbroek and M. Kaeding, 'Europeanization beyond the goodness of fit: domestic politics in the forefront', (2006) 4 *Comparative European Politics* 4, 345

§1. Dependent and Independent Variables

A. The Dependent variable of Directives Regulatory Leeway: Between Flexibility and Discreteness

The dependent variable considered for the purposes of the present thesis is the usage of the directives regulatory leeway. Regulatory leeway matters for transposition. I therefore take in consideration two dimensions of regulatory leeway: the level of obligation and the level of discretion.

Regarding the extent of obligation, the inflexible instruments contained in directives refer to detailed substantive or procedural rules. On the other hand, whereas legally binding, the flexible mesures contained in European directives offer "*exemption and derogation possibilities or several policy options*"[1]. To avoid any confusion, the term *flexibility* in this context is not understood as synonymous with concepts of differentiated integration, to which it has been linked in the context of the theory and practice of European integration.

At a theoretical level, it has been linked, inter alia, to models of differentiated integration such as *Europe of many speeds*, *Europe a la carte*, *variable geometry*... At the institutional level, it is linked to the provisions introduced by the Amsterdam Treaty on enhanced cooperation in the field of non-exclusive competences of the Community.[2] The use of the term has been associated with phrases such as *flexibility means less Europe*,[3] but it is also used by proponents of European integration as a way of continuing the unification process, but also by defenders of national sovereignty who see it as a tool to undermine EU powers.[4] In the present context, regulatory flexibility should be seen as a process and not as a result of policy, given its potential for diversification[5] and diversity[6] on the European Union's path to an *undefined* destination.[7] It starts from a

[1] See E. Thomann, 'Customizing Europe: transposition as bottom-up implementation', (2015) 10 *Journal of European Public Policy* 22.

[2] Title IV, Article 20 of the TEU.

[3] For a thorough analysis of the academic debate on the dilemma of 'uniformity or flexibility', which arose especially after the revisions of the founding Treaties to the Treaty of Amsterdam, see for example G. De Búrca and J. Scott, *Law and New Governance in the EU and the US* (Irish Academic Press, 2006)

[4] G. De Búrca, and J. Scott, *Constitutional change in the EU: From Uniformity to Flexibility* (Hart Publishing, 2000), 10

[5] In the case of the European Union, differentiation between Member States has a broader and narrower meaning. On the one hand, it refers to cases where Member States are not subject to a single legal regime, even if the policy issue falls within the scope of the Treaties. On the other hand, the differentiation concerns cases where, under primary or secondary EU law, Member States may not be subject to the same rule, either because they are excluded from the scope or because some rules apply to some Member States and different rules to others. See J. Pelkmans, *European Integration: Methods and Economic Analysis* (Pearson Education Limited, 3rd edn, 2006), 53

[6] The special character of the European Union is also reflected in the phrase 'united in diversity' (unis dans la diversité), which was included in the preamble to the Treaty establishing a Constitution for Europe, in order to symbolize the common and at the same time diverse identity of the Union and refers to Declaration 52 annexed to the Treaty of Lisbon. The relevant literature states that the idea reflected in this phrase originates from Indian philosophy, cf. M. Lohse in Andenas and C. Andersen, *Theory and Practice of Harmonisation* (Edward Elgar Publishing, 2011), 308

[7] G. De Búrca, and J. Scott, *Constitutional change in the EU: From Uniformity to Flexibility* (Hart Publishing, 2000), 350 and 353

situation in which different regimes coexist, competing with each other, without being part of a single regulatory framework.

The specificity of the political nature and functioning of the European Union is reflected in the combined use and switching between regulatory convergence and regulatory flexibility, as demonstrated in the combination of the traditional tool of harmonising laws and regulatory regimes with flexible and mutual recognition, with which convergence is achieved through competition, but at the same time the diversity of national systems is ensured. The quality, forms, and characteristics of regulation change over time, but in each case the highest level of maturity requires more specific solutions through harmonisation. Contrary to the classic approach of to the discretionary variable on directive transposition,[1] the present thesis takes a qualitative approach on measuring the dependent variable throughout Member States' recurse to the regulatory leeway left by the NIS Directive to them. The measurement of the level of regulatory leeway will be then based on the extent to which Member States are transposing exactly the content of the NIS Directive.

The Member States of the EU are mostly inclined to make usage of the discretionary room granted to them, to adapt NIS directive following objectives pursued by national cybersecurity strategy. In the present research study, the extent to which Member States go beyond the minimum imposed by the directive is considered as a dependent variable, which is measurable. Naturally, mandatory provisions transposition is also assessed. Many NIS directive provisions allow Member States to decide how it is going to be *translated* into national transposition law.

To assess that may affect the extent to which Member States make use of the discretionary room allowed by the NIS Directive, a combination with policy, institutional misfit factors, as well as factors on administrative effectiveness is needed for interpretating the variation of the dependent variable and moreover, the transposition outcomes.

B. Independent Variables: Policy and institutional misfit

The arguments of the domestic interests approach are expressed throughout two independent variables, the domestic policies and institutional misfit (1), as well as the administrative effectiveness (**2**), for answering the research question of this thesis which is: *To which degree the domestic resistances may affect the transposition of the NIS Directive's provisions ?*

[1] See B. Steunenberg and D. Toshkov, 'Comparing transposition in the 27 Member States of the EU: The impact of discretion and legal fit', (2009) 7 *Journal of European Public Policy* 16; See also A. Zhelyazkova and R. Torenvlied, 'The successful transposition of European provisions by Member States: Application to the Framework Equality Directive', (2011) 5 *Journal of European Public Policy* 18

1. Institutional and Policy Misfit

The European directives always affect nation-specific policies, institutions, or processes. This is mostly due to Member States' institutions and policy traditions.[1]

Being one of first authors[2] addressing institutional misfit, *Knill* relates institutional misfit to "*the degree of institutionalisation or institutional stability of sectoral arrangements*"[3]. A such misfit can occur when European directives are privileging the Member States against domestic actor. I consider then that the degree of corporatism will express the extent institutional misfit in the cybersecurity policy area.

The misfit between EU policies and domestic policies constitutes a second type of misfit that may lead to compliance issues.[4] According to this, the contents of an EU Directive are not reflected in the relevant national law due to domestic policies. Thus, the policy misfit refers in the present thesis to the degree of incompatibility between the NIS Directive provisions and the domestic regulatory framerwoks, that were in place in Member States before the directive was adopted. An incompatibility which may lead to regulatory patchwork. Since those Member States that "*were not able to adjust their policies might not only need to change policies but also institutional structures*[5]". Therefore, greater is the misfit the lower the transposition outcome will be. The voluntary provisions will be disregarded from the research work, since they allow Member States to avoid transposing them. Considering the above developments on institutional and political misfit, I have formulated the following two hypotheses:

H1: *The higher the policy misfit, the greater the extent of the modifications by Member States and the divergences upon transposition outcome.*

[1] F. Duina, 'Explaining legal implementation in the European Union', (1997) *International Journal of the Sociology of Law* 25

[2] See F. Duina, 'Explaining legal implementation in the European Union', (1997) *International Journal of the Sociology of Law* 25; See also A. Héritier, D. Kerwer, C. Knill, D. Lehmkuhl, M. Teutsch and A.-C. Douillet, *Differential Europe: New opportunities and restrictions for policymaking in the Member States* (Rowman and Littlefield, 2001); T. Börzel and T. Risse, 'Conceptualizing the Domestic Impact of Europe', in K. Featherstone and C. Radaelli (eds), *The Politics of Europeanisation* (Oxford University Press, 2003), at 57

[3] See C. Knill, 'European Policies: The Impact of National Administrative Traditions', (1998) 1 *Journal of Public Policy* 18

[4] See T. A. Börzel, 'Towards convergence in Europe? Institutional adaptation to Europeanization in Germany and Spain', (1999) 4 *JCMS: Journal of Common Market Studies* 37

[5] E. Mastenbroek, *The politics of compliance: explaining the transposition of EC directives in the Netherlands*, Doctoral Thesis, Department of Public Administration, Faculty of Social and Behavioural Sciences (Leiden University, 2007)

H2: *The higher the degree of corporatism, the greater the extent of the modifications by Member States and the divergences upon transposition outcome.*

2. Administrative effectiveness

The present thesis research work aims to assess the impact of an domestic administration's inefficiency on the transposition outcome. Since it may affect both timeliness and correctness transposition of a directive.[1] *Pridham* argues that "*the southern countries 'Spain, Greece, and Italy' do have particular problems of administrative procedure and competence*". Member States with insufficient public resources or with a negative track record on timeless transposition may concentrate their efforts on the mandatory provisions.

In measuring the *government effectiveness*, I use the index developed in 1996 by the World Bank's researchers *Kaufmann et al*[2]. This measure refers to "*the quality of public services, the quality of civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies*"[3]. Numerous indicators such as the perceptions of governance by citizens and public and private sector experts are composing this index. This index is composed of three components: the performance-related pay for civil servants, the lack of permanent tenure, and the public advertising of open positions.

Regarding the NIS directive, administrative effectiveness could be assumed to affect the levels to which NIS mandatory provisions are transposed. Consequently, the third hypothesis formulated is:

H3 *The higher the administrative effectiveness, the lesser the extent of the modifications by Member States and the divergences upon transposition outcome.*

[1] See G. Ciavarini Azzi, 'The slow march of European Legislation: The implementation of directives', in K. Neunreither, and A. Wiener (eds), *European integration after Amsterdam: Institutional dynamics and prospects for democracy* (Oxford University Press, 2000), at 52; See also R. Thomson, 'Same effects in different worlds: The transposition of EU directives', (2009) 1 *Journal of European Public Policy* 16

[2] See D. Kaufmann, A. Kraay and M. Mastruzzi, *Governance Matters V: Aggregate and Individual Governance Indicators for 1996–2005* (The World Bank, 2006)

[3] *Ibid,* p. 4

§2. Research design

The theoretical approach of the present thesis being already translated into hypotheses, the following paragraph is establishing the research design of the present research. The first point outlines in detail the type of analysis on which the present thesis was based (**A**), as well as the selection methodology used for the case studies (**B**).

A. Qualitative based Analysis

The purpose of quantitative research is to highlight the reasons for changing social phenomena "*through objective measurement and numerical analysis*"[1]. Despite its diversity and sometimes conflicting assumptions about its inherent properties, several authors have attempted to capture the essence of qualitative research by offering various definitions based on its characteristics. The most representative definition is that of *Denzin and Lincoln*, according to which

> "*Qualitative research is an activity that places the observer in the world. This world is made up of a set of interpretations and material practices that make it visible. These practices turn people into performances, which include notes, interviews, photographs, recordings, and memos. At this level, qualitative research undertakes an interpretive, naturalistic approach to this world. This means that quality researchers study things in their natural world and try to interpret them from the point of view of the people themselves*".[2]

Both types of research seek answers to research questions, using the appropriate methodology, collecting and analysing data and drawing valid conclusions. Although methodological monism exists in the legal sciences, that is, there are common methodological principles, and there may be different techniques, there are some differences between quantitative and qualitative research. In summary, the differences between these two types of research relate in the general context, in the research subject, in the form of questions, in the form of data collected, and in design flexibility.

A key difference that is claimed to exist between quantitative and qualitative research is that the first form of research offers "*explanations' of reality (investigates the causal mechanisms that lead to behavioural differences between subjects, is guided by the logic of the cause-effect mechanism where a 'causal model' is*

[1] See J. W. Creswell and V.L. Plano Clark, *Designing and Conducting Mixed Methods Research* (SAGE Publications, 2nd edn, 2010)

[2] See N. K. Denzin and Y. S. Lincoln, *Handbook of Qualitative Research* (SAGE Publications Inc, 2000); See also J. Ritchie and J. Lewis, *Qualitative Research Practice - A Guide for Social Science, Students and Researchers* (SAGE Publications Inc, 2003)

distinguished and standardised based on which the independent and dependent variables are connected to an exact network of causal relationships), while the second form of research provides interpretations". Quantitative research seeks to discover (or invent) causal models that relate variables to each other (in the logic of poetic causality), while qualitative research seeks to detect typologies that refer to subjects (in the logic of classification). In other words, quantitative research answers the question why (why A has a different view from B, what is the reason that A behaves differently from B), while qualitative research answers the question how (describes the differences of position between of A and B interpreting them in the light of the general characteristics of the ideal types).[1] The present thesis is opting for a qualitative approach.

The collection of data was mainly operated throughout a qualitative document analysis and the expert's interviews. The main sources used in the present thesis the NIS directive, the domestic laws of transposition and the pocliy documents from national governments. Moreover, for a better understanding of the transposition outcome, I conducted ten semi-structured interviews with representatives from the European Commission, national administrations and other policy experts (*List of interviews available before appendix section*). The Chatham rules were applied for these interviews due to the sensitivity of the issue. Therefore, the present thesis will refer to them as *interview evidence*.

B. Case Study & Case Selection

In comparative literature, two main strategies are employed, that of *Most Similar Systems Design (MSSD)* and that of *Most Different Systems Design (MDSD)*, which were highlighted by *A. Przeworski* and *H. Teune*, the authors of *The Logic of Comparative Social Inquiry* and follows the comparative tradition of J. Stuart Mill (*A System of Logic, 1843*). The MSSD consists in comparing very similar cases that "*differ in the dependent variable, on the assumption that this will make it easier to find those independent variables which explain the presence/absence of the dependent variable*" [2]. While the MDSD is comparing very different cases with a same common dependent variable. Doing so, any exceptional circumstance that is present in all the cases can be regarded as the independent variable.

In the present research work, I follow the logic of the MSSD. Since the States studied here are similar in the sense that they are Member States of the European Union, subject to the same obligations, placed in a very similar political, economic and social context, because of their membership. But there may be some differences that will explain the differences in terms of transposition (more or less strong use of the regularoty leexway). The case studies were selected by combining three relevant dimensions on the European Union membership to

[1] A. Kaplan, *The conduct of inquiry: Methodology for behavioural science* (Chandler, 1964), 115

[2] A. Przeworski and H. Teune, *The Logic of Comparative Social Inquiry* (Wiley, 1970)

achieve maximum variance on: the successive EU enlargement rounds, the institutional setup of the political economy and the Member States cybersecurity preparedness and awareness.

Regarding the enlargement rounds, the European Economic Communities (EEC), known today as the European Union, was founded in 1952 by six Member States (France, Belgium, Italy, Germany, the Netherlands, and Luxembourg), and constitutes until today the *hard core* of the EU. Since 1952, the European Union (EU) has been continually gaining new members. Up to now, seven enlargement rounds have taken place.[1] Enlargement has strengthened the Union's weight in the world[2] and has made it a dynamic international partner (**Table 20**).

Enlargement groups				
Old Members	**1973 Enlargement**	**1981/86 Enlargement**	**1995 Enlargement**	**2004/07/13 enlargement**
Belgium	*Denmark*	*Greece*	*Austria*	*Bulgaria*
Germany	*Ireland*	*Portugal*	*Finland*	*Croatia*
France	*United Kingdom*	*Spain*	*Sweden*	*Cyprus*
Italy				*Czech Republic*
Luxembourg				*Estonia*
Netherlands				*Hungary*
				Latvia
				Lithuania
				Malta
				Poland
				Romania
				Slovakia
				Slovenia

Table 20: *Enlargement Groups*

(Table made by author)

[1] 1973 (Denmark, Great Britain, Ireland), 1981 (Greece), 1986 (Portugal, Spain), 1995 (Austria, Finland, Sweden), 2004 (Czech Republic, Cyprus, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, and Slovenia), 2007 (Bulgaria, Romania) and 2013 (Croatia).

[2] In 2020, the United Kingdom left the European Union, and currently, four countries from the Western Balkans are officially candidates for membership in the European Union: Northern Macedonia, Montenegro, Albania, and Serbia.

The second approach that I considered for the case selection is the institutional setup of the political economy. For this, the VoC-approach is used. Developed by Hall and Soskice,[1] the VoC-approach is based on assumptions about "*the links between the institutional configurations in a political economy and a country's stance towards regulation*"[2]. Following those developments three approaches are distinguishable. The first approach, the Liberal Market Economies (herafter LME), considers that liberal market economies are more incline to deregulation because "*this is favourable for domestic companies that coordinate their operations primarily through the market*"[3]. On the other hand, the second approach, the Coordinated Market Economies (hereafter CME) are likely to be more in favor of regulation "*because deregulation would endanger the institutional advantages of their nation's economy*"[4]. Authors identify a third one, sometimes described as *Mediterranean* (e.g., Cyprus[5], France, Greece, Italy, Portugal and Spain), marked by "*a large agrarian sector and recent histories of extensive state intervention that have left them with specific kinds of capacities for non-market coordination in the sphere of corporate finance but more liberal arrangements in the sphere of labour relations*"[6]. The VoC literature on Central and Eastern Europe (CEE) countries often cites *Nölke* and *Vliegenthart* who believe that "*the economies of most countries in the region are not accurately described by the LME and the CME models*" [7]. Instead, they are *Dependent Market Economies* (DME), which is characterised by the importance of foreign capital for the socioeconomic setup and is in post-socialist Central Europe (**Table 21**).[8]

[1] See P. A. Hall and D., Soskice, 'An Introduction to Varieties of Capitalism', in P. A. Hall and D. Soskice (eds), *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage* (Oxford University Press, 2001), at 1

[2] See P. A. Hall and D., Soskice, 'An Introduction to Varieties of Capitalism', in P. A. Hall and D. Soskice (eds), *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage* (Oxford University Press, 2001), at 1

[3] P. A. Hall and D., Soskice, 'An Introduction to Varieties of Capitalism', in P. A. Hall and D. Soskice (eds), *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage* (Oxford University Press, 2001), at 1, 58; See C. Buchen, 'Estonia and Slovenia as Antipodes', in: D. Lane and M. Myant (eds), *Varieties of Capitalism in Post-Communist Countries* (Palgrave Macmillan,2007), at 65

[4] P. A. Hall and D. Soskice, 'An Introduction to Varieties of Capitalism', in P. A. Hall and D. Soskice (eds), *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage* (Oxford University Press, 2001), at 1, 52

[5] See A. Pegasiou, 'The Cypriot Economic Collapse: More Than a Conventional South European Failure', (2013) 3 *Mediterranean Politics* 18

[6] P. A. Hall and D. Soskice, 'An Introduction to Varieties of Capitalism', in P. A. Hall and D. Soskice (eds), *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage* (Oxford University Press, 2001), at 1, 21

[7] A. Nölke and A. Vliegenthart, 'Enlarging the Varieties of Capitalism: The Emergence of Dependent Market Economies in East Central Europe', (2009) *World Politics* 4

[8] See K. Jasiecki, 'The Nature of Capitalism in Poland. Controversy over the Economy since the end of 2015: The Prospects of Business Elite and Employer Associations', (2017) 3 *Corvinus Journal of Sociology and Social Policy* 8

VoC Approach			
Liberal Market Economies	**Coordinated Market Economies**	**'Mediterranean' economies**	**Dependent Market Economies**
Estonia	*Austria*	*Cyprus*	*Czech Republic*
Ireland	*Belgium*	*France*	*Hungary*
Slovenia	*Denmark*	*Greece*	*Poland*
United Kingdom	*Finland*	*Italy*	*Slovak Republic*
	Germany	*Portugal*	
	Luxembourg[1]	*Spain*	
	Netherlands		
	Norway		
	Sweden		

Table 21: *VoC Approach*

(Table made by author)

Regarding my third approach upon case studies' selection, cybersecurity awareness or preparedness refers to "*users' attention to security issues online or their understanding of and commitment to security*"[2]. No comprehensive ranking of countries in cybersecurity exists yet, as far as we know. *Seungeun Lee* and *Kim* propose however a typology of "*cross-country profiles of cybersecurity preparedness*"[3]. Based on the analysis of samples of adults from thirty European samples in the Eurobarometer 2014, a region-wide nationally representative survey; the authors propose three models with regard to states preparedness in the area of cybersecurity: *well-prepared*, *moderately prepared*, and *less prepared* countries (**Table 22**).

Cybersecurity Preparedness		
Well prepared	**Moderately prepared**	**Less prepared**
Denmark	*Austria*	*Bulgaria*
Luxembourg	*Belgium*	*Cyprus*
Sweden	*Croatia*	*Greece*
Netherlands	*Czech Republic*	*Hungary*
	Estonia	*Italy*
	France	*Lithuania*
	Finland	*Malta*
	Germany	*Poland*
	Ireland	*Portugal*
	Latvia	*Romania*
		Slovakia
		Spain

Table 22: *Cybersecurity Preparedness*

(Table made by author)

[1] See J. Ahrensa, R. Schweickertb and J. Zenkerc, 'Varieties of capitalism and government spending in developed and developing countries', (2015) 1 *Journal of Economic Development* 40

[2] See S. Hansche, 'Designing a security awareness program: part I', (2008) 1 *Information System Security* 10

[3] C. Seungeun Lee and J. H. Kim, 'Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts', (2020) *Computers & Security* 97, 5

After taking these factors into account, France, Finland, Greece, Ireland, Luxembourg, Poland were selected as case studies. This strategy is based on the identification of similarities between otherwise different cases and thus identify the independent variable affecting the transposition outcome. Instead of controlling for extraneous variance, the strategy's goal is to eliminate as many external variables as possible from the analysis, instead of trying to control their variance.[1] While these six countries share a common membership within the EU, they differ considerably on the EU Enlargement round they belong to, their cybersecurity preparedness and awareness, and the institutional setup of their political economy.

France and Luxembourg are figuring among the oldest members of the EU. While Ireland, Greece, and Finland entered consequently one after the other in the EU, with Poland being part of the latest enlargement round. The selection of France, Finland, Greece, Ireland, Luxembourg, and Poland as case studies was the most prominent choice which helps conserve equal representativeness from the other two criteria groups. France, Finland, and Ireland are moderately prepared on cybersecurity preparedness and awareness. While Luxembourg belongs to the well-prepared group and Greece and Poland to the less prepared one. Concerning the Institutional setup of the political economy Greece and France belong to Mediterranean economies. While Finland and Luxembourg belong to coordinated market economies, Ireland to Liberal market economies and Poland to Dependent market economies (**Table 23**).

	Achieved case selection variance		
	EU membership	**Cybersecurity preparedness and awareness**	**Institutional setup of the political economy**
France	*Old member*	*Moderately prepared*	*Mediterranean*
Finland	*New member (3rd group)*	*Moderately prepared*	*Coordinated market economy*
Greece	*New member (2nd group)*	*Less prepared*	*Mediterranean*
Ireland	*New member (1st group)*	*Moderately prepared*	*Liberal market economy*
Luxembourg	*Old member*	*Well prepared*	*Coordinated market economy*
Poland	*New member (4th group)*	*Less prepared*	*Dependent market economy*

Table 23: *Case studies selection variance*

(Table made by author)

In Chapter I, the theoretical debates upon the limiting effect of the domestic factors on the transposition outcome were presented. It should be remembered that compliance refers to "*a state of conformity or identity*

[1] See B. Guy Peters and G. Fontaine, *Handbook of Research Methods and Applications in Comparative Policy Analysis* (Edward Elgar Publishing, 2020)

between an actor's behaviour and a specified rule"[1]. In studies based on legal explanatory factors, the complexity and poor quality of directives, the characteristics of national constitutions, as well as the extent and diversity of existing national legislation, were classified as the main reasons for countries' non-compliance with Community legislation. The choices, perceptions and reactions of national actors to European pressures and stimuli cannot be interpreted without understanding the creation and evolution of national rules, practices and restrictions that constitute a complex of formal and informal institutions. The adaptation of identities and institutions to an external environment may be affected by internal forces.[2] Therefore, the outcome of actions and policies is determined not only by external pressures, but also by internal factors such as domestic factors.

In this context Börzel viewed a misfit as "*a necessary condition for change. Her main argument is that a misfit can be overcome by adaptational pressure from above such as infringement proceedings, or from below, in the form of domestic mobilisation*"[3]. To explain the gaps in the transposition outcome among the Member States of the EU, the present thesis made therefore the choice of explaining the Member States' usage of regulatory leeway (dependent variable) embedded in the content of the NIS directive with policy-specific factors, administrative factors, and political factors under the approach of the *Goodness of fit*, which is needed for highlighting the gaps in transposition outcomes. Following deductive reasoning, four variables were identified as relevant for the comparative analysis: the usage of the regulatory leeway of the directive, the policy and institutional misfit and the administrative effectiveness. My selection of case studies was at last directed on the following six countries: France, Finland, Greece, Ireland, Luxembourg, Poland. A selection which is representative of the three dimensions of the European Union membership: the successive EU enlargement rounds, the institutional setup of the political economy and the Member States cybersecurity preparedness and awareness. The theoretical framework for the conduction of the thesis research work being defined, it is time now to go on the practical part of the thesis, the empirical analysis of the NIS Directive transposition.

[1] See B. Guy Peters and G. Fontaine, *Handbook of Research Methods and Applications in Comparative Policy Analysis* (Edward Elgar Publishing, 2020), at 539

[2] See J. March and J. Olsen, 'The Institutional Dynamics of International Political Orders', (1998) 4 *International Organization* 52

[3] E. Mastenbroek, *The politics of compliance: explaining the transposition of EC directives in the Netherlands*, Doctoral Thesis, Department of Public Administration, Faculty of Social and Behavioural Sciences (Leiden University, 2007).

Chapter II. The Impact of Domestic Factors: an Empirical Analysis of NIS Directive Transposition

The following chapter will perform a comparative analysis of transpositions outcomes in selected case studies. A detailed comparative account will therefore be offered on how Finland, France, Greece, Ireland, Luxembourg, and Poland transposed the NIS Directive requirements in the policy area of cybersecurity (**Section I**). A second section will finally explain the transposition variance, by testing the relevance of three factors for explaining the differences between the transposition outcomes that were put forward in the previous chapter (**Section II**).

Section I. The Transposition of Provisions providing for Minimum Harmonisation

This section in its first paragraph presents existing NIS legal framework and institutional governance schemes for Finland, France, Greece, Ireland, Luxembourg, and Poland (**§1)**. While the second paragraph offers a comparative analysis for two sets of obligation at the time of the NIS Directive transposition, the obligation of the *Due Time* transposition and the NIS Directive provisions on minimum harmonisation (**§2**). At last, the third paragraph presents the dependent variable outcome on the usage of discretionary room granted to the Member States (**§3**).

§1. The Country's NIS Framework upon transposition Background

Comparative NIS policy, institutional and organisational framework between the selected Member States of the EU will shed light to Member States' background prior to transposition. Thus, the following themes will be presented for each case study: National Cybersecurity Strategies and Policies, the Legal Framework and National authorities.

A. Finland

1. National Cybersecurity Strategy and Policies

The first cross-administrative strategy (Strategy for Securing the Functions Vital to Society) was presented in 2003.[1] The strategy was in the form of a government resolution, and it described the preparedness threat scenarios, strategic tasks of the ministries and the principles for leadership in a crisis. The next update of the strategy took place in 2006 and on this occasion, attention was on the management of incidents, and an extensive matrix to support emergency preparedness planning was presented. In 2010, the strategy was renamed the Security Strategy for Society.[2]

In January 2013, Finland's Cyber Security Strategy was also published as a Government Resolution.[3] According to this document, Finland's vision of cybersecurity relies on ensuring the vital functions of cyberspace in all situations. The strategy covers 14 of the 15 strategic goals in the ENISA self-assessment classification. These strategic goals are Cybercrime; security with privacy balance; citizen awareness; critical information infrastructure protection; national cyber contingency plans; international cooperation; public-private partnership; incident response capability; baseline security requirements; incident reporting mechanisms; R&D; cyber security exercises; incentives for the private sector to invest in security measures; training and educational programmes. On March 11th, 2014 the Security Committee adopted the first Implementation Programme and since then has regularly evaluated the realisation of the Programme.

Based on the assessment of the aforementioned programme, the Security Committee decided on 14 March 2016 to update the Implementation Programme for Finland's Cyber Security Strategy 2017–2020[4] as an expression of the national ambition. The adopted Information Security Strategy for Finland sets out the objectives and measures to enhance the level of trust to Internet and digital practices. It focuses on the development of cybersecurity within the service complex of the state, counties, municipalities, the business sector and the third sector where the individual citizen is the customer. The business community provides most digital services and their cyber security through international service complexes and networks. The strategy also deals with matters that damage trust such as digital security incidents and also partly covers the area of cybercrime.

[1] The Finnish Security and Defence Committee, 'The Strategy for Securing the Functions Vital to Society', Government Resolution, 23 November 2006, available at https://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf (accessed on March 5th, 2021)

[2] The Finnish Security and Defence Committee, 'Security Strategy for Society', Government Resolution, 16 December 2010, available at https://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf (accessed on March 5th, 2021)

[3] The Finnish Security and Defence Committee, 'Finland´s Cyber security Strategy', Government Resolution, 24 January 2013, available at https://www.cyberwiser.eu/sites/default/files/FI_NCSS_en.pdf (accessed on March 5th, 2021)

[4] The Finnish Security and Defence Committee, 'Implementation Programme for Finland's Cyber Security Strategy for 2017–2020', Government Resolution, 24 January 2013, available at https://turvallisuuskomitea.fi/wp-content/uploads/2018/10/Implementation-programme-for-Finlands-Cyber-Security-Strategy-for-2017-2020-final.pdf (accessed on March 5th, 2021)

In its plenary session on October 3rd, 2019, the Finnish Government adopted a resolution on Finland's cyber security strategy. The Cyber Security Strategy 2019[1] sets out the key national objectives for the development of the cyber environment and the safeguarding of related vital functions. The reform and implementation of the strategy are based on the Government Programme. The three strategic guidelines are the following: international cooperation, better coordination of cyber security management, planning and preparedness, and developing cyber security competence. A cyber security development programme extending beyond government terms will improve the allocation of resources and improvement of cooperation for cyber security. The programme will concretise national cyber security policies and clarify the overall picture of cyber security projects, research, and development programmes. The post of Cyber Security Director will be established at the Ministry of Transport and Communications to coordinate the national development of cyber security. The strategy is based on the general principles of Finland's cyber security strategy of 2013.

2. Legal Framework

i. Critical Information Infrastructure Protection

The critical sectors and the protection policies for critical infrastructures are defined in the Security of Supply Act[2] and in the Decree of the National Emergency Supply Agency (NESA) of 1992. The Security of Supply Act is the legal basis for ensuring supplies of various basic materials in the case of emergency situations.

Based on these acts, the Finnish government sets official goals for the development of security of supply, which are updated every 5–6 years. The Government Decision on the Security of Supply 2008[3] is the latest set of official goals and standards relating to the protection of critical infrastructure. Section 2.2 of the decree addresses critical information technology infrastructure. Currently, the following infrastructures and services are deemed to be critical in Finland: Energy Networks and Supply, Electronic Information and Communication Systems, including communication networks, IT systems (including Supervisory Control and Data Acquisition - SCADA - systems), electronic mass media, and payment systems of banks and insurances, Transportation and Logistics Systems, Water supply and Other Municipal Utilities, Infrastructure Construction and Maintenance, Financial Services, Food Supply, Health Services and Print Media.

[1] The Finnish Security and Defence Committee, 'Finland´s Cyber security Strategy 2019', Government Resolution, 3 October 2019, available at https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf (accessed on March 5th, 2021)

[2] Laki huoltovarmuuden turvaamisesta 18.12.1992/ 1390, available at https://www.finlex.fi/fi/laki/ajantasa/1992/19921390 (accessed on March 5th, 2021)

[3] Valtioneuvoston päätös huoltovarmuuden tavoitteista 21.8.2008/539, available at https://www.finlex.fi/fi/laki/ajantasa/2008/20080539 (accessed on March 5th, 2021)

ii. Electronic Communications

In Finland, the following acts regulate e-commerce in addition to general statutes. The Consumer Protection Act 38/1978,[1] which is applicable to e-commerce and contains requirements on the information to be provided to consumers. Information requirements enacted in the Act applies both prior to the conclusion of the sales contract and during the order process, as well as regarding the consumers' right to receive a refund.

The Act on Strong Electronic Identification and Electronic Trust Services 617/2009,[2] which regulates strong electronic identification, electronic signatures, and the offering of these services to service providers using them and to the general public.

The Act on the Provision of Information Society Services (512/2011)[3] entered into force on 1 June 2011. The main issues concerning the freedom to provide information society services, the information requirements for service providers, the electronic orders and electronic contracts, as well as related obligations. The law transposes the EU e-commerce directive (2000/31 / EC).

Finally, the Act on Electronic Communications Services 917/2014[4] of January 1, 2015, which aims to, inter alia, ensure the confidentiality of electronic communication and the protection of privacy. The Act 917/2014 is an umbrella act that consolidates, updates and streamlines the regulation of electronic communications. It is a result of a large reform and entered into force on 1 January 2015. It also regulates, among other things, the provision and offering of information society services, including distance selling, information to be provided by the service provider, electronic direct marketing, cookies as well as protection of privacy and information security.

3. National Authorities

i. Ministry of Transport and Communications

[1] Kuluttajansuojalaki, 20.1.1978/38, available at https://finlex.fi/en/laki/kaannokset/1978/en19780038 (accessed on March 5th, 2021)

[2] Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 7.8.2009/617, available at https://finlex.fi/en/laki/kaannokset/2009/en20090617 (accessed on March 5th, 2021)

[3] Laki tietoyhteiskunnan palvelujen tarjoamisesta annetun lain 15 §:n muuttamisesta 512/2011, available at https://www.finlex.fi/fi/laki/alkup/2011/20110512 (accessed on March 5th, 2021)

[4] Tietoyhteiskuntakaari 917/2014, available at https://www.finlex.fi/fi/laki/kaannokset/2014/en20140917 (accessed on March 5th, 2021)

The Ministry of Transport and Communications is responsible for the legislation's implementation and the development of information security strategies on NIS security. With Finland's Cyber Security Strategy 2019 a post of Cyber Security Director will be established at the Ministry of Transport and Communications to coordinate the national development of cyber security. The role of the Cyber Security Director will be to ensure the coordination of the development, planning and preparedness of cyber security in society. The Cyber Security Director also acts as an adviser to the central government in cyber security related matters. Under their leadership, the overall picture and development programme of cyber security will be developed, drawing on the expertise of ministries, the Security Committee and cyber security actors.

ii. Ministry of Finance

The Finnish Ministry of Finance[1] has overall responsibility for guiding and developing information security in the Government of Finland.[2] The Ministry of Finance is responsible for the guidance of joint basic ICT services of government agencies. Service provision is based on the Act and Decree on the Provision of Shared Government Information and Communications Technology Services[3] [4] and the Act and Decree on the Operation of the Government Security Networks. [5] [6] The Ministry of Finance has also established the Government Information Security Management Board (VAHTI) on issues related to cooperation and the development of information security in the central government.[7] The task of the Information Management Board is to promote the implementation of information management and data security procedures laid down in the Act on Public Administration Information Management and to ensure that the requirements of the Act are met. The Information Management Board is not a general authority for information management; its tasks are related to the Act on Public Administration Information Management.

---

[1] Valtiovarainministeriö

[2] Finnish Ministry of Finance, 'Digital security: Guidance of services and security', available at https://vm.fi/en/information-security-and-cybersecurity (accessed on March 5th, 2021)

[3] Laki

valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 1226/2013, available at https://finlex.fi/fi/laki/alkup/2013/20131226 (accessed on March 5th, 2021)

[4] Valtioneuvoston asetus

valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 132/2014, Available at https://www.finlex.fi/fi/laki/alkup/2014/20140132 (accessed on March 5th, 2021)

[5] Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015, available at https://finlex.fi/fi/laki/alkup/2015/20150010 (accessed on March 5th, 2021)

[6] Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015, available at https://www.finlex.fi/fi/laki/alkup/2015/20151109 (accessed on March 5th, 2021)

[7] Available at https://vm.fi/en/information-management-board (accessed on March 5th, 2021)

iii. Finnish Transport and Communications Agency (TRAFICOM)

The Finnish Transport and Communications Agency (TRAFICOM)[1] is a government agency under the Ministry of Transport and Communications and acts as a national authority for information security. Known as Finnish Communications Regulatory Authority (FICORA) until January 2019, TRAFICOM's mission is to build the connections that keep people, data and goods moving smoothly, securely, and sustainably. It consists of four Areas of Expertise (Services for Motorists, Transport System Services, Digital Connections, National Cyber Security Centre Finland) and three Impact Networks (Efficient Traffic and Transport for the Future, Sustainable and Clean Environment, Transport Market).

The goals of TRAFICOM's supervision are to recognise problems on time and prevent them; settle matters in cooperation with players, but by ensuring the confidentiality of the information; act in such a manner that the effects of the measures are as effective as possible and apply to a large group; act flexibly in such a manner that unnecessary litigations are avoided; invest in steering and supervision of basic services; and to issue, always when necessary, a written decision which may be appealed to an administrative court.

TRAFICOM also works as a single contact and information point on free flow of data in Finland. As such, it gives advice on the free flow of data and data localisation restrictions in Finnish legislation and transmits data requests from authorities in other EU countries to relevant competent authorities in Finland. The legislation supervised by TRAFICOM does not concern the content of communications at all, for example the content provided on the internet. However, requirements concerning the program content have been imposed on television and radio operators, and on providers of Video-on-Demand services.

iv. National Cyber Security Centre Finland (NCSC-FI)

The National Cyber Security Centre of Finland (NCSC-FI)[2] was established in 2014 through a merger of CERT-FI and NCSA-FI. The Finnish national CERT (CERT-FI), [3] whose task is to promote security in the information society by preventing and resolving security incidents and disseminating information on information security threats, was integrated into the new NCSC-FI Cybersecurity Centre on January 1st 2014, along with NCSA-FI.[4]

[1] Available at https://www.traficom.fi/en/ (accessed on March 5th, 2021)

[2] Available at https://www.kyberturvallisuuskeskus.fi/en/ (accessed on March 5th, 2021)

[3] Available at https://www.kyberturvallisuuskeskus.fi/en/our-activities/cert (accessed on March 5th, 2021)

[4] Available at https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa (accessed on March 5th, 2021)

The NCSC-FI, which is a sub-agency of the FICORA, acts as the national competent authority for network and information security. The body is responsible for coordination of incident response and information security measures for both government institutions and the private sector. It monitors cyber security risks for gathering, processing, and communicating information with other partners. NCSC-FI also provides guidelines, advice, and tips (guidelines and recommendations service). These materials are intended to organisations, individuals as well as service administrators and they are available on organisation's website.

NCSC-FI collects and correlates information from a variety of sources. Finnish telecommunications service providers are required by law to report information security incidents to the NCSC-FI. By law, threats to information security must also be reported. The NCSC-FI also requests voluntary reports from all other public and private sector organisations, as well as from individuals. The centre is highly networked and comes into daily contact with private sector organisations and various government agencies in Finland and abroad. CERT-FI cooperates with national and international CERTs and with representatives of trade and industry, as well as with the public administration.

v. National Emergency Management Agency

The National Emergency Management Agency (NESA)[1] is a central government organisation operating under the Ministry of Economic Affairs and Employment of Finland. Its strategic tasks are to coordinate preparedness cooperation between the private and public sectors; oversee the practical arrangements related to the maintaining of national emergency stockpiles and security and compulsory stockpiles; ensure the functionality of essential technical systems and safeguard critical goods and service production; and to monitor international developments and maintain contact with foreign authorities and institutions. The key pieces of legislation governing security of supply are the Act on the Measures Necessary to Secure Security of Supply (1390/1992)[2] and the Government Decree on the National Emergency Supply Agency(1048/2018).[3]

The operations of the National Emergency Supply Agency are steered by the NESA's Board of Directors. The NESA's operative activities are managed by the chief executive officer based on guidelines issued by the Board of Directors. The CEO is supported by the management team and communications manager and provided with strategic support by the planning manager. The NESA's organisation includes the Primary Production Department, the Energy Supply Department, the Infrastructure Department, the Planning and Analysis

[1] Huoltovarmuuskeskus. Available at https://www.huoltovarmuuskeskus.fi/en (accessed on March 5th, 2021)

[2] Laki huoltovarmuuden turvaamisesta 18.12.1992/ 1390

[3] Valtioneuvoston päätös huoltovarmuuden tavoitteista 1048/2018, available at https://www.finlex.fi/fi/laki/alkup/2018/20181048 (accessed on March 5th, 2021)

Department and the Administration Department. The NESA employs just over 50 people, the majority of whom are experts in various fields.

vi. Police of Finland

The police are the competent authority for carrying out investigations related to cybercrime.[1] The police generate an analysed, high-quality cybercrime situation picture. The police cooperate closely with the National Cyber Security Centre. International operational cooperation and the exchange of information take place with the EU and with other countries' corresponding law enforcement officials, such as the Europol.

vii. Office of the Data Protection Ombudsman

The Data Protection Ombudsman is a national supervisory authority which supervises the compliance with data protection legislation. With Data Protection Ombudsman and two Deputy Data Protection Ombudsmen there are approximately 40 specialists in the office. The Data Protection Ombudsman is an autonomous and independent authority who is appointed by the government. Their term of office is five years. The Data Protection Ombudsman and deputy data protection ombudsmen form the Sanctions Board tasked with imposing administrative fines in accordance with the General Data Protection Regulation. The Board is chaired by the Data Protection Ombudsman. The Expert Board, operating in connection with the Office of the Data Protection Ombudsman, is tasked with issuing statements on significant questions related to the application of the legislation governing the processing of personal data at the request of the Data Protection Ombudsman. The term of the Expert Board began on 1 October 2020 and will end on 30 September 2023. Data Protection Ombudsman represents Finland in the European Data Protection Board.

B. France

1. National Cyber Security Strategy and Policies

Public authorities' awareness of IT security issues began in the 2000s. Among the first initiatives, we include the plan to strengthen the security of state information systems, decided by the French Prime Minister in 2004, *Jean-Pierre Raffarin*. In 2005, the deputy *Pierre Lasbordes* wrote a report on "*The security of information*

[1] Available at https://poliisi.fi/en/investigating-cybercrime (accessed on March 6th, 2021)

systems - A major issue for France", made public in January 2006.[1] For the first time, the approach goes beyond the only perimeter of the State's information systems to also assess the question of the vital infrastructures necessary for the country and includes the business world. The report already concludes that France is lagging in this area and notes several points: the dispersion and autonomy of the various actors within state services, insufficient resources, and vulnerable businesses. The computer attack against Estonia in 2007 as well as the attack on several French state services (in particular diplomats stationed in embassies) caused general awareness which attracted the interest of the Senate. Senator Roger Romani thus published in July 2008 a report on cyber defence, the first official document to address the subject in depth.[2] Almost simultaneously, in June 2008, the White Paper on Defence and National Security raised the issue,[3] identifying priorities, including cyberattacks as one of the main threats to national territory.

In February 2011, France issued its first National Strategy for the Defence and Security of Information Systems.[4] The strategy had four main objectives: to make France a world power in cyber defence, while maintaining its autonomy, to guarantee freedom of decision-making with the protection of national sovereignty information, to strengthen the security of critical infrastructure and to achieve cyber security. In order to achieve these goals, seven axes were selected: a better forecasting and analysis of the environment, in order to make appropriate decisions; identify and deal with attacks, warn potential victims and provide assistance; increase of scientific, technical and industrial skills, in the direction of maintaining the necessary autonomy; protection of state information systems and infrastructure operators vital to better national resilience; adapt laws to take account of technological developments; development of international cooperation in the fields of information systems security, the fight against cybercrime, and cyber defence; communication and information so that French citizens can better understand issues related to the security of information systems.

In 2015, France adopted a *National Strategy for Digital Security*[5] intended to support the digital transition of French society. In terms of security, it highlights the provision of a strong response against acts of cyber-malware and aims to make digital security a competitive advantage for French companies. It responds to the

[1] P. Lasbordes, 'La sécurité des systèmes d'information : un enjeu majeur pour la France', [Rapport Public] *Vie Publique*, 18 January 2006, available at https://www.vie-publique.fr/rapport/27943-la-securite-des-systemes-dinformation-un-enjeu-majeur-pour-la-france (accessed on March 6th, 2021)

[2] R. Romani, 'Rapport d'information fait au nom de la Commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense' [Rapport Public] *Vie Publique*, 8 July 2008, available at https://www.vie-publique.fr/rapport/29979-rapport-dinformation-fait-au-nom-de-la-commission-des-affaires-etranger (accessed on March 6th, 2021)

[3] See J.-C. Mallet, *Défense et Sécurité nationale – Le Livre Blanc* (La documentation Française, 2008), available at http://bdc.aege.fr/public/Defense_et_securite_nationale_Livre_Blanc.pdf (accessed on March 5th, 2021)

[4] ANSSI, Défense et sécurité des systèmes d'information: Stratégie de la France, February 2011, available at https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf (Accessed on March 7th, 2021)

[5] SGDSN, 'Stratégie Nationale pour la Sécurité du Numérique', October 2015, available at https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf (accessed on March 7th, 2021)

new challenges arising from changes in digital uses and related threats with five objectives: guaranteeing national sovereignty; provide a strong response against acts of cyber malicious acts; inform the general public; make digital security a competitive advantage for French companies and strengthen France's voice internationally. In December 2017, *France's international digital strategy*[1] supplemented this document by specifying the principles and objectives pursued by France in the area of digital technology at the international level. Built around three main axes (governance, economy, security), this strategy aims to promote an open, diverse, and globally trusted digital world; affirm a European model of balance between economic growth, fundamental rights and freedoms, and security; and to strengthen the influence, attractiveness, security and commercial positions of France and French players in the digital world.

The *Cyber defence strategic review*[2] presented in February 2018 defines a cyber crisis management doctrine and clarifies national cyber defence strategic objectives. Confirming the relevance of the French model and the primary responsibility of the State in matters of cybersecurity, it revolves around seven main principles: improving the protection of our country's information systems; discouraging attacks through a set of measures of a defensive nature, enhanced resilience as well as reaction and response capacities; the affirmation and exercise of French digital sovereignty; a more effective criminal response to cybercrime; promoting a shared culture of IT security; participation in the development of a secure and trustworthy digital Europe; as well as international action in favour of collective and controlled governance of cyberspace.

On February 18 2021, the President of the French Republic exchanged views with actors from the hospitals of *Dax* and *Ville franche-sur-Saône* via videoconference, which have recently been the subject of cyberattacks, and therefore decided to accelerate the renewal of the national strategy for cybersecurity. As the President stated,

> "*We are going to endow ourselves with one billion euros, largely as part of the recovery plan and the investment program for the future to invest in several areas. First, provide support for research and development of new, sovereign technologies, and in doing so create a much more cohesive, more efficient ecosystem, which will be brought together in the cyber campus which has just been presented to us and will therefore open its doors in the fall*" [3].

[1] Ministère des Affaires Etrangères, 'Stratégie internationale de la France pour le numérique', December 2017, available at https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf (accessed on March 7th, 2021)

[2] SGDSN, 'Revue stratégique de cyberdéfense', February 2018, available at http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf (accessed on March 7th, 2021)

[3] E. Macron, 'Déclaration de M. Emmanuel Macron, président de la République, sur les cyberattaques dans les hôpitaux et la stratégie nationale pour la cybersécurité, à Paris le 18 février 2021', [discours] *Vie Publique*, February 2018, available at https://www.vie-publique.fr/discours/278659-emmanuel-macron-18022021-cybersecurite (accessed on March 7th, 2021)

2. Legal Framework

i. Critical Information Infrastructure Protection

The need to enhance the information systems security in sectors of vital importance in France (SAIV),[1] was already recognised since 2005 by the Law No. 2005-1550 of December 12, 2005[2] amending various provisions relating to defence. This law established in the Defence Code an inter-ministerial security system for SAIV. Managed by the General Secretariat for Defence and National Security (SGDSN),[3] the system aims to protect operators of vital importance (OIV),[4] against malicious acts and technological, natural and health risks that could impact them.[5] The Decree n° 2006-212[6] on the security of vital importance activities, amended by two ministerial orders on June 2, 2006[7] and July 3, 2008[8] identified the sectors of vital importance and designated the coordinating ministers within them. Nevertheless, the transposition of the Council Directive 2008/114/EC[9] of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, was not deemed necessary by France.[10]

Article 22 of Law n° 2013-1168 of December 18, 2013[11] on the military programming for the years 2014 to 2019, the existence of which was based on the recommendations of the White Paper on Defence and National Security of 2013,[12] required then from the OIV's to strengthen the security of their vital importance information systems (SIIV).[13] The conditions for the implementation of this law were specified by Decree N° 2015-351 of

[1] Sécurité des Activités d'Importance Vitale (SAIV)

[2] Loi n° 2005-1550 du 12 décembre 2005 modifiant diverses dispositions relatives à la défense (1), JORF n°289

[3] Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN). Available at http://www.sgdsn.gouv.fr/ (accessed on March 7th, 2021)

[4] Opérateurs d'Importance Vital (OIV)

[5] Article L1332-1 of the 'Code de la Défense'

[6] Décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale, JORF n°47

[7] Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, JORF n°129

[8] Arrêté du 3 juillet 2008 portant modification de l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, JORF n°156

[9] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008/114/EC, OJ L 345, 23.12.2008, p. 75–82.

[10] Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=NIM:177674 (accessed on March 7th, 2021)

[11] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n°0294

[12] Available at http://www.livreblancdefenseetsecurite.gouv.fr/ (accessed on March 7th, 2021)

[13] Systèmes d'Information d'Importance Vitale (SIIV)

March 27, 2015[1] on to the security of the information systems of the OIV. France has also incorporated these obligations affecting stakeholders in the digital sector intended to overlap with the OIV regime by decree n ° 2015-350 of March 27, 2015[2] on the qualification of security products and trusted service providers for the needs of information systems security. Following the working groups, the French Cybersecurity Agency (ANSSI),[3] proposes regulations adapted to the business sectors. The first decrees are signed by the Prime Minister and define the criteria for executing the measures that came into force on July 1, 2016 (**Table 24**).

Sector (SAIV)	Decrees	Entry to force
Health products	Decree of June 10, 2016	July 1, 2016
Water management	Decree of June 17, 2016	July 1, 2016
Food	Decree of June 17, 2016	July 1, 2016
Electricity supply	Decree of August 11, 2016	October 1, 2016
Natural gas	Decree of August 11, 2016	October 1, 2016
Petroleum hydrocarbons	Decree of August 11, 2016	October 1, 2016
Terrestrial	Decree of August 11, 2016	October 1, 2016
Maritime and river	Decree of August 11, 2016	October 1, 2016
Aerial	Decree of August 11, 2016	October 1, 2016
Audio-visual	Decree of November 28, 2016	January 1, 2017
Electronic communications and Internet	Decree of November 28, 2016	January 1, 2017
Industry	Decree of November 28, 2016	January 1, 2017
Finances	Decree of November 28, 2016	January 1, 2017
Nuclear	Decree of March 10, 2017	April 1, 2017
Industrial armaments activities	Decree of September 8, 2017	October 1, 2017
Space	Decree of September 8, 2017	October 1, 2017
Civilian State Activities	Decree of May 29, 2019	October 1, 2019
Public research	Decree of July 13, 2020	October 1, 2020

Table 24: *Decrees laying down the security rules and the procedures for declaring 'SIIV' and security incidents relating to the sub-sector of the 'SAIV'*

(Table made by author)

ii. E-commerce legislation

Law n° 2004-575 of the June 21, 2004, on Trust in the Digital Economy[4] has implemented the EU e-commerce directive (2000/31 / EC) and established the legal framework for the development of e-commerce

[1] Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense, JORF n°0075

[2] Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information, JORF n°0075

[3] Agence nationale de la sécurité des systèmes d'information (ANSSI)

[4] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1), JORF n°0143

services in France. Among other things, this law establishes the principle for receiving e-mails for advertising and regulates the liability of certification service providers that issue recognised digital certificates.

The law was subject to a seisure from the French Constitutional Council, filed on May 18, 2004, by the opposition (60 Deputies[1] and 60 Senators[2]). The Constitutional Council rendered its decision on June 10, 2004 and rejected the majority of the opposition's requests, while considering a few words of the bill as unconstitutional and adding a reservation of interpretation concerning article 62 of the Constitution.[3] From a strictly legal point of view, §7 of this decision declares that: "*The transposition of a Community directive into domestic law results from a constitutional requirement to which, it could not be obstacle because of an express provision of the Constitution; that in the absence of such a provision, it belongs only to the Community judge, referred to as a preliminary ruling, to monitor the respect by a Community directive both of the powers defined by the treaty and fundamental rights guaranteed Article 6 of the [TEU]*".

However, the transposition of the directive has been delayed because of the virulent oppositions it has born from the internet players. The hosts (Article 6-I-2 of the law of 21 June 2004) was rapidly concerned with the writing of the initial text, demanding from their part a priori verification (before the upload) of the lawfulness of all the accounts hosted in their care. A technically difficult measure to put in place yet made mandatory by law in preparation. To better be heard, and to emphasise the incongruous nature of the bill, the hosts then threatened to suspend all the personal pages they accommodated. The debate also carried on the question of the confidentiality of private correspondence for e-mails. In addition, the law has prohibited the fact of publicly disclosing vulnerabilities accompanied by operating code. Art. 6 of the law of 21 June 2004 was thus modified by the Article 6 of the Law No. 2006-64 of 23 January 2006 on the fight against terrorism.[4]

3. National Authorities

i. Ministry of the Interior

The mission of the Ministry of the Interior is to fight against all forms of cybercrime, targeting institutions and national interests, economic players, and public authorities, as well as individuals. To this end, it mobilises the specialised central services and the territorial networks of the national police, the national gendarmerie and

[1] Conseil Constitutionnel, Décision n° 2004-496 DC du 10 juin 2004 - Saisine par 60 députés

[2] *Ibid*

[3] *Ibid*

[4] Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, JORF n°0020

internal security. They are responsible for investigations aimed at identifying the perpetrators of cyber-malicious acts and bringing them to justice. These services also contribute to prevention and to raising the awareness of the public concerned.

ii. Inter-ministerial Commission for the Coordination of Electronic Communications Networks and Services for Defence and Public Security

The Minister responsible for electronic communications chairs the Inter-ministerial Commission for the Coordination of Electronic Communications Networks and Services for Defence and Public Security (CICREST).[1] The Commission shall draw up and propose rules to be applied taking into account, on the one hand, the operation of networks and services and, on the other, the needs of national defence and public security (Article R1334-2, para. 2 of the Code de la Défense). The composition and operation of the committee is determined by a decision of the Prime Minister (Article R1334-2, para. 1 of the Defence Code).

iii. The National Information Systems Security Agency (ANSSI)

The French national cybersecurity authority (ANSSI)[2] is responsible for dealing "*immediately*" with attacks on state-of-the-art computers. The ANSSI was created by the « *Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé Agence nationale de la sécurité des systèmes d'information*"[3]. The agency is under the authority of the Prime Minister and is attached to the Secretary General of Defence and National Security and has national jurisdiction. It assists the Secretary-General in carrying out his security responsibilities for information systems and the electronic command and communications assets necessary for the highest defence and national security authorities. Finally, it is the national authority on the security of information systems. This agency is a rather hierarchical organisation. With Almost 600 agents dispersed across 5 branches and a Cyber Anticipation Cell, which works as an anticipation coordinator for decision support, ANSSI has almost 9 times more staff than the ENISA. The main missions of the organisation are the detection and timely response to cyberattacks, with the creation of a strong operational defence centre, which operates 24/24h and is responsible for the continuous monitoring of sensitive government networks, as well as the implementation of appropriate defence mechanisms; threats prevention by supporting the

[1] Commission Interministérielle de Coordination des Réseaux Et des Services de Communications Electroniques pour la défense et la sécurité publique - (CICREST). Article R1334-2 of the Code de la Défense

[2] Available at https://www.ssi.gouv.fr/en/mission/what-we-do/ (accessed on March 7th, 2021)

[3] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », JORF n°0156

development of reliable products and services for public and economic actors; the reliable advice and support to government agencies and critical infrastructure companies.

In France there are several CERT teams depending on the sector in which they operate.[1] The official governing body is CERT-FR, which operates within ANSSI and is responsible for strengthening administrative bodies, implementing protection measures and dealing with incidents and attacks.

iv. Central Office for the Fight against Information and Communication Crime (OCLCTIC)

The Central Office for the Fight against Information and Communication Crime (OCLCTIC),[2] is owned by the French police and aims to facilitate and coordinate police activities against cybercrime at the national level. OCLCTIC's responsibilities include conducting investigations and assisting the police, the Directorate-General for Competition, Consumption and Anti-Fraud. It also supports the local and regional police in matters of information technology, data collection, and other needs of cybercrime.

v. Regulatory Authority for Electronic Communications, Posts and Press Distribution (ARCEP)

The Regulatory Authority for Electronic Communications, Posts and Press Distribution (ARCEP),[3] was created on January 5, 1997, under the name of Telecoms Regulatory Authority (*Autorité de régulation des télécoms*).

ARCEP is an independent administrative authority. Arcep is made up of a college of seven members with respect for gender parity. The members are appointed by different political authorities, because of their economic, legal, and technical qualifications, in the fields of electronic communications, posts and the economy of the territories. The President of the Republic appoints the President of ARCEP as well as two other members. The President of the National Assembly and the President of the Senate each appoint two members. College members are appointed for 6 years. To guarantee their independence, their mandate is neither revocable nor renewable. They are also subject to a regime of incompatibility of functions and to ethical obligations.

ARCEP regulates the electronic communications and postal sectors, on behalf of the state, but with complete independence from political power and economic actors. More specifically it defines the regulations applicable

[1] Available at https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map (accessed on March 7th, 2021)

[2] Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)

[3] Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP)

to all or some of the operators; allocated through individual decisions frequencies;[1] Ensures the financing and provision of the universal service;[2] Shares its expertise, through the opinions it renders at the request of the Government, Parliament or other regulatory authorities, for example the Competition Authority or the Superior Audiovisual Council; Enacts acts of *soft law*, such as guidelines or recommendations to give visibility to the sector on the exercise of its skills or guide the behaviour of actors; and conducts regular dialogues with industry players, to maintain in-depth knowledge of the markets it regulates adjusting its regulatory decisions and making them known.

In 2015, it launched a strategic review of its activities, called *ARCEP pivots*. An open, transparent, and participatory process, which involved the Arcep teams, but also external actors. At the end of this process, ARCEP established a roadmap, defining the "*causes to be defended*" for the coming years. It also adopted a manifesto, a short text which aims to define its fundamental raison d'être.

vi. National Commission for Informatics and Freedoms (CNIL)

The French Data Protection Authority (CNIL),[3] has the overall responsibility to ensure that the development of information technology remains at the service of citizens and does not violate human rights, privacy or personal data or public freedoms. Created in 1978 by Law n° 78-17 of January 6, 1978, on data processing, files and freedoms, Data Protection Act,[4] the CNIL is an independent administrative authority, made up of a college of 18 members and a team of contractual agents of the State.

C. Greece

1. National Cyber Security Strategy and Policies

In January 2006, a comprehensive Digital Strategy for the period 2006-2013[5] was launched in Greece, which aims at the most efficient use of information technologies and the Internet throughout society and the economy. This Strategy aimed to make a *Digital Leap* and was analysed in two directions, the productivity improvement,

[1] Art. L. 42-1 and s., and art. L. 44 of the 'Code des postes et des communications électroniques

[2] Art. L. 35 and s. of the 'Code des postes et des communications électroniques'

[3] Commission Nationale de l'Informatique et des Libertés (CNIL)

[4] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978

[5] Υπουργείο Οικονομίας & Οικονομικών – Ειδική Γραμματεία Ψηφιακού Σχεδιασμού, 'Ψηφιακή Στρατηγική 2006-2013: Τεχνολογικά εργαλεία για την ανάπτυξη των δήμων', available at https://kedke.gr/psifiaki-stratigiki-2006-2013-technologika-ergaleia-gia-tin-anaptyxi-ton-dimon/ (accessed on March 8th, 2021)

and the quality-of-life improvement through the use of new technologies. The Digital Strategy 2006-2013 offered new development opportunities in the municipalities of the whole country, utilizing the new technologies. The Special Secretariat for Digital Design of the Ministry of Economy at that time aimed to enrich the already existing policy tools of the municipalities with new digital possibilities, through a series of interventions, such the action *Digital Local Government* that enables all municipalities in the country to develop digital services for citizens and to promote their special local characteristics (budget € 60 million) or the promotion of broadband, with demonstration projects in more than 40 municipalities of the country (budget € 11 million).

In December 2016, a second digital strategy was adopted for the period between 2016-2021.[1] This strategy focuses on seven areas of intervention with specific priorities for each sector such as, developing next generation national infrastructures; further digitalising the economy; boosting the ICT sector to develop the digital economy and employment; Empowerment of human resources with digital skills; Radical review of how to provide Digital Public Services; Lifting off exclusions and spreading the benefits of the digital economy and ; Strengthening Security and Confidence. The priorities correspond to recognised gaps in the Greek public administration, economy and society and form a coherent framework of ICT interventions, focusing on the production of results and the best possible utilisation of available public resources.

Until 2018, Greece had no National Cybersecurity Strategy. It is only on March 7th, 2018, that Greece implemented its first cybersecurity strategy.[2] The goal of the strategy was to create a secure Internet environment, infrastructure, and services, which will boost citizens' trust and lead them to further use new digital products and services and to stimulate the economic development of Greece. The basic principles of this strategy were the development and consolidation of a secure and resilient cyberspace; the continuous development of protection capabilities against cyberattacks, with a particular emphasis on critical infrastructure and institutional protection; and the development of a strong cybersecurity culture among the society. The goals defined are the designation of the Bodies participating in the National Cybersecurity Strategy and of the stakeholders; the Definition of Critical Infrastructure; the Risk Assessment at National Level; the Recording and improving the Existing Institutional Framework; the National Cyber Emergency Plan; the Defining Basic Safety Requirements; the Dealing with Security Incidents; the National Readiness Exercises; the Awareness of users – citizens; the Mechanisms for Reliable Information Exchange; the Support for Research and Development Programs; the and Academic Education Programs; the Collaborations at International Level and; the Evaluation and Review of the National Strategy. The National Cybersecurity Strategy includes two sub-phases. The

[1] Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης - Γενική Γραμματεία Ψηφιακής Πολιτικής, Εθνική Ψηφιακή Στρατηγική 2016-2021, December 2016, available at http://www.epdm.gr/el/Documents/EP_MDT/GR-Digital-Strategy_2016-2021.pdf (accessed on March 8th, 2021)

[2] Available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/@@download_version/50cded9109d442e7839649f42055da60/file_en, accessed on March 8th, 2021.

development and implementation of the Strategy in the first stage and its evaluation and review in the second stage. These phases define a continuous life cycle, in the sense that the National Strategy is first developed and implemented, then evaluated, based on predetermined evaluation indicators and, if necessary, reviewed and updated.

Although Greece cannot be considered as exposed to cyber threats as other Member States of the Union, as well as equally capable of managing problems in its cyberspace, its cooperation allows - being less financially and militarily strong - to deal with threats effectively.[1] In this light, and taking into account the modern requirements and needs, the National Cyber Security Authority of the Ministry of Digital Government updated the National Cybersecurity Strategy in December 2020[2], in order to assess the current situation, identify new challenges and form an appropriate strategic framework for immediate implementation. An update which coincides with the new cybersecurity strategy adopted by the EU on December 16th, 2020, for the next Digital Decade.[3] The 2020-2025 Greek Cybersecurity Strategy is more explicit from the previous ones as it counts 81 pages instead of 18 pages in 2018.

Through a detailed framework of actions with 15 specific objectives and over 50 activities, attempts are made to reduce the range of incidents that can jeopardise the integrity of critical infrastructure and threaten the proper functioning of the State and the security of citizens and businesses. Considering the continuous increase of threats, which is indicated by the latest data of ENISA, the National Cybersecurity Strategy is systematised in five strategic pillars of intervention, each of which includes three specific objectives for the specialisation and better management of the strategic framework (cascade effect), which in turn specialise in activities to cover the full range of recognition, recruitment, protection, deterrence and recovery from cyber-attacks.

The Strategy is articulated around five pillars and 15 goals. The first strategic pillar concerns the creation of an operational system of governance and aims at the specific activities that include the optimisation of the framework of organisation and operation of structures and procedures, the effective planning of risk assessment and emergency management but also the strengthening of cooperation in national, European, and international level. This is followed by the shielding of critical infrastructure, with security and new technologies, which will be achieved through understanding the technological developments and how they affect digital governance, by upgrading the protection of critical infrastructure and by shielding systems and applications through enhanced security requirements. The third pillar is defined as incident management optimisation, the fight against cybercrime and the protection of privacy. The specific objectives of this pillar are optimisation of methods,

[1] See S. Biscop, 'Differentiated integration in defence: a plea for PESCO', (2017) *Instituto Affari Internazionali*

[2] Υπουργείο Ψηφιακής Διακυβερνησης - Εθνική Αρχή Κυβερνοασφάλειας, Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025, December 2020, available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/@@download_version/f45a6e4d8a8d421781a6bd9b61cabdee/file_en (accessed on March 8th, 2021)

[3] European Commission, Joint Communication to the European Parliament and the Council on 'The EU's Cybersecurity Strategy for the Digital Decade', 16 December 2020, JOIN(2020) 18 final

techniques and tools for analysis, response and notification of events, strengthening of prevention mechanisms and optimisation of business cooperation and cyber security and protection of privacy. At the same time, an attempt is being made to create a modern investment environment with an emphasis on the promotion of Research and Development through the provision of appropriate investment incentives and the utilisation of Public-Private Partnerships (PPPs). The fifth and final pillar of the project is capacity building and the promotion of information and awareness. This will be achieved by aiming to improve skills through the organisation of appropriate exercises, the use of modern methods and tools of training and education and the ongoing information of agencies and citizens regarding cybersecurity issues. The activities in the pillars also include interventions for cybersecurity of public bodies, framework for promoting excellence in the field of cybersecurity, risk assessment planning, strengthening cooperation at European and international level, measures to challenge new security technologies, , incident prevention and response systems, strengthened business partnerships, incentives to invest in secure systems, and an integrated capacity building and awareness-raising framework.

The success of the strategy, as clarified, depends on specific conditions which must be considered by all stakeholders. In this context, it is expected to promote the strengthening of investment programs in cybersecurity by the private sector and other agencies, something that will be done by providing appropriate financial incentives, such as tax relief and incentives for cooperation. It should be reminded that this initiative follows a series of actions of the Ministry of Digital Government on cybersecurity such as: the definition of the critical infrastructure of the country and the framework of their obligations, the upgrade of the National Cyber Security Authority to the General Directorate of the Ministry and participation of the competent services in preparedness exercises, the use of advanced systems for the prevention and response to electronic attacks. The update of the National Cybersecurity Strategy is one of the 18 total projects (9 in progress) included in the "*Digital Transformation Book 2020-2025*"[1] in the field of cybersecurity, which are considered a condition for building trust in users of digital services and applications.

2. Legal Framework

i. Critical Information Infrastructure Protection

Presidential Decree 39/2011[2] Regarding Critical Infrastructure Protection harmonises Greek legislation with the European Union Directive 2008/114/EC on the identification, designation, and assessment of critical

[1] Available at https://digitalstrategy.gov.gr/, accessed on March 8th, 2021.

[2] Προεδρικό Διάταγμα Υπ'Αριθμ. 39, 'Προσαρμογή της ελληνικής νομοθεσίας προς τις διατάξεις της Οδηγίας 2008/114/ΕΚ του Συμβουλίου της 8ης Δεκεμβρίου 2008', available at http://www.kemea.gr/images/documents/pd39-2011.pdf (accessed on March 8th, 2021)

infrastructure. The Decree defines the Hellenic Centre for Security Studies (KE.ME.A.)[1] as a National Contact Point and in its relevant responsibilities, as well as in the determination of the obligations of the Greek bodies involved towards the critical infrastructures that are characterised as European. In addition, the Regulation for the Safety and Integrity Network and Electronic Communications Services 2013,[2] adopted by the Hellenic Authority for Communication Security and Privacy[3] and updated by a decision of the same authority in 2017,[4] addresses network-based and electronic critical infrastructure.

ii. Electronic communications legislation

Presidential Decree 131/2003[5] on e-commerce transposes Directive 2000/31 of the European Parliament on certain legal aspects of information society services, in particular e-commerce, in the internal market. Law 3471/2006[6] was issued on June 28th, 2006, as a revision of law 2472/1997.[7] It defines the general framework for the provision of electronic communications networks and services in Greece, while at the same time implementing the full transposition of EU regulations 2002/19 / EC, 2002/20 / EC, 2002/21 / EC, 2002 / 22 / EC, and 2002/77 / EC in National Law. Law 3674/2008[8] defines the obligations of service providers regarding the security of communication services.

[1] See section 'viii. The Hellenic Centre for Security Studies' of the present thesis

[2] Απόφαση Α.Δ.Α.Ε. 205/2013 - ΦΕΚ 1742/Β/15-7-2013

[3] See section 'vii. Hellenic Authority for Communication Security and Privacy' of the present thesis

[4] Απόφαση ΑΔΑΕ Αριθμ. 99/2017 - ΦΕΚ 4073/Β/23-11-2017

[5] Προεδρικό Διάταγμα Υπ'Αριθμ. 131, 'Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. (Οδηγία για το ηλεκτρονικό εμπόριο)', available at https://www.wipo.int/edocs/lexdocs/laws/el/gr/gr236el.pdf (accessed on March 9th, 2021)

[6] Νόμος 3471/2006, Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997, ΦΕΚ 133/Α/28-6-2006

[7] Νόμος 2472/1997, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ΦΕΚ Α-50/10-4-1997

[8] Νόμος 3674/2008, Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις, ΦΕΚ 136/Α/10-7-2008

3. National Bodies

i. General Directorate of Cyber Security (National Cyber Security Authority)

The General Directorate of Cyber Security[1] of the Ministry of Digital Government (National Cyber Security Authority) is responsible for the management of the Strategy and the coordination of the Bodies during the implementation of the required measures. Through the Strategic Plan, it aims at the definition of appropriate organisational, technical and operational measures, at their implementation by the Bodies, at the evaluation of the Strategy, as well as its revision. In particular, the responsibilities of the Authority include, inter alia, the overall management of a national cybersecurity strategy, the definition of basic safety requirements, the management of the institutional framework, the implementation of a cybersecurity and incident management framework, the audit and evaluation of national bodies, the response to security incidents of the Authority and / or Bodies, the evaluation and review of basic safety requirements or even the cooperation in cybersecurity issues at national, European and international level (agencies, Member States, etc.).

ii. National Intelligence Service

The Presidential Decree 96/2020 (A'232),[2] which amends the Presidential Decree 1/2017 (A'2)[3] on the organisation of the Services of the National Intelligence Service,[4] defines the responsibilities of the Cyberspace Directorate of the "Ε.Υ.Π.", which include technical issues of information security (INFOSEC National Authority)[5] and in particular for the security of national communications, information technology systems, as well as for the evaluation and certification of classified communications and information security devices and systems; the evaluation and certification of cryptosystems, as well as the support of the Armed Forces and public sector services in matters of cryptocurrency (National Authority CRYPTO);[6] the safeguarding of national electronic telecommunications equipment against leakage due to unwanted, electromagnetic and non-

[1] Γενική Διεύθυνση Κυβερνοασφάλειας

[2] Προεδρικό Διάταγμα Υπ'Αριθμ. 96/2020, 'Τροποποίηση και συμπλήρωση διατάξεων του π.δ. 1/2017 «Οργανισμός της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.)» (Α' 2)', ΦΕΚ 232/Α/20-11-2020

[3] Προεδρικό Διάταγμα Υπ'Αριθμ. 1/2017, 'Οργανισμός της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.)', ΦΕΚ 2/Α/18-1-2017

[4] Εθνικής Υπηρεσίας Πληροφοριών (ΕΥΠ)

[5] Retrieved from https://www.itsecuritypro.gr/kyvernoamyna-stin-ellada-e-e-nato/ (accessed on March 10th, 2021)

[6] Προεδρικό Διάταγμα Υπ'Αριθμ. 96/2020, 'Τροποποίηση και συμπλήρωση διατάξεων του π.δ. 1/2017 «Οργανισμός της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.)» (Α' 2)', ΦΕΚ 232/Α/20-11-2020

transmissions (National TEMPEST Authority);[1] the responsibilities of the Cyber Attack Response Team (National CERT),[2] within the national cybersecurity network defined by the National Cyber Security Authority, for cyberattacks against the public bodies of the country, which do not fall under the competence of the Cyber Defence Directorate of the General Staff of National Defence (CSIRT).

In particular, the National CERT of the National Intelligence Service supports the Presidency of the Government and the Ministries, except for the Ministry of National Defence, for the prevention, early warning, and response to cyber-attacks against them. In addition, it is responsible for the collection and processing of electronic data and the information of the competent bodies. According to Law n°3649/2008,[3] article 6, paragraph 1, the public services, the legal entities under public law and the public enterprises are obliged to provide to specially authorised employees of the National Intelligence Service any information, element or assistance for the fulfilment of its mission.

FORTH CERT[4] is the Team of the Institute of Informatics of the Foundation for Research and Technology and provides information security incident services. Key services include alerts, incident handling and action coordination. GRNET-CERT[5] provides security incident services for the National Infrastructures for Research and Technology (GRNET) and all Greek Universities, research institutes and educational networks in Greece. AUTH-CERT[6] deals with security incidents involving Aristotle University's network users.

iii. Cyber Defence Directorate of the General Staff of National Defence

The Cyber Defence Directorate of the General Staff of National Defence[7] is the Hellenic Computer Security Incident Response Team (CSIRT) regarding the response to incidents in the military sector - cyberdefence (military CSIRT), the response of incidents to agencies that fall within the scope of the law n°4577/2018[8] and the operational completion. The mission of the above Service is to reduce the risk of national challenges in the

[1] OJ L 72, 17.3.2015, p. 53–88

[2] Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT)

[3] Νόμος 3649/2008, 'Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις', ΦΕΚ 39/Α'/3.3.2008

[4] Available at http://www.forthcert.gr/ (accessed on March 10th, 2021)

[5] Available at https://cert.grnet.gr/en/home/ (accessed on March 10th, 2021)

[6] Available at https://www.cert.auth.gr/ (accessed on March 10th, 2021)

[7] 'Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας (ΔΙΚΥΒ/ΓΕΕΘΑ). Available at https://geetha.mil.gr/ (accessed on March 10th, 2021)

[8] Νόμος 4577/2018, 'Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις', ΦΕΚ 199/Α/3-12-2018

field of cyber security and communications. It is also responsible for the issuance of the National Security Regulation[1] in collaboration with the National Intelligence Service.

iv. Cybercrime Prosecution Directorate

The Presidential Decree 178/2014 (A '281)[2] provided for the establishment and structure of the Cybercrime Prosecution Directorate[3] based in Athens and the establishment and structure of the Cybercrime Prosecution Sub-Directorate based in Thessaloniki. The mission of the Cybercrime Prosecution Directorate includes the prevention, investigation and repression of crimes or anti-social behaviours, committed via the internet or other electronic means of communication. The Cybercrime Prosecution Directorate is an independent central Service and reports directly to the Chief of the Hellenic Police. The Cybercrime Prosecution Directorate, in its internal structure, consists of five departments that complete the whole spectrum of user protection and cyber security: the Department of Administrative Support and Information Management; the Department of Innovative Actions and Strategy; the Department of Electronic and Telephone Communications Security and Software and Copyright Protection; the Department of Internet Minor Protection and Digital Investigation and; the Department of Special Cases and Prosecution of Cybercrime.

v. Hellenic Personal Data Protection Authority (HPDPA)

The Personal Data Protection Authority[4] is a constitutionally guaranteed independent authority responsible for supervising the implementation of the General Data Protection Regulation (GDPR), of the law 4624/2019[5] and of the law 3471/2006[6] and other regulations concerning the protection of the individual from the processing of personal data, and exercises the responsibilities assigned to it each time. In particular, the Personal Data Protection Authority is responsible for monitoring the implementation of the provisions of the General Data

[1] Εθνικού Κανονισμού Ασφάλειας (ΕΚΑ). Υπουργική Απόφαση Φ. 120/01/510313/Σ.94 (1), Κύρωση του Εθνικού Κανονισμού Ασφαλείας (ΕΚΑ), ΦΕΚ 683/Β/27.2.2018

[2] Προεδρικό Διάταγμα Υπ'Αριθμ. 178/2014, 'Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας', ΦΕΚ 281/Α/31.12.2014

[3] Available at http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang= (accessed on March 10th, 2021)

[4] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - (Α.Π.Δ.Π.Χ.). Available at https://www.dpa.gr/ (accessed on March 10th, 2021)

[5] Νόμος 4624/2019, 'Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων', ΦΕΚ 137/Α/29.8.2019

[6] Νόμος 3471/2006, Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997, ΦΕΚ 133/Α/28-6-2006

Protection Regulation (EU) 2016/679 (GDPR), [1] in order to protect the fundamental rights and freedoms of individuals against the processing of data concerning them and to facilitate free movement of data in the Union (article 51, para. 1 and recital 123). It contributes to the coherent implementation of the GDPR throughout the Union and to this end cooperates with the supervisory authorities of the EU Member States and with the Commission (Article 51, para. 2 and recital 123).

Within this context, the Authority, among others, monitors and enforces the implementation of the GDPR; Promotes public awareness of the issues of personal data protection and those responsible and executors of their obligations under the GDPR. Special attention is paid to activities aimed specifically at children; Advises the national parliament, government and other bodies and agencies on legislative and administrative measures related to the protection of personal data; Provides on request information to data subjects regarding the exercise of their rights; Handles complaints submitted for violation of GDPR provisions; Conducts research on the implementation of the GDPR; Compiles and maintains a list in relation to the requirement for impact assessment (Article 35 (4) of the GDPR) and provides advice on the processing operations of Article 36 (2) of the GDPR; Approves codes of conduct and certification criteria and drafts accreditation criteria; Cooperates with other supervisory authorities through the exchange of information and provides mutual assistance to them in order to ensure the coherence of the implementation of the GDPR; Contributes to the activities of the European Data Protection Board;[2] It has control powers, as well as corrective, advisory and licensing powers, as specified and analysed in Article 58 of the GDPR.

vi. Hellenic Telecommunications and Post Commission

Hellenic Telecommunications and Post Commission (E.E.T.T.)[3] is an Independent Administrative Authority and is responsible for the integrity and availability of public communication networks - even in times of emergency. It is the National Regulator that regulates, supervises, and controls the electronic communications market (fixed and mobile telephony, wireless and internet companies) and the postal market (postal service companies and courier services). In addition, "E.E.T.T." is the regulation authority in the above-mentioned markets and has all the powers and rights of the Hellenic Competition Commission[4] in the implementation of free competition legislation in these markets (Law n°3959 / 2011 (A '93),[5] Articles 101/102 TFEU and Council Regulation 1/2003 EC). The implementation of the legislation on free competition by "E.E.T.T." in the markets

[1] OJ L 119, 4.5.2016, p. 1–88.

[2] Available at https://edpb.europa.eu/edpb_en (accessed on March 9th, 2021)

[3] Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (E.E.T.T.). Available at https://www.eett.gr/opencms/opencms/EETT_EN/index.html (accessed on March 10th, 2021)

[4] Available at https://www.epant.gr/ (accessed on March 10th, 2021)

[5] Νόμος 3959/2011, 'Προστασία του ελεύθερου ανταγωνισμού', ΦΕΚ Α-93/20.4.2011

of its exclusive competence was provided by laws n°2867 / 2000[1] on the organisation and the functioning of telecommunications, n°3431 / 2006[2] related to Electronic Communications, and n°4070 / 2012 on Electronic Communications, Transport, Public Works Arrangements.[3]

vii. Hellenic Authority for Communication Security and Privacy

The Authority for Ensuring the Privacy of Communications [4] is responsible for maintaining confidentiality and free communication, for the certification of security products and for the control of all involved bodies. The Authority is a constitutionally guaranteed independent authority that enjoys administrative autonomy. Its headquarters are in Athens, but it can decide to establish and operate offices in other cities in Greece. The decisions of the Authority are reported to the Minister of Justice, while at the end of each year a Report of its activities is submitted to the Speaker of Parliament, the Minister of Justice and the leaders of the parties represented in Parliament and the European Parliament.

The main responsibilities of the Authority are to carry out regular and extraordinary inspections in public service facilities or private companies dealing with postal, telecommunications or other services; to control, from the point of view of legality, conditions and procedures followed during the application of the provisions for the removal of the confidentiality; to hear providers of electronic communications services and postal services for possible violations of the confidentiality; to impose the provided administrative sanctions, in case of violation of the current legislation on the confidentiality of communications; to adopt regulatory and other necessary acts regarding the applicable measures to ensure the confidentiality of communications; to issue opinions, recommendations and suggestions on issues within the competence of the Authority and finally; to examine complaints for violation of the confidentiality of the telephone and internet communications or communications through postal services.

[1] Νόμος 2867/2000, 'Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις', ΦΕΚ 273/Α/19.12.2000

[2] Νόμος 3431/2006, 'Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις', ΦΕΚ 13/Α/13.2.2006

[3] Νόμος 4070/2012, 'Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις', ΦΕΚ 82 Α/10.4.2012

[4] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.). Available at http://www.adae.gr/ (accessed on March 10th, 2021)

viii. The Hellenic Centre for Security Studies

The Centre for Security Studies (KE.ME.A)[1] is a research and advisory body of the Ministry of Civil Protection (formerly Public Order and Citizen Protection) in the field of Security. It is the National Authority of the country in terms of the protection of critical infrastructure, as well as the National Contact Point with the competent bodies of the European Commission and the Member States of the European Union.

To fulfil its goals, the "KE.ME.A." conducts research programs and studies on issues of internal security related to the Ministry of Civil Protection (formerly Public Order and Civil Protection) and the services under it, as well as other internal bodies; prepares and carries out research programs as a representative of the bodies supervised by the Ministry of Civil Protection, on behalf of or in cooperation with relevant bodies of the European Union, other states or international organisations in accordance with the relevant rules and procedures; develops cooperation at national and international level with organisations and services, research and educational centres and institutions, social, scientific and productive bodies, public and private, as well as with NGOs; studies the criminal phenomenon and the qualitative and quantitative changes of crime in the Greek Territory and its geographical distribution, as well as the design of methods and practices in the exercise of anti-crime policy; proposes the harmonisation of measures for the prevention and suppression of crime with constitutional principles, civil and political rights, the rule of law and respect for human dignity; monitors and studies the technological developments of security systems and evaluates the new achievements in this field; formulates proposals for the utilisation of the know-how it possesses; supports cross-border cooperation procedures; organises and conducts conferences, publishes research and general scientific findings and related projects, conducts training seminars and provides certified training in security issues and prepares certified studies in such matters and develops any other activity related to its purposes. "KE.ME.A." is also a certification body for procedures, studies, security plans, bodies, organisations, and companies of the Private and Public Sector. Finally, "KE.ME.A." is one of the contracting members established by the Greek Cyber Crime Centre (CyberCC). [2] The Centre is part of a coordinated European effort to improve cybercrime education. At the same time, utilizing both the close cooperation with KEMEA and the research experience of its members, the GCC intends to become a centre of excellence in the field of cybercrime research. The CyberCC combines the know-how of national law enforcement authorities with the industrial and academic world.

[1] 'ΚΕντρο ΜΕλετων Ασφαλείας - (KE.ME.A). Available at http://www.kemea.gr/el/ (accessed on March 9th, 2021)

[2] Available at http://www.cybercc.gr/ (accessed on March 10th, 202)

D. Ireland

1. National Cyber Security Strategy and Policies

In July 2013, the Department of Communications, Energy and Natural Resources published a National Digital Strategy entitled "*Doing More with Digital*"[1], to help Ireland reap the full benefits of a digitally activated society. Although the strategy sets several measures and targets for Ireland's digital development, engaging both the government, private companies and the people of Ireland, there is little reference to cyber security activities. The measures mainly concern the protection of users (with emphasis on children) from the dangers of the internet.

Ireland's first National Cyber Security Strategy was agreed by the Government and published in July 2015[2] and covers the period 2015 to 2017. It set out a road map for the development of the National Cyber Security Centre (NCSC)[3] and a series of measures to better protect Government data and networks, and critical national infrastructure. The Strategy was based on three key principles: the rule of law, subsidiarity, and proportionality. In accordance with these principles, the objectives that the Government aims to achieve through the implementation of the Strategy were to improve the resilience of critical information infrastructure in crucial economic sectors, particularly in the public sectors; to continue engaging with international partners and international organisations to ensure that cyber space remains open, secure, unitary and free and able to facilitate economic and social development; to raise awareness of the responsibilities of businesses and of private individuals around securing their networks, devices and information and to support them in this by means of information, training and voluntary codes of practice; to ensure that the State has a comprehensive and flexible legal and regulatory framework to enable An Garda Síochána to combat cybercrime. This framework must also be robust, proportionate, and fair. It is crucial that this frame pays due regard to the protection of sensitive or personal data to ensure that the regulatory framework that applies to the holders of data, personal or otherwise, is also robust, proportionate and fair; and to build capacity across public administration and the private sector to engage fully in the emergency management of cyber incidents.

Key measures also include to formally establish the NCSC, which would focus on securing government networks, critical national infrastructure and assisting individuals and industry in protecting their own systems; to improve the network and information security used by Government Departments and Agencies; to introduce primary legislation to formalise arrangements in law and to comply with EU requirements on capabilities, co-

[1] Department of Communications, Energy and Natural Resources, 'Doing more with Digital – National Digital Strategy for Ireland – Phase 1 – Digital Engagement', July 2013

[2] Department of the Environment, Climate and Communications, 'National Cyber Security Strategy 2015 – 2017', June 2015

[3] Available at https://www.ncsc.gov.ie/ (accessed on March 11th, 2021)

operation and reporting; to transpose the NIS Directive and bringing forward legislation to give effect to the Budapest Convention on Cybercrime and Directive 2013/40/EU on attacks against information systems; to engage with key partners on an international level with a view to delivering policy measures to improve cyber security; and to develop a programme of education and training for citizens and SMEs and foster general awareness.

On December 27, 2019,[1] the Irish Government published its five-year plan to ensure its infrastructure and computer networks are "*resilient, safe and secure*". The new National Cyber Security Strategy 2019-2024 is an update to the first strategy which was published in 2015. A key proposal is to develop Ireland's NCSC, increase incident monitoring, respond to incidents and threats and work with the Defence Forces and the Gardai (Police) on critical national infrastructure issues. The strategy recognises Ireland's role in hosting data centres for many world-leading tech companies. "*Ireland is home, according to some estimates, to over 30% of all EU data, and to the European Headquarters of many of the world's largest technology companies. Our economic success is therefore tightly bound up with our ongoing ability to provide a secure environment for these companies to operate here*", the document states. The strategy's other key deliverables include thus the appointment of Cyber Attachés to Ireland's key foreign diplomatic missions, ratification of the Budapest Convention on Cybercrime, expanding the current Threat Sharing Group (TSG), refining existing arrangements with the UK on information sharing and incident response and providing support to Cyber Ireland to develop a Cyber Security Cluster of industry, academia and government.

The strategy's main objectives are to continue to improve Ireland's ability to respond to and manage cybersecurity crisis, including those involving national security; Identify and protect critical national infrastructure by increasing its resilience to cyberattacks and ensure that OES have appropriate incident response plans for minimising and managing disruptions to services; Improve the resilience and security of public sector IT systems for better protecting data and services; Invest in educational initiatives to prepare the workforce for advanced IT and cybersecurity careers; Increase business awareness for securing their networks, devices and informations and for enhancing cybersecurity research and development in Ireland, including new technology investment; Continue to engage with international partners and international organisations to ensure that cyberspace remains open, secure, unitary, free and able to facilitate economic and social development; Increase the general level of skills and awareness among private individuals about basic cyber hygiene and support them with information and training.

The new strategy notes furthermore some of the changes that have taken place since the first version was published in 2015. For example, the NCSC itself has grown significantly in scale and capacity. The introduction of the EU Network and Information Security (NIS) Directive in 2016 has given Government departments and agencies a framework for managing their systems. The strategy gives special credence to Critical National

[1] Government of Ireland, 'National Cyber Security Strategy 2019-2024'

Infrastructure (CNI) across seven named sectors (energy, transport, drinking water, banking, financial markets, healthcare, and digital infrastructure). Seventy *Operators of Essential Services* have been identified and are subject to a formal set of security requirements and are obliged to follow a predefined reporting process in the event of a security breach. These developments mean that national infrastructure operators are "*far better prepared to deal with cyber security related risks than before*", the document says. One thing the report does well is to break down each of the 20 measures into their component parts, identify each component's owner and stakeholders and put a timeframe on each task's completion.

2. Legal Framework

i. Critical Information Infrastructure Protection

A CIIP or similar programmes were not in place at the time of the NIS Directive transposition

ii. Electronic communications legislation

Through the Communications Regulation Act of 2002[1] and secondary law (a series of legislative acts), Ireland transposed all the directives of the EU Electronic Communications Framework, namely: Directives 2002/21 / EC (Framework Directive) 2002 / 20 / EC (Licensing Directive) 2002/19 / EC (Access Directive) 2002/22 / EC (Universal Service Directive) and 2002/58 / EC (Directive on privacy in electronic communications).

Section 6 of the act establishes the Commission for Communications Regulation, which will replace the existing national regulatory authority, the Office of the Director of Telecommunications Regulation. The commission will consist of at least one but no more than three members, and the current director of telecommunications regulation, *Etain Doyle*, will automatically be appointed to the commission. Although the enforcement of competition law has been entrusted to the Irish Competition Authority under the Competition Acts 1991-2002, it is notable that one of the commission's objectives is to "*promote competition*", which includes ensuring that there is no distortion or restriction of competition in the electronic communications sector.

According to Section 10 of the act, the commission has to ensure the companies' compliance with their obligations in relation to the supply of and access to electronic communications services; to manage the radio frequency spectrum and the national numbering resource; to ensure compliance by providers of postal services with their obligations in relation to the provision of postal services; to investigate complaints in relation to the

[1] Available at http://www.irishstatutebook.ie/eli/2002/act/20/enacted/en/html, accessed on March 11th, 2021.

supply of and access to electronic communications services and networks; and to ensure compliance by persons in relation to the placing of communications equipment on the market.

Part 3 of the act sets the commission's powers of enforcement. Pursuant to Section 39, commission-appointed "*authorised officers*" may enter premises connected with the provision of electronic communications services and remove and retain books, documents or records for further examination. One of the most significant initiatives of the 2002 act is to substantially increase the penalties that may be imposed on telecommunications companies for a breach of a condition in their licences. Pursuant to Section 45, an undertaking may be liable on summary conviction to a fine not exceeding €3,000, or on conviction on indictment to a fine not exceeding €4 million or 10% of turnover in the previous financial year, whichever is the greater. Previously, the maximum fine that could be imposed for such a breach was €1,900.

3. National Authorities

i. Department of the Environment, Climate and Communications (DECC)

The Department of Communications, Climate Action and Environment (DECC)[1] is responsible for cyber security policy in Ireland. It is also responsible for coordinating the governmental emergency response to any national-level cyber security incidents. The Department published the National Cyber Security Strategy 2015-2017 in 2015, as well as the *Make IT Secure* awareness program. The Department discharges these responsibilities through the National Cyber Security Centre.

ii. National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC)[2] was established in 2011 following a government decision.[3] This decision was based on a detailed analysis of the evolving threats to security, and an assessment of the most appropriate type of organisation to respond to issues and to proactively improve the resilience of key infrastructure and services. This organisational concept has since come to represent best practice in Europe,

[1] Available at https://www.gov.ie/en/organisation/department-of-the-environment-climate-and-communications/?referrer=http://www.dccae.gov.ie/ (accessed on March 12th, 2021)

[2] Available at https://www.ncsc.gov.ie/ (accessed on March 12th, 2021)

[3] Government decision S180/20/10/481

primarily because it allows for the creation of a single critical mass of experience and operational expertise, and for the end-to-end management of incidents of all types.[1]

The Centre is largely located in rental accommodation on the UCD campus. The Centre's primary focus is on securing government networks, on assisting industry and individuals in protecting their own systems and on securing critical national infrastructure.[2] The core roles of the NCSC are to lead the cyber crisis management, provide assistance to citizens and businesses, and develop strong international cybersecurity relationships for the purposes of information sharing. Since 2011, the NCSC has focused its efforts on cyber capacity-building.

The NCSC contains the State's national/governmental Computer Security Incident Response Team (CSIRT-IE). CSIRT.IE[3] is the National CERT of Ireland which was instituted in 2013. It is an internationally accredited response team for the enhancement of situational awareness for constituents and for the provision of incident response for national cyber security incidents. CSIRT-IE has initially focused on the State sector and acts as a national point of contact for all cyber security matters concerning Ireland. Its functions include the enhancement of *situational awareness* and the provision of incident response for national cyber security incidents. Situational awareness is the perception of environmental factors and events in order to understand how information, events, and one's own actions will impact the environment immediately and in the future. The CSIRT.IE received on November 28, 2017, the *Trusted Introducer* accreditation, which signifies to the bodies that the CSIRT has reached a required level of maturity and operational capacity. CSIRT-IE has been also designated as the Single Point of Contact for the purposes of the EU Network and Information Security Directive.[4]

The 2019 – 2024 National Cyber Security Strategy states that, the NCSC, with the assistance of the Defence Forces and Garda Síochána, will perform an updated detailed risk assessment of the current vulnerability of all Critical National Infrastructure and services to cyberattack. It will also develop a baseline security standard to be applied by all Government Departments and key agencies. The NCSC will be tasked by the Government to issue recommendations regarding the use of specific software and hardware on Government IT and telecommunications infrastructure.

As both the assessment of Critical National Infrastructure carried out by the NCSC during the designation process and the application of the security measures after designation have shown that some of the infrastructure in the State outside of the scope of the NIS Regulations is in fact also critical, and that there are several interdependencies between Critical National Infrastructure sectors that are likely to give rise to risks.

---

[1] Government of Ireland, 'National Cyber Security Strategy 2019-2024'

[2] Critical national infrastructure comprises critical elements necessary for the delivery of essential services such as electricity, water, transportation, telecommunication, commerce and health.

[3] Available at https://www.ncsc.gov.ie/CSIRT/ (accessed on March 12th, 2021)

[4] Available at https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-ireland (accessed on March 12th, 2021)

iii. Ireland's National Police and Security Service

Ireland's National Police and Security Service[1] through the Garda National Cyber Crime Bureau (GNCCB),[2] investigates serious and complex fraud cases, such as cybercrime. The Bureau is the national Garda unit tasked with the forensic examination of computer media seized during any criminal investigations. In addition, the bureau conducts investigations into cyber dependent crime including network intrusions, data interference and attacks on websites belonging to Government Departments, institutions, and corporate entities. The Bureau is part of Organised & Serious Crime and is staffed by civilian personnel and Garda members of various ranks up to Detective Superintendent. Members of the unit undergo intensive training in forensic computing and cybercrime investigations and give expert witness testimony on all types of investigations and prosecutions in court. In addition to its forensic and investigative role, GNCCB acts as a liaison with various partner agencies and law enforcement bodies. The NCSC and Garda National Cyber Crime Bureau have developed a positive co-operative relationship with ongoing shared training and secondment opportunities for staff.

iv. Data Protection Commission (DPC)

The Data Protection Commission (DPC)[3] is the national independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. Individuals who feel their rights are being violated can lodge a complaint with the Commissioner, who will investigate the matter and take the appropriate steps necessary to resolve it. Accordingly, the DPC is the Irish supervisory authority responsible for monitoring the application of the GDPR, and we also have functions and powers related to other regulatory frameworks, including the Irish e-Privacy Regulations (2011)[4] and the EU Directive known as the Law Enforcement Directive.[5] The statutory powers, duties and functions of the DPC are as established under the Data Protection Act 2018, which gives further effect to the GDPR, and also gives effect to the LED.

[1] Garda Síochána. Available at https://www.garda.ie/en/?Page=29 (accessed on March 12th, 2021)

[2] Available at https://www.garda.ie/en/about-us/organised-serious-crime/garda-national-cyber-crime-bureau-gnccb-/ (accessed on March 12th, 2021)

[3] Available at https://www.dataprotection.ie/ (accessed on March 12th, 2021)

[4] S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, Prn. A11/1165

[5] OJ L 119, 4.5.2016, p. 89–131

v. Ireland's Cyber Defence

In general, Ireland's cyber defence relies heavily on self-regulation and agreements between trade unions, government, and corporations. The 2015 Defence White Paper notes that "*(...) the Department of Communications, Energy and Natural Resources has lead responsibilities relating to cyber security*" and explained that "*the primary focus of the Department of Defence and the Defence Forces will remain the protection of Defence networks*". However, "*(...) as in any emergency/crisis situation, once Defence systems are supported, the Department of Defence and the Defence Forces will provide support to the CSIRT-IE team in so far as resources allow*". As such, the role of Defence Forces regarding cyber security is explicitly a supporting one, with their primary responsibilities in this area relating to the protection of their own systems. This supporting role has evolved over time, and the Defence Forces continue to play a central role in facilitating the operations of the NCSC. The NCSC maintains close cooperation with the Defence Forces and the Gardaí on national security issues and has a secondment arrangement with both entities.

E. Luxembourg

1. National Cyber Security Strategy and Policies

The National Cybersecurity Strategy was announced in Luxembourg by the Ministry of Justice in 2012 during a conference on cybersecurity.[1] This document sets out action lines for enhancing the security and resilience of infrastructure and thus helps to protect the citizens of professionals and participants in public life in the digital environment. To achieve the above, the Strategy defines five pillars: Ensuring the functionality of the infrastructure of communication and information processing systems. The operational measures aimed at achieving this goal are the establishment of an Emergency Plan, the implementation of information security response exercises and sensitive or critical communications, the participation in European exercises, and the establishment of a specialised agency able to handle security incidents; The modernisation of the legal framework to respond to changes in technology and the internationalised environment of cyberspace; The development of national and international cooperation. At national level, effective cooperation between all actors is defined as a precondition for the implementation of the strategy. At the international level, cooperation can be based on multilateral relations with the BENELUX countries, Interpol and Europol, the EU, the Council of Europe, NATO, the OECD and the OSCE; Information, education, and risk awareness to all stakeholders, i.e., end users, students, parents, teachers, civil servants, small and medium-sized enterprises, service providers and infrastructure operators; and to Establish standards for risk analysis methods, policies, and safety standards.

[1] Gouvernement du Grand-Duché de Luxembourg, 'Stratégie nationale en matière de cyber sécurité', November 2011

A second version of the national cybersecurity strategy (SNCS II) was approved by the government on March 27, 2015.[1] The working group in charge of revising the first version of 2012, chaired by the High Commission for Protection national and composed of representatives of the State Information Technology Centre, the government CERT, the Media and Communications Service, the Ministry of the Economy, the Government Communications Centre, the Intelligence Service, the Grand-Ducal and Army Police, first of all analysed the impact of the strategy adopted in 2012 and then made the changes that turned out to be necessary based on the conclusions of the said analysis. Therefore, the adaptation of this strategic document corresponds to the axes defined in 2012 and reflects the will, even the determination of Luxembourg to provide the country with electronic communication infrastructures that meet international security standards.

The new cybersecurity strategy aimed to protect public and private actors against cyberthreats while promoting economic and social development in cyberspace. Therefore, the government recognised that information security should not be seen as a burden, but rather as an opportunity. It is about democratising information security by promoting collaboration while reducing complexity and costs for all stakeholders. The government intended thus to achieve this goal by defining the following objectives and action plans: Strengthen national cooperation; Strengthen international cooperation; Increase the resilience of digital infrastructure; Fight cybercrime; Inform, train and raise awareness of the risks involved; Establish norms, standards, certificates, labels and requirements repositories for the State and critical infrastructures; and Strengthen cooperation with academia and research. These objectives have been defined by the Government for the next three years. Each objective is thus supplemented by an action plan which describes the concrete measures to be implemented according to a determined timetable, as well as the actors called upon to contribute to their implementation.

As the cybersecurity strategy is intended to evolve over time, it was revised again in 2018[2] to adapt to new realities. The new national cybersecurity strategy (SNCS III) shows that the Government is aware of both the opportunities and the risks inherent in new technologies. It is with this in mind that the strategy, which covers the period 2018-2020, is structured around the following three central guidelines: strengthening public confidence in the digital environment; the protection of digital infrastructures, as well as the promotion of the economic place. To perpetuate governance in cybersecurity and facilitate the implementation of the objectives of SNCS III, an inter-ministerial coordination committee has been set up by the Government.

The objectives of this strategy are once again supplemented by an action plan which describes the technical measures to be implemented according to a determined timetable, as well as the actors called upon to contribute to their implementation. The action plan is available on request from the Office of the High Commissioner for National Protection, while the Cybersecurity Board and the Interministerial Cybersecurity Coordination

[1] Gouvernement du Grand-Duché de Luxembourg, Stratégie Nationale en matière de Cybersécurité II, 2015

[2] Gouvernement du Grand-Duché de Luxembourg, Stratégie Nationale en matière de Cybersécurité III, 2018

Committee support the execution of the action plan. The action plan will thus be periodically revised within the interministerial coordination committee, to remain updated with a constantly changing digital environment.

2. Legal Framework

i. Critical Information Infrastructure Protection

A CIIP or similar programmes were not in place at the time of the NIS Directive transposition

ii. Electronic communications legislation

The Law of May 30, 2005[1] transposed the EU regulatory framework for electronic communications (Directives 2002/19 / EC, 2002/20 / EC, 2002/21 / EC, 2002/22 / EC). It is part of the Luxembourg Telecommunications Legislation package, which also includes a special law on the processing of personal data in the field of electronic communications. The law regulates access to electronic communications networks and their interconnection by creating a sustainable and competitive environment, as well as ensuring the interoperability of electronic communications services.

The amended law of February 27th, 2011, on electronic communications networks and services,[2] which was put into force on April 1st, 2011, deals in Title VII, Articles 45 and 46 with the security and integrity of electronic communications networks and services accessible to the public. The methods of notification of security measures to be taken by companies providing public communications networks and / or electronic communications services to the public within the framework of article 45 (1) and (2) of the law of February 27th, 2011 on electronic communications networks and services are detailed in Regulation 15/200 / ILR of December 18th.[3] Criteria and thresholds in relation to the significant impact on the operation of networks or services that must be reported to the Institute in the event of a security breach or loss of integrity of electronic communications networks and services are set by Regulation 14/181 / ILR of August 28th, 2014[4] defining criteria and thresholds in relation to the significant impact on the operation of networks or services that must be reported

[1] Loi du 30 mai 2005 sur les réseaux et les services de communications électroniques, JO A-N°73 7.6.2005

[2] Loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques, JO A-N°43 8.3.2011

[3] Institut Luxembourgeois de Régulation - Règlement 15/200/ILR du 18 décembre 2015 portant sur les modalités de notification des mesures de sécurité à prendre par les entreprises fournissant des réseaux de communications publics et/ou des services de communications électroniques au public dans le cadre de l'article 45 (1) et (2) de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques - Secteur Communications électroniques

[4] Institut Luxembourgeois de Régulation - Règlement 14/181/ILR du 28 août 2014 portant définition de critères et de seuils en relation avec l'impact significatif sur le fonctionnement des réseaux ou des services à signaler obligatoirement à l'Institut en cas d'atteinte à la sécurité ou à la perte d'intégrité de réseaux et de services de communications électroniques - Secteur Communications électroniques

to the Institute in the event of breach of security or loss of integrity of electronic communications networks and services.

A bill[1] transposing Directive (EU) 2018/1972[2] of the European Parliament and of the Council of 11 December 2018, which establishes the European electronic communications code, and amending the law of 30 May 2005 was under discussion in July 2020. Directive (EU) 2018/1972 overhauls the 4 directives (2002/19 / EC, 2002/20 / EC, 2002/21 / EC, 2002/22 / EC) that are part of the regulatory framework applicable to electronic communications networks and services. The bill continues thus to consolidate the internal electronic communications market, which results in increased effective competition aimed at avoiding any distortion on the market. The purpose of the bill is primarily to facilitate the launch of new very high capacity fixed networks, by making the rules applicable to co-investments more predictable and by encouraging risk sharing in the deployment of very high capacity networks and by promoting a sustainable competition for the benefit of consumers; promote the deployment of 5G networks, by ensuring the availability of 5G radio frequencies in the Union by the end of 2020 and by offering operators predictability in the granting of spectrum licenses , in particular through better coordination of radiofrequency allocation forecasts; set up a universal service now including an adequate access service to broadband Internet at an affordable price; and to strengthen consumer protection by encouraging transparency in pricing and comparison of contractual offers. The bill then introduces many new features into the Luxembourg system which can also be found in the directive to be transposed, such as the migration from ex post regulation to ex ante regulation of dominant operators, the introduction of very high-capacity networks or even the Access to wireless local area networks.

3. National Authorities

The large number of sectors, areas and policies affected by cybersecurity make the subject a matter of responsibility and attributions to several state entities.

i. Ministry of the Economy

In the application of the Grand-Ducal decree of January 28, 2015[3] to establish the ministries, the Ministry of Economy is responsible for IT security, risk awareness and private sector vulnerabilities. In this context, the

[1] Available at https://www.csl.lu/fr/telechargements/avis/37d482d3d7 (accessed on March 13th, 2021)

[2] OJ L 321, 17.12.2018, p. 36–214.

[3] Arrêté grand-ducal du 28 janvier 2015 portant constitution des Ministères, JO A-N°15 30.1.2015

Security Made in Luxembourg Economic Interest Group (GIE Smile)[1] is tasked with supporting information and communication systems security strategies through the Cyberworld Awareness & Security Enhancement Services (CASES), the National Cybersecurity Skills Centre (C3), the Computer Incident Response Centre Luxembourg (CIRCL), a post-incident coordination and action service, the latter also performing the function of CERT for private and non-governmental entities and municipalities.

ii. Directorate of Defence and the Luxembourg Army

Luxembourg Defence (Ministry of Foreign and European Affairs (MAEE) - Directorate of Defence and the Luxembourg Army) is in charge of cybersecurity aspects that fall within its national responsibilities and obligations generated within NATO and the EU.

iii. Ministry of State's Media and Communications Service

The Ministry of State - Media and Communications Service follows the Telecom Council which is discussing at European level both the European cybersecurity strategy and the *cybersecurity package*. The Media and Communications Service also coordinates the work of the Cybersecurity Board which, according to the Grand-Ducal Decree of January 28, 2015[2] establishing the ministries, falls within the competence of the Ministry of State.

iv. Ministry of Foreign and European Affairs

The Ministry of Foreign and European Affairs[3] coordinates the work at the level of the horizontal Cyber Working Group of the Council of the European Union, which has just drawn up the *cyber diplomatic toolbox*[4] adopted in June 2017.

[1] Available at https://te.public.lu/fr/participations/etablissements_publics/Smile.html (accessed on March 13th, 2021)

[2] Arrêté grand-ducal du 28 janvier 2015 portant constitution des Ministères, JO A-N°15 30.1.2015

[3] Available at https://maee.gouvernement.lu/fr.html (accessed on March 13th, 2021)

[4] See E. Moret and P. Pawlak, 'The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?', (2017) *European Union Institute for Security Studies (EUISS)*

v. Luxembourg Regulatory Institute

The Luxembourg Institute of Telecommunications (ILR)[1] was established in 1997 to ensure that all competitors can offer their services on an equal footing and without being able to abuse their market position. Its main mission was to establish rules and conditions allowing the creation of a fair environment for all telecommunications operators. The ILR became the national regulatory authority for this sector but was also responsible for the management of radio frequencies. The ILR had to then extend its missions to energy and postal services sectors and was replaced in 2000 by the ILR.[2]

The board of directors adopts the Institute's budget and annual accounts and decides on the terms of financing by the operators of the Institute's operating costs. Other board tasks include the appointment of an auditor; approval of the internal management rules; approval of acts having an impact on the budget; and approval of the staffing report.

The ILR is organised into different departments according to the sectors for which it is responsible. Specific technical experts are grouped together in each service and the functions of international representations are performed in each service. The Institute counts 63 employees.

vi. The Financial Sector Supervisory Commission

The Financial Sector Supervisory Commission CSSF[3] is a public institution created through an organic law on December 23rd, 1998, which supervises the professionals and products of the Luxembourg financial sector. This law defines the CSSF tasks and scope.

The CSSF is among other things responsible for ensuring compliance with professional obligations in the fight against money laundering and the financing of terrorism by all persons supervised, approved, or registered by it. Activities which often fall under the category of malicious activities in cyberspace. The CSSF has a wide range of measures enabling it to act against persons subject to its supervision who contravene the regulations relating to the financial sector applicable to them or who do not comply with the professional obligations imposed on them. It also cooperates with the Central Bank of Luxembourg, the European supervisory authorities and other prudential supervision and resolution authorities at European and international levels.

The CSSF Council is made up of seven members appointed by the Grand Duke on a proposal from the government in council for a period of five years. The Directorate is the superior executive authority of the CSSF.

---

[1] , 'Institut Luxembourgeois des Télécommunications (ILR)

[2] Available at https://web.ilr.lu/FR/ILR (accessed on March 13th, 2021)

[3] Commission de Surveillance du Secteur Financier (CSSF). Available at https://www.cssf.lu/fr/ (accessed on March 13th, 2021)

It is made up of a director general and two to four directors appointed by the Grand Duke on a proposal from the government in council for a period of five years. Among others, a responsible is appointed for protecting the information used by the CSSF to carry out its mission. Its objective is to provide the Directorate with a comprehensive and continuous view of the risks related to information security to which the CSSF is exposed or could be exposed. It works on the implementation of the security policy adopted by the Directorate, oversees the application of security measures and ensures their effectiveness. It coordinates security actions to have the best control.

Lastly, the information systems monitoring along with the professional supporting service in the financial sector are responsible for: monitoring the information systems of supervised entities, as well as auditing them; on-site inspections, evaluation of the IT part of the reports of external and internal auditors communicated to the CSSF, technical advice on specific questions or on the internal IT system, IT security and national or international work in IT; prudential supervision of professionals listed in Articles 29-1 to 29-6 of the Law of April 5th, 1993 on the financial sector and the examination of periodic financial information to be submitted to the CSSF, on-site inspections and analysis of the comments and the assessment provided by the approved statutory auditors and the internal auditors of the support PSF. Also, the Information Systems department of the CSSF (IT) is in charge of the information systems used by the CSSF for the performance of its missions. The service is in charge of project management, IT developments and IT production, i.e., the management of technical infrastructure including servers and networks, as well as applications and databases.

vii. State's Information Technologies Centre

The State's Information Technologies Centre (CTIE)[1] falls under its amended organic law of April 20, 2009.[2] Its mission is, among other things, to ensure, within the framework of its attributions, the security of the IT, the management of electronic and computer equipment and appropriate security, the administration of the State's computer network as well as the production of secure administrative documents.

viii. State's Intelligence Service

The State's Intelligence Service, for its part, has the task of researching, analysing, and processing information relating to cyber threat, insofar as it may be related to espionage. , interference, terrorism, violent

[1] Available at https://ctie.gouvernement.lu/fr.html (accessed on March 13th, 2021)

[2] Loi du 20 Avril 2009 portant création du Centre des technologies de l'information de l'Etat, JO A-N°81 27.4.2009

extremism, and the proliferation of weapons of mass destruction or defence-related products and related technologies.

ix. High Commission for National Protection

The High Commission for National Protection (HCPN)[1] is an inter-service and civil-military committee for consulting, coordinating, and planning the various areas of national protection. Its action is defined through the emergency response plan in the face of attacks against information systems, from the moment the crisis is likely to generate serious consequences for part of the territory or the population of Luxembourg. It also acts as the National Agency for the Security of Information Systems (ANSSI), whose mission is to develop guidelines for information security. The Governmental Centre for the Treatment of Computer Emergencies (GOVCERT),[2] which also operates under the responsibility of the High Commission for National Protection, intervenes in the management of large-scale security incidents affecting networks and communication systems.

x. Inter-ministerial Coordination Committee for Cyber Prevention and Cybersecurity

Given that the subject of cybersecurity covers a whole panoply of fields and falls under the remit of several state entities, the Government decided, on December 13, 2017,[3] to set up an inter-ministerial committee which brings together the actors concerned, and which is responsible for ensuring national coordination in cybersecurity. The committee should ensure, alongside the rather strategic Cybersecurity Board, the pragmatic coordination of initiatives forming part of cybersecurity. To this end, the committee's mission is to ensure the consistency of actions and initiatives undertaken in the areas of cyber prevention and cybersecurity; to coordinate the implementation of initiatives launched and measures decided at European and international level in the field of cyber prevention and cybersecurity; to monitor the implementation at national level of policies decided at European and international level; to advise the Government on cyber prevention and cybersecurity by identifying the subjects and priorities to be explored in this area, as well as the actors responsible for their implementation; and to discuss the positions to be adopted by national representatives in European and international forums in the area of cyber prevention and cybersecurity. The committee is made up of members of the main state entities that intervene at the national level in cybersecurity, and the committee is chaired by the High Commissioner for National Protection which is also responsible for secretariat.

[1]Available at https://hcpn.gouvernement.lu/fr.html (accessed on March 13th, 2021)

[2] Available at https://www.govcert.lu/en/ (accessed on March 13th, 2021)

[3] J. Mercier, 'Une cybersécurité désormais coordonnée', [Article Online] *Paperjam*, 13 December 2017, available at https://paperjam.lu/article/news-une-cybersecurite-desormais-coordonnee (accessed on March 13th, 2021)

xi. National Commission for Data Protection

The National Commission for Data Protection (CNPD)[1] is an independent body responsible for overseeing the legality of file collection and for the uses and transmission of information. In this context, it must ensure respect for the fundamental rights and freedoms of individuals, in particular the right to privacy. The CNPD produces an annual report on its activities, which includes a list of the types of infringements notified and the types of sanctions imposed in accordance with Regulation 2016/679 (GDPR) and the Act of 1 August 2018[2] on the protection of natural persons with regard to the processing of personal data in criminal and national security matters. These reports are submitted to the Chamber of Deputies, the Government, the European Commission and the European Data Protection Board and are made public. The CNPD has investigative powers, corrective powers, authorisation, and advisory powers.

The CNPD is a collegiate body constituted up to four members[3]. The members are called Data Protection Commissioners and are authorised to use the title of *Commissioner*[4]. Four deputy members are also appointed. The deputy members are called to replace members of the college when they are absent or unable to attend. It operates in the form of a public establishment under the supervision of the Minister whose responsibilities include data protection. It is nevertheless independent in the exercise of its functions.

The CNPD meets regularly for deliberations. The college may validly sit and deliberate only if at least three members of the college are present. The decisions are adopted by majority vote[5]. The members of the college and the deputy members cannot sit, deliberate, or adopt decisions in cases where they have a conflictual interest. The internal rules of procedure are adopted unanimously by the members of the college in plenary session. These rules, which are published in the Official Gazette of the Grand Duchy of Luxembourg, determine operating conditions for the CNPD; the organisation of the services of the CNPD; and the procedures for convening the members of the college and holding collegiate meetings.

In addition to its statutory tasks in national terms, the CNPD is also responsible for taking part in implementing and supervising observance of the protection of individuals regarding automatic processing of

[1] Available at https://cnpd.public.lu/fr.html (accessed on March 13th, 2021)

[2] Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, JO A-N°686 16.8.2018

[3] One of which is a President.

[4] With this title having no impact on their rank or their remuneration.

[5] If the number of votes is equal, the president has the deciding vote. Abstentions are not permitted.

personal data at both the European and international levels. The CNPD represents the Grand Duchy of Luxembourg on a number of bodies and working parties, various Council of Europe committees, and the body that supervises application of the Schengen Agreements.

F. Poland

1. National Cyber Security Strategy and Policies

Published in 2010, the *Polish Cyber Protection Program 2011-2016* was currently the most important document planning actions related to the Polish cyberspace.[1] The Program recommended actions that would lead to the prevention and control of threats and includes proposals for legal, organisational, technical, and educational activities. In addition, the goal of the Program was to identify the bodies responsible for cyber security. It also aimed to establish a risk assessment system for public bodies (which will include guidelines for private bodies as well), and a coordination system for threat mitigation and prevention, as well as for cooperation and exchange of information with partner countries, international organisations and above all, with the private sector. Other proposed solutions aimed at improving cyber security include the creation of an Inter-ministerial Coordination Group, responsible for coordinating cyber security-related actions. The project also called for changes in cyber security legislation (e.g., on cybercrime). In addition, the program provided for the appointment of a Government Representative and a representative to head the cyber organisation for the protection of public administration, as well as the creation of a similar position for the private sector. The Ministry of Interior was considered responsible for bringing the program into force.

However, the first national cyber security strategy, entitled "*Cyberspace protection policy of the Republic of Poland*" was launched in 2013 by the Internal Security Agency of the Ministry of Public Administration and Digitisation.[2] The Policy, which relies on a comprehensive cybersecurity strategy with clear goals, defined a series of specific objectives. Among them we denote the following: Increasing the level of security of the State ICT infrastructure, Improving the capacity to prevent and combat threats from cyberspace; Reducing the impact of incidents threatening the ICT security; Determining the competence of entities responsible for the security of cyberspace; Creating and implementing a coherent system of cyberspace security management for all government administration entities and establishing guidelines in this area for non-state actors; Creating a sustainable system of coordination and exchange of information between the entities responsible for the security

[1] Ministerstwo Spraw Wewnętrznych I Administracji, 'Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej Na Lata 2011-2016', Czerwiec 2010

[2] Ministry of Administration and Digitisation, Internal Security Agency, 'Cyberspace Protection Policy Of The Republic Of Poland', June 2013

of cyberspace and the cyberspace users; and Increasing awareness of cyberspace users on the methods and safety measures in cyberspace.

In March 2017, a draft cyber security strategy was published for years 2017 to 2022, in response to the changing threat landscape and to the European NIS Directive on protecting national networks and systems, and which demands a more coordinated approach from EU members.[1] After the adoption of the Cybersecurity Act from the EU, which introduces a common cybersecurity certification scheme for IT products and services, valid in all EU countries, Poland's Ministry of Digitisation has drafted a cybersecurity strategy for 2019-2024.[2] The strategy will develop the country's National Cybersecurity System established by a law adopted last year, which allocated tasks and responsibilities to prevent and minimise the effects of cyberattacks in Poland. By implementing the Cybersecurity Strategy of the Republic of Poland for 2019–2024, the government of Poland will fully guarantee the right to privacy and hold the position that free and open Internet is an important element of the functioning of a modern society. It will also seek to expand Poland's information-exchange system and boost its cybersecurity technology potential. Other proposals include mechanisms for cooperation between the public and private sector, so that officials and entrepreneurs can better address cyber threats.

2. Legal Framework

i. Critical Information Infrastructure Protection

Pursuant to Article 3 (2) of the Act of April 26th, 2007, on crisis management,[3] critical infrastructure is understood as systems and mutually bound functional objects contained therein, including constructions, facilities, installations and services of key importance for the security of the state and its citizens, as well as serving to ensure efficient functioning of public administration authorities, institutions and enterprises.

The essence of the tasks related to critical infrastructure comes down not only to ensuring its protection against threats, but also to ensuring that the potential damage or disruption of its functioning is short-lasting, easy to remove and not causing additional losses for the citizens and the economy. The Critical Infrastructure Protection (CIP) is understood as all steps aimed at ensuring the functionality, continuity, and integrity of critical infrastructures in order to prevent threats, risks or vulnerabilities and limitations as well as neutralising their effects. It will also allow a quick reconstruction of the infrastructure in case of failures, attacks and other events disrupting its appropriate functioning.

[1] Ministerstwo Cyfryzacji, 'Strategia Cyberbezpieczenstwa Rzeczypospolitej Polskiej Na Lata 2017–2022', 2017

[2] Ministry of Digital Affairs, 'Cybersecurity Strategy Of The Republic Of Poland For 2019–2024', 2019

[3] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r. Nr 89, poz. 590

Outline of threats, risk assessment, information about critical infrastructures can be found in the National Critical Infrastructure Protection Plans.[1] This Plan is based on the National Security Threats Report,[2] which in turn is developed pursuant to the Act of April 26th, 2007, on crisis management[3] and Regulation of the Council of Ministers of 30/4/2010[4] laying down the list of the most serious potential threats that may cause a crisis situation. A National Critical Infrastructure Protection Programme (NCIPP) under provision of the Crisis Management Act has been adopted by the Council of Ministers on 26th March 2013 and updated in 2015 and 2020.[5] It outlines a series of actions with the purpose of improving the security and resilience of critical infrastructure in Poland. The Government Centre for Security is responsible for the preparation of the National Critical Infrastructure Protection Programme in close collaboration with the ministers and heads of central offices competent in matters of national security as well as responsible for the following systems: Energy, fuel and energy resources supply systems, Communication systems, Tele-information network systems, Financial systems, Food supply systems, Water supply systems, Health protection systems, Transportation systems, Rescue systems, Systems ensuring the continuity of public administration activities, Systems of production, storing and use of chemical and radioactive substances, including pipelines for hazardous substances; The Programme aims at creating conditions for improving the security of critical infrastructure, in particular: preventing the malfunctioning of critical infrastructure; preparing for crisis situations that could adversely affect critical infrastructure; response in the event of destruction or disruption of critical infrastructure functioning; and reconstruction of critical infrastructure. The Programme specifies national priorities, objectives, requirements and standards, to ensure the smooth functioning of critical infrastructure; the ministers in charge of government administration units and heads of central offices responsible for the systems mentioned above; and detailed criteria which enable to identify objects, installations, facilities and services included in the critical infrastructure systems, taking their importance into account for proper functioning of the state and satisfying the needs of the citizens.

Cooperation between public administrations under the CIP is based on constant exchange of information, which accelerates and increases the effectiveness of the protection and influence on the process of security management of critical infrastructure. The cooperation includes, in particular: a database of experts on issues related to critical infrastructure within the CI sectors. Experts database speeds up the process of consultation and at the same time provides substantive support in the event of disruption of the CI and within the framework

[1] Narodowy Program Ochrony Infrastruktury Krytycznej, available at https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej (accessed on March 16th, 2021)

[2] Raport o zagrożeniach bezpieczeństwa narodowego, https://www.gov.pl/web/rcb/raport-o-zagrozeniach-bezpieczenstwa-narodowego (accessed on March 16th, 2021)

[3] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r. Nr 89, poz. 590

[4] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz. U. z 2010 r Nr 83, poz. 542

[5] Narodowy Program Ochrony Infrastruktury Krytycznej, available at https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej (accessed on March 16th, 2021)

of public-private forum; CIP contact points lists within the public administration and governmental services (including ministries, central offices, voivodeship offices, Police Headquarters, Internal Security Agency, Intelligence Agency and the Headquarters of the Border Guards and State Fire Service); and participation in the development, revision and implementation of the National Critical Infrastructure Protection Programme.

ii. E-commerce

The e-Services Act entered into force on 10 March 2003.[1] It implements the provisions of Directive 2000/31 / EC on certain legal aspects of information society services, in particular e-commerce, in the internal single market. Among other issues, the law regulates the obligations and responsibilities of electronic service providers, as well as the protection of personal data of individuals using electronic services. The issue of spamming is also being addressed.

iii. Electronic Communications

Adopted in July 2004 and entered into force on September 3, 2004, the Law on telecommunications transposes the EU regulatory framework for electronic communications.[2] It was then amended in 2005 to upgrade the telecommunications regulatory process, better align national provisions in EU regulations, and introduce new regulations which favour consumers.

3. National Authorities

i. Digital Affairs Ministry

The Digital Affairs Ministry[3] performs several tasks, including those falling within the scope of the digitisation of public administration, techniques, and standards, as well as supporting investments in the field of information technology, the implementation of IT solutions in information society and its development. Finally, it fulfils Poland's international IT commitments. The ministry is responsible for coordinating, preventing, dealing with and rehabilitating disasters, including in the IT and telecommunications sectors, as it has taken over these responsibilities from the Ministry of Interior.

[1] Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług, Dz.U. z 2004 r. Nr 54, poz. 535

[2] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. z 2004 r. Nr 171, poz. 1800

[3] Ministerstwo Cyfryzacji. Available at http://archiwum.mc.gov.pl/en/the-areas-of-our-activity (accessed on March 16th, 2021)

ii. Internal Security Agency

The Internal Security Agency (ISA)[1] is a government institution which protects the internal security of the Republic of Poland and its citizens. Its primary objective is to know as much and as early as possible in order to effectively neutralise threats to the State's internal security. The ISA's status of a special service as well as its tasks and powers are regulated by a single law – the Internal Security Agency and Foreign Intelligence Agency Act of 24 May 2002.[2] The ISA carries out its duties following both the spirit (rule) of legalism and the rule of law, which are characteristic of every single act undertaken by ISA officers.

The scope of tasks given to the ISA was complemented by several operational and investigative powers. In carrying out their tasks specified by statute, ISA officers have the same investigative powers as the Police under the Code of Criminal Procedure. The ISA can, on order from a court of law or a public prosecutor's office, carry out acts in proceedings specified in the Code of Criminal Procedure or the Punishment Execution Code. While carrying out their duties ISA officers may, among other things, carry out the following acts within the limits of existing legal provisions: Order specific behaviour; Require individuals to produce their ID or give their personal details; Arrest individuals; Search individuals and premises; Carry out body searches; Inspect the contents of luggage as well as cargo in land, air and water transport; Require help from government institutions, government and self-government administration bodies as well as entrepreneurs doing business in the Public Utilities Services sector; and Request indispensable help from other (...) entrepreneurs, entities and public organisations, and to request any person, in situations of utmost urgency and within the limits of binding legal regulations, for immediately needed assistance.

The ISA has its own, specialised anti-terrorist team whose tasks include, among other things, making sure arrests are made safely during investigations run by the Agency. To gather evidential material for court, it is often necessary to use sophisticated scientific expertise in many fields. In organisational structure the ISA has a special unit - Forensic Laboratory where specialists in various branches of science carry out examinations and give expert opinions on evidence obtained in proceedings. The ISA operational and investigative powers are subject to supervision by various democratic institutions, from the President of the Republic of Poland, from the Parliament of the Republic of Poland, from the Constitutional Tribunal and from the Commissioner for Civil Rights Protection.

[1] (Agencja Bezpieczeństwa Wewnętrznego. Available at https://www.abw.gov.pl/en/ (accessed on March 16th , 2021)

[2] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczenstwa Wewnetrznego oraz Agencji Wywiadu, Dz.U. z 2002 r. Nr 74, poz. 676

iii. Government Centre for Security (Rządowe Centrum Bezpieczeństwa)

Established under the Act of 26 April 2007 on Crisis Management (article 10),[1] the Government Centre for Security (GCS)[2] is responsible for coordinating critical infrastructure actions. The GCS is a supraministerial structure which aims to optimise and standardise the perception of threats by individual government departments, thereby increasing the degree of ability to cope with difficult situations by the competent services and public administration authorities. The GCS helps to organise the functioning of the units responsible for crisis management, created pursuant to the provisions governing the functioning of public administration authorities in the event of natural disasters.

The GCS shall ensure services to the Council of Ministers, Prime Minister, the Government Crisis Management Team, and a minister competent for internal affairs within the scope of crisis management. Moreover, the Centre serves as a national centre for crisis management. The Government Centre for Security has been operating since August 2nd, 2008.

Currently, the organisational structure and operating mode of the Centre is regulated by a Regulation of the Prime Minister of 11 April 2011 on the organisation and operating mode of the Government Centre for Security. It is a state budget unit subordinated to the Prime Minister.

iv. Office of Electronic Communications (Urzędu Komunikacji Elektronicznej)

The Office of Electronic Communications (UKE)[3] is the regulatory authority responsible for telecommunications and postal activities and frequency resources management. It is also a supervisory authority responsible for controlling compliance of products emitting or vulnerable to emission of electromagnetic field, including radio equipment placed on the market in Poland. Its tasks include, inter alia, regulating and supervising telecommunications services, managing radio spectrum, and enforcing compliance with electromagnetic compatibility requirements.

[1] Narodowy Program Ochrony Infrastruktury Krytycznej, available at https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej (accessed on March 16th, 2021)

[2] Available at https://rcb.gov.pl/ (accessed on March 16th, 2021)

[3] Available at https://www.uke.gov.pl/en/ (accessed on March 16th, 2021)

vi. Cyber Security Emergency Response Teams

Also known as CERT POLSKA, the CERT.PL operates as part of the Research and Academic Computer Network (NASK). It is a member of FIRST (international forum of response teams) and part of the working group of European response teams (TERENA TF-CSIRT). In 2005 it formed the Abuse Forum and in 2010 joined the Anti-Phishing WG, which brings together companies and institutions actively fighting crime on the network. Its main tasks include recording and handling network security incidents; responding to incidents; co-operating with other CSIRTs in Poland and globally; malware analysis systems and exchanging information on threats; developing tools for detection, monitoring, analysis, and correlation of risks; regularly publishing national reports on national internet resources.

CERT.GOV.PL[1] is the Government team and its main task is to protect the public administration from cyber threats. The team is part of the Polish Internal Security Service and the services provided include coordination of the incident response process, publication of security threat notifications, detection, resolution and analysis of security incidents. CERT Polska, CERT GOV PL and the national Internal Security Agency are the main contact points for IT security. Responsibility for combating cyber threats lies with CERT.GOV.PL which is a coordination platform for dealing with incidents that threat the security of information systems or networks used by government agencies whose destruction could lead to a serious disruption of the country. One of the tasks of the team is to implement and oversee the Arakis-GOV early warning system.[2]

§2. Comparative Analysis: The obligation of 'Due Time' Transposition and the Minimum Harmonisation Provisions

The first part focuses on a comparative analysis on the due time obligation for the transposition of the NIS Directive (**A**). While a second one highlights the national transposition of NIS Directive's minimum harmonisation provisions (**B**). The last section concludes with an account of the NIS Directive transposition results (**C**).

[1] Available at http://www.cert.gov.pl/ (accessed on March 16th, 2021)

[2] Available at https://csirt.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html?search=5688448729351 (accessed on March 17th, 2021)

A. The obligation of 'Due Time' Transposition

The NIS Directive was adopted on July 6th, 2016, and left an almost two-year period to EU Member States for adopting and publishing by May 9th, 2018, the laws, regulations, and administrative provisions necessary to comply with the NIS Directive. On October 2nd, 2019, from the 28 Member States (The United Kingdom included) only 8 States had transposed the NIS Directive in due time (The Czech Republic, Cyprus, Finland, Germany, Slovakia, Slovenia, Sweden, and the UK). On 19 July 2018 the Commission sent a notification to 17 Member States,[1], asking them to "*fully transpose the NIS Directive into national law*". Although Estonia, Italy and Malta had transposed the NIS Directive with delay no formal notice (according to Article 258 TFEU) was found for them. A situation making important the need for the Commission to be transparent on formal notices' content. From the 17 Member States notified by formal notice on July 19th, 2018, Belgium and Luxembourg had almost exceeded one year from the transposition deadline. Meanwhile, Hungary still had a partial transposition status of the NIS Directive on October 2nd; 2019 (**Table 25**).

NIS Transposition status on 02.10.2019					
States	**Status**	**Transposition date**	**States**	**Status**	**Transposition date**
Austria	Transposed	28.12.2018	Italy	Transposed	09.06.2018
Belgium	Transposed	03.05.2019	Latvia	Transposed	24.10.2018
Bulgaria	Transposed	13.11.2018	Lithuania	Transposed	03.07.2018
Czech Republic	Transposed	01.08.2017	Luxembourg	Transposed	28.05.2019
Croatia	Transposed	15.02.2019	Malta	Transposed	06.07.2018
Cyprus	Transposed	05.04.2018	Netherlands	Transposed	08.11.2018
Denmark	Transposed	10.05.2018	Poland	Transposed	13.08.2018
Estonia	Transposed	22.05.2018	Portugal	Transposed	13.08.2018
Finland	Transposed	09.05.2018	Romania	Transposed	28.12.2018
France	Transposed	25.05.2018	Slovakia	Transposed	30.01.2018
Germany	Transposed	29.06.2017	Slovenia	Transposed	26.04.2018
Greece	Transposed	23.12.2018	Spain	Transposed	08.09.2018
Hungary	Partial transposition	18.09.2018	Sweden	Transposed	22.06.2017
Ireland	Transposed	21.09.2018	United Kingdom	Transposed	20.04.2018

Table 25: *NIS Transposition status on 02.10.2019*

(Table made by author)

[1] Austria, Bulgaria, Belgium, Croatia, Denmark, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, and Spain.

More specifically, the six Member States considered in this study have transposed the NIS directive each in their own manner. Among those Member States, only Finland had fully transposed the NIS Directive in due time. France had *partially* transposed the directive, while transposition was *in progress* for the others.[1]

In Finland, transposition study of the NIS Directive started on October 7th, 2016, with the establishment of a working group of the Ministry of Transport and Communications of Finland. On April 20th, 2017, the working group published a closing report regarding their proposals for guidelines on how to transpose the NIS Directive.[2]

On December 19th, 2017, the Finnish Government submitted a proposal to Parliament for legislative amendments to improve the information security of services essential to society and to increase the authorities' opportunities to help in improving information security.[3] The legislative proposal aimed at setting out obligations for providers of essential services and certain digital services (for example online marketplaces, cloud computing services, online search engines) to manage risks posed to information security and report on security incidents to the supervision authority. However, Finland has opted for a sectoral approach and merely amended the sector-based legislation instead of passing a new law as the necessary changes were made to existing sector specific acts. Altogether twelve Finnish acts were modified: Information Society Act,[4] Aviation Act,[5] Railway Act,[6] Vessel Traffic Service Act,[7] Act for Security Measures on certain Ships and in Ports serving them and on monitoring the Security Measures (Port Security Act),[8] Transport Services Act,[9] Electricity Market Act,[10] Natural Gas Market Act,[11] Act on the Electricity and Natural Gas Market Supervision,[12] Water Services

[1] Available at https://www.difesaesicurezza.com/en/cyber-en/not-all-the-eu-member-states-are-compliant-with-the-nis-directive-right-now/ (accessed on March 17th, 2021)

[2] Verkko- ja tietoturvadirektiivi Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti - 9/2017.

[3] https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f8057a85c (accessed on March 17th, 2021)

[4] Laki sähköisen viestinnän palveluista / Lag om tjänster inom elektronisk kommunikation (917/2014) 07/11/2014, viimeksi muutettuna / ändring senast genom (281/2018) 04/05/2018

[5] Ilmailulaki / Luftfartslag (864/2014) 07/11/2014, viimeksi muutettuna / ändring senast genom (282/2018) 04/05/2018

[6] Rautatielaki / Järnvägslag (304/2011) 08/04/2011, viimeksi muutettuna / ändring senast genom (283/2018)-04/05/2018

[7] Alusliikennepalvelulaki / Lag om fartygstrafikservice (623/2005) 05/08/2005, viimeksi muutettuna / ändring senast genom (284/2018) 04/05/2018

[8] Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta / Lag om sjöfartsskydd på vissa fartyg och i hamnar som betjänar dem och om tillsyn över skyddet (485/2004) 11/06/04, viimeksi muutettuna / ändring senast genom (285/2018) 04/05/2018

[9] Laki liikenteen palveluista / Lag om transportservice (320/2017) 24/05/2017, Lag om ändring av lagen om transportservice (286/2018) 04/05/2018

[10] Sähkömarkkinalaki / Elmarknadslag (588/2013) 09/08/2013, viimeksi muutettuna / ändring senast genom (287/2018) 04/05/2018

[11] Maakaasumarkkinalaki / Naturgasmarknadslag (587/2017) 25/08/2017, viimeksi muutettuna / ändring senast genom (288/2018) 04/05/2018

[12] Laki sähkö- ja maakaasumarkkinoiden valvonnasta / Lag om tillsyn över el- och naturgasmarknaden (590/2013) 09/08/2013, viimeksi muutettuna / ändring senast genom (289/2018) 04/05/2018

Act.[1] The official government proposal was accepted in the parliament on April 10th, 2018 and the modifying laws came into force on May 1st, 2018.[2] For the banking,[3] financial market infrastructures[4] and healthcare[5] sectors NIS Directive's requirements were provided by legislative Acts already in place. Competent Authority requirements were introduced amending the Financial Supervisory Authority Act[6] and the Act amending section 6 of the Act on the Licensing and Supervision Agency for the Social and Health Sector.[7]

In France, the NIS Directive was implemented through Act n° 2018-133 of February 26th, 2018, relating to implementation of EU provisions in the field of security, which came into effect on February 27th, 2018.[8] However, certain provisions of the NIS Directive were further specified in French Decree n° 2018-384 of May 23rd, 2018, on the networks and information systems security of essential and digital services providers.[9] This entered into force on May 25th, 2018. By choosing an ambitious transposition, France has established a list of sectors for essential services, following consultations by ANSSI with public and private stakeholders and its European partners. This list refers to many sectors including banking, logistics or catering.

Law n° 4577/2018 transposing the NIS Directive in Greece was adopted on December 3rd, 2018. The Act was submitted to the Greek Parliament on November 12th, 2018 and voted nine days later. Provisions of the NIS Directive were adopted with the exact wording used in the Directive. Also, a Ministerial Decree n° 1027/2019 was published on October 4th, 2019, relating issues of implementation and procedures of (transposition) law 4577/2018. The purpose of the Decree was to issue the basic security requirements for network and information systems, the process of providing information and notification of security incidents to the competent authorities, the methodology for identifying OES and the methodology for DSPs evaluation and control, according to the provisions of the Implementing Regulation (EU) 2018/151.[10]

Ireland opted for the implementation of the NIS Directive by way of Statutory Instrument No. 360 of 2018, "*European Union (Measures for a High Common Level of Security of Network and Information Systems)*

[1] Vesihuoltolaki / Lag om vattentjänster (119/2001) 09/02/2001, viimeksi muutettuna / ändring senast genom (290/2018) 04/05/2018

[2] Available at https://valtioneuvosto.fi/hanke?tunnus=LVM037:00/2016 (accessed on March 17th, 2021)

[3] Luottolaitostoiminnasta annetun lain (610/2014)

[4] Laki kaupankäynnistä rahoitusvälineillä (1070/2017)

[5] Suomessa terveydenhuoltolakia (1326/2010)

[6] Laki kaupankäynnistä rahoitusvälineillä (1070/2017) 28/12/2017; Laki luottolaitostoiminnasta (610/2014) 08/08/2014, viimeksi muutettuna (1073/2017) 28/12/2017

[7] Laki Sosiaali- ja terveysalan lupa- ja valvontavirastosta annetun lain 6 §:n muuttamisesta (669/2008)-28/12/2017.

[8] Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, JORF n°0048

[9] Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, JORF n°0118

[10] OJ L 26, 31.1.2018,

Regulations 2018"[1], which were signed by then-Minister of Communications, Climate Action and Environment, Denis Naughten, TD, on 18 September 2018. In the Republic of Ireland, the term *statutory instrument* is given a much broader meaning than under the UK legislation. Under the Statutory Instruments Act 1947[2] a statutory instrument is defined as being "*an order, regulation, rule, scheme or bye-law made in exercise of a power conferred by statute*". Contrary to the other five Member States of the EU of this study, statutory instruments are not enacted in Ireland by the National Parliament (Oireachtas) but allow persons or bodies to whom legislative power has been delegated by statute to legislate in relation to detailed day-to-day matters arising from the operation of the relevant primary legislation. Statutory instruments are used, for example, to implement European Council Directives, designate the days on which particular District Courts sit and delegate the powers of Ministers. Therefore, there is no possibility of retracing the legislative process on the adoption of the statutory instrument related to NIS Directive implementation. However, it is worth mentioning that the Irish Department of Communications, Climate Action & Environment published a consultation paper on the proposed approach to take on the NIS Directive in November 2017, with the deadline for submissions having closed on December 20th, 2017.[3]

After a bill (n°7314) had been filed on June 6th, 2018, with the Luxembourg Parliament, in May 28th, 2019, the Grand Duchy of Luxembourg transposed the NIS Directive (UE) 2016/1148 into national law and entered in force on July 1st, 2019.[4] A point of interest of the law of May 28th, 2019 is the choice made by the legislator to designate competent authorities in matters of network security and information systems which are different according to the sector concerned: the Financial Sector Supervisory Commission (CSSF)[5] is responsible for the financial sector (including digital service providers to this sector), while the Luxembourg regulatory institute (ILR)[6] will deal with other sectors. An interesting specialisation, which was not duplicated however in the field of data protection for example. This division of competences can be seen through the two national regulations,

[1] S.I. No. 360/2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018

[2] Statutory Instruments Act, 1947, Number 44 of 1947

[3] Department of the Environment, Climate and Communications, 'Department of the Environment, Climate and Communications', November 2017

[4] Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, JO A-N°372 31.5.2019

[5] Available at https://www.cssf.lu/en/ (accessed on March 18th, 2021)

[6] Available at https://web.ilr.lu/FR/ILR (accessed on March 18th, 2021)

CSSF n° 20-04[1] and ILR/N19/1,[2] both adopted in 2020 and relating to the definition of essential services. Infringement proceeding initiated by the Commission[3] against Luxembourg was closed on March 7th, 2021.[4]

The process of implementing Directive (EU) 2016/1148 in Poland was initiated with the Act of July 5th, 2018, on national cybersecurity systems into the Polish legal order.[5] As the NIS Directive is a minimum harmonisation, the Polish legislator has also included the public administration and the telecommunications sector in the scope of the law. The law entering in force on August 28th, 2018, the transposition was not realised in due time which forced the Commission once again to initiate an infringement proceeding.[6] Furthermore, a Regulation listing essential services and defining thresholds on significant disruptive effect was adopted on September 11th, 2018 by the Council Ministers of Poland (Government of Poland).[7] A regulation relating thresholds definition for considering an incident as serious was also adopted one month later by Polish Council of Ministers.[8] The Regulation supplements the law on the National Cybersecurity System Act (NCSA) of July 5th, 2018, and considers serious incidents which operators of essential services are required to report. The regulation indicates thresholds for different sectors and sub-sectors of the economy and provides a relevant table of classification. Entered in force on November 21st, 2018, the NIS Directive was thus fully implemented since that date. The infringement proceeding was therefore closed by the Commission a few months later along with Greece and Luxembourg.[9]

B. Minimum Harmonisation Provisions: Cross-Case Analysis of the Transposition

In these six cases, NIS Directive's provisions were either fully transposed in due time or fully transposed after being formaly noticed according to Art. 258 TFEU proceeding by the Commission. Therefore, I consider all mandatory provisions as transposed. Voluntary provisions are considered as cases of discretion-passed-on. While voluntary provisions that address Member States (e.g., *Member States may do …*) are considered as not

[1] CSSF Règlement N° 20-04 du 15 juillet 2020 relatif à la définition des services essentiels selon la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne, JO A-N°621 16.7.2020

[2] Institut Luxembourgeois de Régulation - Règlement ILR/N19/1 du 5 novembre 2019 portant sur la fixation des services essentiels - Service NISS, JO A-N°768 11.11.2019

[3] Available at https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4486 (accessed on March 17th, 2021)

[4] Available at https://ec.europa.eu/commission/presscorner/detail/EN/MEMO_19_1472 (accessed on March 18th, 2021)

[5] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

[6] Available at https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4486 (accessed on March 17th, 2021)

[7] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Dz.U. 2018 poz. 1806

[8] Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny, Dz.U. 2018 poz. 2180

[9] Available at https://ec.europa.eu/commission/presscorner/detail/EN/MEMO_19_1472 (accessed on March 18th, 2021)

transposed. From mandatory provisions will be only considered minimum harmonisation provisions, where a certain regulatory flexibility is given (**Table 26**).

NIS Directive's Provisions of Minimum Harmonisation					
Art.5 §1	Art. 6 §1	Art. 8 §3	Art. 9 §1	Art. 14 §1	Art. 14 §5 Al. 2
Art. 5 §2	Art. 6 §2	Art. 8 §4	Art. 9 §2	Art. 14 §2	Art. 14 §5 Al. 3
Art. 5 §3	Art. 7 §1	Art. 8 §5 al. 1	Art. 9 §3	Art. 14 §3	Art. 14 §5 Al. 4
Art. 5 §4	Art. 8 §1	Art. 8 §5 al. 2	Art. 10 §2	Art. 14 §4	Art. 15 §2
Art. 5 §5	Art. 8 §2	Art. 8 §6	Art. 10 §3 Al. 1	Art. 14 §5 Al. 1	Art. 15 §4

Table 26: *NIS Directive's Provisions of Minimum Harmonisation*

(Table made by author)

A comparative analysis will be conducted for the following provisions of the NIS Directive: national strategy criteria (**i**), NIS governance framework's identification (**ii**), CSIRT tasks (**iii**), identification criteria for OES (**iv**), appropriate and proportionate security requirements for OES (**v**), OES notification obligations (**vi**) and penalties (**vii**).

1. National Strategy Criteria (Art. 7)

The NIS Directive requires each Member State to draw up a national strategy defining the framework, vision, objectives and priorities for network and information security at national level.

The Finnish Information Security Strategy adopted by the Minister of Transport and Communications in March 2016[1] has emphasised that the starting point in accordance with the Finnish legal order can be considered to be that the framework, objectives and priorities for network and information security are defined primarily in the legislation in force. The strategy sets out objectives to ensure the quality of legislation to the extent that legislation can have an impact on network and information security and, in a way, on the development of the growth environment of digital business. The implementation of the strategy's measures is addressed to responsible authorities or other entities in the strategy. The division of responsibilities is based on existing legislation on the powers of the authorities. The strategy puts thus into practice Article 7 of the NIS Directive.

France adopted a national digital security strategy in 2010, revised in 2015 in a participatory and interdepartmental approach across all administrations, which meets the aspirations and objectives of article 7 of the directive. The document defines five strategic axes : Fundamental interests, defence and security of state

[1] The Finnish Ministry of Transports and Communications, 'Information Security Strategy for Finland The World's Most Trusted Digital Business Environment', September 2016

information systems and critical infrastructures, major IT crisis; Digital trust, privacy, personal data, cyber-surveillance; Awareness, initial training, continuing training; Environment of digital companies, industrial policy, export, internationalisation; and Europe, digital sovereignty, cyberspace stability. The French national cybersecurity authority, the "*Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)*"[1] has been designated as responsible for developing the national strategy provided for in article 7 of the directive on the security of networks and information systems, in line with the national strategy for digital security which was adopted in 2015. However, nowhere in the Law of 2018-133 can a definition of a National Strategy for NIS be found. The content thus of French cybersecurity strategy is defined outside the limit of the law for NIS matters.

Greek law n° 4577/2018[2] of November 21st, 2018, which transposed the NIS Directive provisions, made by publishing a national strategy of network and information systems, a legal obligation of the Greek state (Article 6). An obligation which goes much further from what is requested from Article 7 of the NIS Directive as only a National Strategy on the Security of NIS was asked. However, as stated by the European Commission in the Annexed document to its Communication on "*Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union*"[3], the national strategy for the security of networks and information systems can be considered as equivalent to a national strategy for cybersecurity. Article 6, para. 1 of Greek law n° 4577/2018 mentions that "*The National Cybersecurity Authority updates the 'National Cyber Security Strategy' approved by Ministerial Decision 3218/2018 of the Minister of Digital Policy, Telecommunications and Information (…)*". It is important to mention that contrary to Finland and France, Greece had no National Cybersecurity Strategy. It is only on March 7th, 2018, that Greece implemented its first cybersecurity strategy. It was thus important to adopt a National Cybersecurity Strategy before proceeding to NIS Directive transposition. The 2018 National Cybersecurity Strategy stated that "*[the National Strategy] is also harmonised with the requirements of relevant EU regulations and directives (in particular with Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6th, 2016, concerning measures for a common high level of security of network and information systems across the Union – NIS Directive)*". The competent Minister approved the new Cybersecurity Strategy of Greece for the period 2020-2025 by mentioning Article 6 of Greek law n° 4577/2018 in its consideration.

As it was the case for Greece, Ireland has also integrated the National Strategy requirement in its national legal order (Part 3, Regulation 11 of the S.I. No. 360/2018) using the same wording of Article 7 of the NIS Directive. However, the term of *National Strategy on the security of NIS* was not replaced with the term *National*

[1] Available at https://www.ssi.gouv.fr/en/mission/what-we-do/ (accessed on March 7th, 2021)

[2] Available at https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=81773968-f2b7-4b3b-83bd-a99600cc1d29 (accessed on March 19th, 2021)

[3] European Commission, Annex to the Communication on 'Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', 13 September 2017, COM(2017) 476 final/2, 5

Cybersecurity Strategy, as it was the case for Greece. Which is of importance, as Ireland has not published, since then, any kind of National Strategy on the security of NIS. The Government of Ireland states in its Cybersecurity Strategy 2019-2024 that the "*2015 strategy was written in anticipation of the NIS Directive (…)*", while it makes among others its "*Critical National Infrastructure Protection system flowing from the NIS Directive*" a part of this new Strategy.[1]

In Luxembourg, the Law of May 28th, 2019, transposing Directive (EU) 2016/1148,[2] introduced the provisions related to the National Strategy on security of NIS requirement, by modifying the law of July 23rd, 2016 establishing a High Commission for National Protection. In the NIS Directive provisions we find commentary from the Government to the House of Representatives of the Grand-Duchy of Luxembourg, following the deposit of the bill on June 6th, 2018;

> "*Given that this national strategy for the security of networks and information systems can be considered as equivalent to a national strategy for cybersecurity[3] and that Luxembourg already has such a national strategy for cybersecurity drawn up by an inter-ministerial committee chaired by the High Commission for National Protection (HCPN), the new law strengthens this role of coordinator by giving it a legal basis in the HCPN law*".

It should be noted that the third version of the National Cybersecurity Strategy saw the light of day in 2018.

Poland followed the same practice as Greece by transposing Article 7 of the NIS Directive with the same wording in Chapter 9, Article 56 of the National Cybersecurity System Act (NCSA) of 5 July 5th, 2018.[4] The term of Cybersecurity Strategy was privileged and had to be adopted by the Council of Ministers (Government of Poland). The Minister of Digital Affairs becomes responsible for preparing and monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland, the implementation of action plans for its implementation and the conduct of information policy on the national cybersecurity system. In April 2017, resolution No. 52/2017 of the Council of Ministers adopted a strategy paper on cybersecurity in the form of the National Cybersecurity Policy Framework of the Republic of Poland for the period 2017-2022.[5] One of the main tasks identified in the National Cybersecurity Policy Framework is to achieve a high level of resilience of

[1] Government of Ireland, 'National Cyber Security Strategy 2019-2024'

[2] Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, JO A-N°372 31.5.2019

[3] European Commission, Annex to the Communication on 'Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', 13 September 2017, COM(2017) 476 final/2, 5

[4] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

[5] Ministerstwo Cyfryzacji, 'Strategia Cyberbezpieczenstwa Rzeczypospolitej Polskiej Na Lata 2017–2022', 2017

national ICT systems for the provision of essential services, digital services and public administration services. Furthermore, the aim of the Strategy was to develop the national cybersecurity system in such a way as to be geared towards building capabilities for day-to-day threat monitoring and national cybersecurity management. Therefore, the Strategy was in line with the content in Article 7 of the NIS Directive (**Appendix 7**: NCSS Analysis).

Member States	Article 7 Compliance
Finland	Yes
France	Yes
Greece	Yes
Ireland	Yes
Luxembourg	Yes
Poland	Yes

Table 27: *Article 7 Compliance*

(Table made by author)

2. NIS Governance Framework's Identification

Articles 8 and 9 of the NIS Directive lay down obligations for all Member States to designate national competent authorities, single points of contact, and CSIRTs with tasks related to the security of network and information systems. They also ask from Member States to ensure that the competent authorities, the CSIRTs and the single points of contact have adequate resources to carry out, "*in an effective and efficient manner*", the tasks assigned to them.

Under the 2017 Finnish government proposal on amending the laws related to the implementation of the NIS Directive, sector specific authorities received competence for the supervision of: The Energy Authority, the Financial Supervisory Authority, the National Supervisory Authority for Welfare and Health, the Finnish Transport Safety Agency, the Centre for Economic Development, Transport and the Environment and the National Cyber Security Centre (NCSC) of the Finnish Communications Regulatory Authority (FICORA) (Table).[1] The NCSC acts as a designated single point of contact and national CSIRT (**Table 27**).

[1] FICORA, the Finnish Transport Safety Agency (Trafi), and certain functions of the Finnish Transport Agency were merged to form the new Finnish Transport and Communications Agency (TRAFICOM) on January 1st, 2019.

Sector	Competent Authority
Transport	Traficom
Energy supply	The Energy Authority
Healthcare	Valvira
Financial sector	The Financial Supervisory Authority
Financial market infrastructure	The Financial Supervisory Authority
Water supply	ELY Centres
Digital infrastructure	Traficom
Digital services	Traficom

Table 28: *Finland's essential sectors and corresponding national competent authority*

(Table made by author)

France adopted the route of a centralised approach designating the French National Agency for the Security of Information Systems (ANSSI) as the competent national authority for OES or DSP's. ANSSI also became the national Single Point of Contact. In doing so, Decree n° 2009-834 of July 7th, 2009,[1] on ANSSI's missions has been amended by Decree n° 2018-1136 of December 13th, 2018,[2] to extend its scope. Among ANSSI's missions there is: carrying out inspections of the information systems of public or private operators; implementing monitoring devices for detecting events likely to affect the security of the information systems of public and private operators; collecting technical information relating to incidents; and coordinating the reaction to these events. Since 2015 Decree n° 2009-834 also states that "*ANSSI has the means necessary for the accomplishment of its missions*". The CERT-FR (ANSSI) is designated as a French CSIRT meeting the requirements set out in Article 9 of the directive, while Decree No. 2009-834 relating to ANSSI describes the role of the CSIRT.

Greek law n° 4577/2018 implemented NIS Directive provisions on governance framework using the same wording. According to article 7 of the Greek law, the Cybersecurity Directorate of the General Secretariat for Digital Policy of the Ministry of Digital Policy, Telecommunications, and Information is considered as the National Competent Authority for the security of NIS. While article 8 of the same law designates the Cyber Defence Directorate of the General Staff of National Defence as CSIRT, which covers the areas and services defined by the NIS Directive.

[1] Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », JORF n°0156

[2] Décret n° 2018-1136 du 13 décembre 2018 pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques, JORF n°0289

Contrary to France and Greece, Ireland designated the National Cyber Security Centre (NCSC), Department of Communications, Climate Action & Environment, as the national Single Point of Contact (Part 2, Regulation 9 of the S.I. 360-2018) as the national competent authority for DSPs (Part 2, Regulation 8 of the S.I. 360-2018) and for OES in the following essential sectors: Energy, Transport, Health, Drinking water supply and distribution, Digital infrastructure (Part 2, Regulation 7 (1) of the S.I. 360-2018). While the Central Bank of Ireland was designated as competent authority for banking and financial market infrastructure (Part 2, Regulation 7(2) of the S.I. 360-2018). Lastly, the unit of the Department of Communications, Climate Action and Environment became the national CSIRT (Part 2, Regulation 10 of the S.I. 360-2018).

Luxembourg opted for the same approach with Ireland. The Financial Sector Supervisory Commission,[1] became the competent authority for the security of NIS covering the sectors of banking and financial market infrastructures (Art. 3, para. 1 of the Law of May 28th, 2019), as well as the digital services provided by an entity falling under the supervision of the CSSF. While the Luxembourg Regulatory Institute,[2] is the competent authority in matters of NIS security covering the remaining essential sectors, as well as the digital services provided by an entity for which the CSSF is not the competent authority (Art. 3, para. 2 of the Law of May 28th, 2019), ILR is the single national point of contact for network and information system security (Art. 4 of the Law of May 28th, 2019). By way of Grand-Ducal decree,[3] GovCERT has been mandated to act as the official national point of contact for national and international governmental CERTs. [4] It performs this function under the name of NCERT.LU (National CERT). Since NCERT.LU is operated by the governmental CERT, the policies used at NCERT.LU are the same that are used by GovCERT.

Poland followed the same sectoral approach as Finland, thus article 41 of the NCSA states that the competent authorities shall be "*(1) for the energy sector, the Ministry of State Assets, Department of Security and Crisis Management; (2) for the transport sector, excluding the water transport subsector, the Ministry of Infrastructure; (3) for the water transport subsector, the Ministry of Marine Economy and Inland Navigation; (4) for the banking sector and financial market infrastructure, the Polish Financial Supervision Authority; (5) for the health sector,[5] Ministry of Health; (6) for the drinking water supply and distribution sector, the Ministry*

[1] Commission de surveillance du secteur financier

[2] Institut luxembourgeois de régulation

[3] Arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental », JO A-N°424 29.5.2018

[4] GovCert was already established by a Decree of the Grand-Ducal on July 30th, 2013. Available at http://legilux.public.lu/eli/etat/leg/agd/2013/07/30/n2/jo (accessed on March 20th, 2021).

[5] Ministry of National Defence of the Republic of Poland, Department of Science and Military Education, Development and Cybersecurity Unit only for specific entities referred to in Article 26 item 5 of the Act of 5 July 2018 on the national cyber security system.

of Marine Economy and Inland Navigation; (7) for digital infrastructure,[1] *the Ministry of Digital Affairs, Department of Cybersecurity*", while the competent authority for DSPs[2] shall be the Ministry of Digital Affairs, Department of cybersecurity (Art. 41 item 1 (10) of the NCSA). The Ministry of Digital Affairs, Department of cybersecurity is also designated as Single Contact Point (Art. 48 of the Act of 5 July 2018). Finally, Article 4 of Act of 5 July 2018 also includes three CSIRTs within the cybersecurity system of Poland: (1) CSIRT NASK (led by Research and Academic Computer Network – National Research Institute); (2) CSIRT MON (led by the Minister of National Defence); and (3) CSIRT GOV (led by the Head of the Internal Security Agency) (**Appendix 8**:).

Member States	Article 8 Compliance	Article9§1 Compliance
Finland	Yes	Yes
France	Yes	Yes
Greece	Yes	Yes
Ireland	Yes	Yes
Luxembourg	Yes	Yes
Poland	Yes	Yes

Table 29: *Articles 8 and 9§1 Compliance*

(Table made by author)

3. CSIRT tasks (Art. 9§2)

In accordance with Article 9 of the NIS Directive, the tasks of the Finnish CSIRT are included in the statutory tasks of FICORA (now became TRAFICOM) under the Information Society Act (917/2014).[3] Following section 304§ of the Information Society Act, the tasks of FICORA seem to meet the CSIRT tasks provisions of the NIS Directive. The Act of May 4th, 2018,[4] amending the Information Society Act in accordance with the decision of

[1] Ministry of National Defence of the Republic of Poland, Department of Science and Military Education, Development and Cybersecurity Unit only for specific entities referred to in Article 26 item 5 of the Act of 5 July 2018 on the national cyber security system.

[2] Ministry of National Defence of the Republic of Poland, Department of Science and Military Education, Development and Cybersecurity Unit only for specific entities referred to in Article 26 item 5 of the Act of 5 July 2018 on the national cyber security system.

[3] Laki sähköisen viestinnän palveluista (917/2014) 07/11/2014, viimeksi muutettuna (281/2018) 04/05/2018

[4] Laki tietoyhteiskuntakaaren muuttamisesta (281/2018) 04/05/2018

Parliament,[1] furthermore incorporated the collection of information on NIS security breaches and threats to the network services, communication services, value-added services and information systems, as well as on failures and disruptions of NIS. National CSIRT also establishes cooperation relationships with the private sector. Therefore, modified section 308§ of the of the Information Society Act (917/2014) calls the Ministry of Transport and Communications, FICORA, the Data Protection Commissioner, competition authorities and consumer authorities to co-operate. Furthermore, FICORA shall, where appropriate, co-operate with the supervisory authority responsible for FICORA of a State belonging to the European Economic Area or a State party to the Council of Europe Television Convention.

The designated French CSIRT, CERT-FR (ANSSI), meets the requirements set out in Article 9 of the directive. Under modified Decree No. 2009-834 of May 23rd, 2018[2] the ANSSI (and so on the CERT-FR) implements a system for detecting events likely to affect the security of State information systems and coordinates the reaction to these events; collects technical information relating to incidents affecting the information systems of the State and of public or private operators; and can provide assistance in response to these incidents; participates in international negotiations and liaises with its foreign counterparts. It is worth noting that there is no mention of CERT-FR neither in Law 2018-133 nor in Decree No. 2009-834.

The Grand-Ducal decree of May 9th, 2018,[3] which modifies the Grand-Ducal decree of July 30th, 2013,[4] attributes the following to GovCERT: the responsibilities of providing a service for monitoring, detecting, alerting and responding to computer attacks on NIS; operating a specialised response team capable of supporting the prevention and response to large-scale security incidents; maintaining a centralised inventory of incidents affecting the security of these systems; ensuring a permanent availability 24 hours a day, 7 days a week in order to react effectively in a crisis situation; facilitating by all means, within a national and international framework, the collaboration of the various governmental and private entities related to the security of information systems; representing Luxembourg in international meetings with regard to its field of competence; acting as a national computer emergency treatment centre (National CERT) and as a military centre for processing computer emergencies (Military CERT). Obligations which meet Article 9 provisions of the NIS Directive. In his role as National CERT, it operates within the confines imposed by Luxembourg's legislation.

[1] Eduskunnan vastaus EV 25/2018 vp, Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta, HE 192/2017 vp

[2] Décret n° 2018-1136 du 13 décembre 2018 pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques, JORF n°0289

[3] Arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental », JO A-N°424 29.5.2018

[4] Arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé «Computer Emergency Response Team Gouvernemental», JO A-N°161 6.9.2013

Following Article 8, para. 2 of Greek Law n° 4577/2018, the Cyber Defence Directorat of the General Staff of National Defence meets all requirements required by Article 9 of the NIS Directive, as the provision and Annex I were *copy-pasted* with the same wording. Therefore, there is no need to explicitly note the provisions of Greek transposition law. Ireland[1] and Poland[2] also adopted the same approach as Greece.

The clause of Article 9 of the NIS Directive, relating on adequate resources for ensuring business continuity (e.g., appropriate managing and routing system equipment or adequate staff and infrastructure for ensuring availability at all times), was not sufficiently dealt with in this part of the study. Contrary to Greece, Ireland and Poland created a legal obligation of this requirement by using the same wording of the NIS Directive, whereas Finland and Luxembourg mentioned "*permanent availability 24 hours a day*". Meanwhile, France via modified Decree No. 2009-834 of May 23rd, 2018, does not make such a reference. It is therefore almost impossible and irrelevant to assess France's compliance to such provisions in the present thesis. However, bearing in mind the structure and the importance of ANSSI in France, it is clear that France perfectly complies with this requirement without having to specify it legislatively or through government act. (**Appendix 9:** CSIRTs by Country).

Member States	Article 9§2 Compliance
Finland	Yes
France	Yes
Greece	Yes
Ireland	Yes
Luxembourg	Yes
Poland	Yes

Table 30: *Article 9§2 Compliance*

(Table made by author)

4. OES Identification Criteria (art. 5 and 6)

According to the Commission's report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of NIS Directive, it is mentioned that Finland, Greece, Ireland, Luxembourg and Poland have delivered all information requesting the list of essential services, the number of OES identified for each sector and an indication of their importance in

[1] Part 2, item 10 of the S.I. 360-2018.

[2] Chapter 6 of the Act of 5 July 2018 on the National Cybersecurity System.

relation to that sector; and thresholds (Article 5, para 7 of the NIS Directive). France has only communicated the list of essential services and the Number of OES. But this does not affect the compliance of France upon NIS Directive provisions.

According to Finnish Government's proposal to Parliament on implementing NIS Directive, it is specified that "*the legislation in force does not contain any actual procedures for directly identifying key service providers under the Network and Information Security Directive*". Therefore, the cross-governmental working group established by the Finnish Ministry of Transport and Communications on October 2016, to support the national implementation of the NIS Directive in the country, proposed in its final report that OES falling within the scope of the Directive should be defined at the level of the law. Amending Acts have been analysed and a summarised list of the type of entities identified may be found in the Annex of the present study (**Appendix 10**: Identified essential services by Finland). Thresholds for determining the significance of a disruptive effect have not been however explicitly defined by any amending act, as the sectoral competent authority may be defined through regulatory instruments. The Commission retains an on-time delivery of list of services, number of OES and thresholds in its report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services (COM/2019/546 final). It is possible to consider that Article 6 was correctly implemented and that a non-public document may exist.

In France, Article 5 of Law 2018-133 states that "*the list of the essential services shall be provided by a decree in Council of State*"[1]. Decree n°2018-384 adopted on May 23rd, 2018, relating on the security of the NIS for the OES and DSPs, mentions indeed in Article 2 that

> "*[OES] are designated operators providing at least one service mentioned in the appendix to this decree, when networks and information systems are necessary for the provision of this service and an incident affecting these networks and systems would have serious consequences on the provision of this service, assessed with regard to the following criteria:*
>
> *1° the number of users relying on the service provided by the entity concerned*
>
> *2° the dependency of other sectors referred to in Annex II on the service provided by that entity*
>
> *3° the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety*
>
> *4° the market share of that entity*
>
> *5° the geographic spread with regard to the area that could be affected by an incident*

[1] State Council.

6° the importance of the entity for maintaining a sufficient level of the service, considering; the availability of alternative means for the provision of that service.

7 ° where applicable, sectoral factors".

A definition which coincides exactly with Articles 5 and 6 provisions of the NIS Directive. In the annexe of Decree n°2018-384 the following sectors are identified as essential services: (i) Civil activities of the State, (ii) Judicial activities, (iii) Military activities of the State, (iv) Food, (v) Electronic, audio-visual and information communications, (vi) Energy, (vii) Space and research, (viii) Finance, (ix) Water management, (x) Industry, (xi) Health, and (xii) Transport (**Appendix 11**: Identified essential services by France). As it was the case in Finland, the thresholds related to the disruptive effect does not however figure in any legislative act in France. Article 3 of Decree n°2018-384 states that

"*the [OES] are appointed by decree of the Prime Minister. This decree mentions the services essential to the functioning of society or the economy provided by the operator. The Prime Minister notifies each operator concerned of his intention to designate him as operator of essential services. The operator has a period of one month from this notification to present his observations. When the operator whose designation is envisaged provides an essential service in one or more other Member States of the European Union, its designation is preceded by prior consultation of the Member States concerned*".

For an operator to be considered as an OES in Greece it must meet the criteria provided in Art. 4, para. 2 of Law 4577/2018, which corresponds exactly to Article 5, para. 2 of the NIS Directive. A table with same sectors, sub-sectors and type of entities figures at the end of Greek law 4577/2018. There is so no need to replicate here Annex II table. In addition, Article 5 of the same law on the *significant disruptive effect* reproduces the same content as article 6 of the NIS Directive and provides that "*The National Cybersecurity Authority,*[1] *in cooperation with the competent regulatory or supervisory authorities and other national bodies involved in each essential service sector, shall determine the criteria for determining an incident as a serious disturbance*". Consequently, in 2019 Ministerial Decision n° 1027/4 October 2019 on the implementation measures of Law 4577/2018 was issued. This Decision defines further criteria on the significant disruptive effect. Thereafter ,any event is considered a serious disruption, which:

"*especially meets at least one of the following conditions: a) the continuity*[2] *of the service provided by the institution is affected for more than 100,000 user hours. b) affects the population*

[1] Which belongs to the Greek Ministry on Digital Governance.

[2] Continuity of service defines the ability to provide the service at acceptable levels of confidentiality, integrity, availability and authenticity.

at least 50.000 users; c) threat to human life;[1] *or causes material damage to the body itself or to other bodies in excess of 1,000,000 euros*" (Art. 7 of the Ministerial Decision n° 1027).

Furthermore, this Decision states the methodology and criteria for determining the OES in Article 16: "*in order to meet the conditions and to be designated as OES, an entity must belong to a sector or sub-sector of Law 4577/2018, offer a basic service based on Annex 1 of the same law, the service provision must be based on network and information systems and meet at least one of the following [sectoral] criteria in this article*". Contrary to Finland and France, Greece has made thus the choice of publishing the thresholds officially in a governmental act (**Appendix 12**: Identified essential services by Greece).

Ireland's behaviour upon implementation of OES designation provision of the NIS Directive remains the same as Greece. The competent authority shall designate an entity as an OES which satisfies the criteria defined by Article 5 of the NIS Directive (Part 4, Regulation 12, para. 1 of the S.I. 360/2018). Irish transposition law incorporates by using the exact wording of the rest of the provisions of Article 5 and the content of Annex II of NIS Directive. The only additions concern the Credit Institution sub sector where the following type of entities are specified : Payment Services provided to non-Monetary Financial Institutions in the State, Cash Services provided in the State Access to retail payment systems provided to credit institutions in the State. The remaining elements are the same, thus there is no need to replicate Annex II table here.

Significant disruptive effect, Part 4, Regulation 12 (5) of the Statutory Instrument 360/2018 reproduces the content of Article 6 of the NIS Directive in the same wording. However, Ireland does not publicly provide, contrary to Greece, any indication of the thresholds retained upon designation of OES.

"*In determining the significance of a disruptive effect referred to in paragraph (1) (f) insofar as it relates to the provision by a person of an essential service in the State, a competent authority shall, where it considers it appropriate to do so, take into account factors specific to the sector to which the person providing the service belongs and, in every case, shall take into account the following: (a) the number of users relying on the service provided by the person; (b) the extent to which other sectors set out in Schedule 1 depend on the service provided by the person; (c) the impact that an incident could have in terms of degree and duration on economic or societal activities or public safety; (d) the market share of the service provided by the person; (e) the geographic spread with regard to the area that may be affected by an incident; (f) the importance of the person in the maintenance of a sufficient level of the service in the State taking into account the availability of alternative means for the provision of the service concerned*".

Contrary to Article 5 of NIS Directive, the S.I. 360/2018 provides however a detailed legal procedure for OES designation (Part 4, Regulation 13) and for adding (cancelling) new (designated) sectors and subsector or essential service (Part 4, Regulation 14 and 15). It is also interesting to mention that article 5, para. 3 of the

[1] In case of loss of human life, the incident is automatically notified.

NIS Directive asks from each Member State to establish a list of OES. Ireland has gone deeper by creating a national Register of OES (Part 4, Regulation 16). "*A competent authority shall establish and maintain an [Operators Register] containing particulars of operators of essential services in each sector in respect of which the competent authority is designated as the competent authority*" (para. 1). The Operators Register shall contain particulars of the person, and the category of sector and, as appropriate, subsector and the essential service in respect of which the person is an operator of essential services (para. 2). This register shall be reviewed on a regular basis and, in any event, not less than once every two years from 9 May 2018 (para. 3).

As it was mentioned in the NIS Governance Framework's Designation, the Financial Sector Commission of Supervision (CSSF in French) is the competent authority in Luxembourg for the security of NIS covering the sectors of banking and financial market infrastructures (Art. 3, para. 1 of the Law of May 28th, 2019), while the Luxembourg Regulatory Institute is the competent authority for remaining essential sectors, as well as the digital services provided by an entity for which the CSSF is not the competent authority (Art. 3, para. 2 of the Law of May 28th, 2019). The same scheme is thus reproduced for the designation of OES. In accordance with the sectors and its sub-sectors listed in the annex of NIS law, the Institute establishes thus a list of essential services based on the description of the types of entities that are described by the different laws specific to each sector by regulation ILR / N19 / 1 of November 5th, 2019[1] establishing essential services. Amongst the responsibilities of the CSSF are the designation of essential services by means of regulation and the subsequent identification of OES. The CSSF has duly listed the essential services in CSSF Regulation n° 20-04.[2] The Law of May 28th, 2019, transposing the NIS Directive in Luxembourg,[3] states in its Article 7, para. 3 that

> "*(3) The extent of the disruptive effect referred to in paragraph 2, point 3, is determined on the basis of cross-sectoral and sectoral factors, including at least: 1° the number of users relying on the service provided by the entity concerned; 2 ° the dependency of other sectors referred to in Annex II on the service provided by that entity; 3° the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; 4° the market share of that entity; 5° the geographical spread with regard to the area that could be affected by an incident; 6° the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service*".

[1] Institut Luxembourgeois de Régulation - Règlement ILR/N19/1 du 5 novembre 2019 portant sur la fixation des services essentiels - Service NISS, JO A-N°768 11.11.2019

[2] CSSF Règlement N° 20-04 du 15 juillet 2020 relatif à la définition des services essentiels selon la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne, JO A-N°621 16.7.2020

[3] Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, JO A-N°372 31.5.2019

As it was the case for Greece, the significant disruptive effect provided by Article 6 of the NIS Directive figures also within a legislative act in Luxembourg and in the same way, a regulation defines the thresholds upon which an incident shall be considered as having such an effect (**Appendix 13**: Identified essential services by Luxembourg).

In Poland, Chapter 2, Article 6 of the National Cybersecurity System Act (NCSA) of July 5th, 2018, provides that the Council of the Minister is the competent authority for determining a list of essential services, based on the annexed to this law table of sectors, subsectors and type of entities falling within the scope of the NCSA, the importance of the service for the maintenance of critical social or economic activity. Furthermore, the Council of the Minister is also responsible for determining regulation thresholds allowing to materialise the significant disrupt effect of an incident for services figuring on the lists of essential services. Criteria upon which thresholds should be determined match requirements defined by Article 6 of the NIS Directive. Therefore, it is a Regulation of the Council of Ministers of September 11th, 2018, which establishes the aforementioned thresholds. The table annexed to the present study merges data from the NCSA table with those of the table provided by this Regulation (**Appendix 14**: Identified essential services by Poland). It should be mentioned however that mostly sector-specific factors were retained by Poland.

Moreover, Chapter 8, Article 42 of the NCSA imposes several obligations upon the competent authority for each essential sector, which consist of examining the market to identify potential OES, to begin administrative proceedings and collect information for the identified entity, to check whether the entity complies with the requirements of the competent authority's regulation and to nominate the OES through an administrative decision. After that, the OES has 3 to 12 months to adapt to the requirements contained in the competent authority's regulation and to perform the obligations arising from the NCSA. The deadlines run from the moment of receiving the administrative decision recognising the entity as an OES. It is worth mentioning that Poland lays down detailed procedure about the constitution and amendment of its OES. In the same way as Ireland did but without mentioning any register. Finally, an obligation for the Ministry of Digital Affairs is stated to make available data from the list of OES to a restraint number of authorities and that, to the extent which is necessary to perform their statutory tasks (Chapter 2, Art. 7, para. 8 of the NCSA). Those authorities are the national competent authorities for cybersecurity; the Police; the military police; the Border Guard; the Central Anti-Corruption Bureau; the Internal Security Agency and the Foreign Intelligence Agency; the Military Counterintelligence Service and the Military Intelligence Service; Courts; the prosecutor's office; bodies of the National Tax Administration; the director of the Government Centre for Security; and the State Protection Service. It should be noted that identification of the OES has already given rise to appeals before the Provincial

Administrative Court in Warsaw (Wojewódzkiego Sądu Administracyjnego w Warszawie - VI SA / Wa 2666/19; [1] VI SA / Wa 2151/19; [2] and VI SA / Wa 2667/19[3]).

Member States	Article 5 Compliance	Article 6 Compliance
Finland	Yes	Yes
France	Yes	Yes
Greece	Yes	Yes
Ireland	Yes	Yes
Luxembourg	Yes	Yes
Poland	Yes	Yes

Table 31: *Article 5 and 6 Compliance*

(Table made by author)

5. Appropriate and Proportionate Security Requirements for OES (Art. 14, para. 1 and 2)

As it may be seen from the comparative table on sectoral Acts implementing the provisions of the NIS Directive in Finland, the OES shall manage "*the risks to the networks and information systems it uses'. For the banking, financial markets, and healthcare sectors already in place, legislation sufficiently meeting the security requirements of the NIS Directive has been deemed necessary*"[4]. Contrary to Article 243 of the Information Society /Act (917/2014), which has not been modified by the Governmental Proposition, there is however no mention of the terms *appropriate* and *proportionate* in other Acts. Newer amending Acts were researched in case changes intervening the latter, but without any success. It could be the case that Finland made the choice of placing the responsibility of each sector's Competent Authority for defining the security measures to be adopted for each essential service through soft law instruments (e.g., guidelines). For example, the Competent Authority of the Healthcare sector, Valvira, published on June 17th, 2019, a "*Cybersecurity guide for social and health care providers*", which provides guidelines on matters like risk management, fault identification and response or Cyber Disruption Management.[5] Furthermore, according to Chapter 9, Section 24 of the Act on the

[1] Wyrok, Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 22 października 2020 r., VI SA/Wa 2666/19

[2] Wyrok, Wojewódzkiego Sądu Administracyjnego w Warszawie, z dnia 3 września 2020 r., VI SA/Wa 2151/19

[3] Wyrok, Wojewódzkiego Sądu Administracyjnego w Warszawie, z dnia 5 sierpnia 2020 r., VI SA/Wa 2667/19

[4] Governmental Proposition for NIS Directive Implementation – HE 192/2017, pp. 19-21. Available at https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_192+2017.aspx, accessed on March 27th, 2021.

[5] Cybersecurity guide for social and health care providers (2019), pp. 22, 25, 26. Available at https://julkaisut.valtioneuvosto.fi/handle/10024/161683, accessed on March 25th, 2021.

Operation of Credit Institutions (610/2014), the Finnish Financial Supervisory Authority (Finanssivalvonta) may issue more detailed provisions on the operational risk. Finanssivalvonta has thus adopted provisions on the management of operational risk within the financial sector (**Appendix 15:** Security provisions by Finland).[1]

Law 2018-133 of February 26th, 2018, transposing the NIS Directive provisions in France, states that,

> "*The Prime Minister sets the security rules necessary for the security of the networks and information systems [of the OES]. These rules are intended to ensure a level of security adapted to the existing risk, considering the state of knowledge' (Art. 6 of the Law). They define the appropriate measures to prevent incidents that compromise the security of networks and information systems used for the provision of essential services or to limit their impact in order to ensure the continuity of these essential services*".

However, French law gets more precise by further detailing these rules. It states that "*the rules provided for in the first paragraph of this article are defined in each of the following areas: 1° The governance of the security of networks and information systems; 2° Protection of networks and information systems; 3° The defence of networks and information systems; 4° The resilience of activities*". A description which coincides with ENISA guidelines of 2017 on Mapping of OES Security Requirements to Specific Sectors.[2] Upon proposal from the ANSSI, a Ministerial Order from the Prime Minister sets therefore the security rules in those areas and the time limits within which they apply (Art. 10 of the Decree No. 2018-384 of May 23rd, 2018). Also, a Ministerial Order was adopted on September 14th, 2018, setting the security rules and deadlines. In this way, France meets the exact requirements of Article 14, para. 1 and 2 of the NIS Directive and details it further. Lastly, Article 6 para 3 Law 2018-133 of February 26th, 2018, provides the possibility for the State to prescribe that "*operators use hardware or software devices or computer services whose security has been certified*".

Like in France, Greek Law 4577/2018 transposing the requirements of the NIS Directive provides for the OES the obligation to take appropriate and proportionate technical and organisational security measures. Article 9, para. 1 (a) and (b) of Law 4577/2018 commits thus the National Cybersecurity Authority with an obligation of insurance, in collaboration with the competent CSIRT and the other involved bodies by sector of essential service. Ministerial Decision 1027/2019 further specifies those measures. Article 2 of the aforementioned Decision states that "*every OES or DSP is responsible for the commitments of any partner, natural or legal person, whom it uses for the construction, installation, maintenance or handling of its NIS for the provision of its essential services*". Article 3 of the same Decision forces both the OES and DSP to maintain a single policy for the security of its NIS. While Articles 4 and 5 further detail the security requirements. Finally, Article 6

[1] Määräykset ja ohjeet, Operatiivisen riskin hallinta rahoitussektorin valvottavissa on päivitetty, 8/2014; Määräykset ja ohjeet, Ulkoistaminen rahoitussektoriin kuuluvissa valvottavissa, 1/2012

[2] ENISA, 'Mapping of OES Security Requirements to Specific Sectors', January 2018

enumerates the obligations of the *Information and Network Security Officer*. Hence, the Greek provisions fully comply with Article 14, para 1 and 2 of the NIS Directive.

Ireland followed the same path as Finland by having recourse to a combination of hard and soft law instruments. Part 4, Regulation 17 of the S.I. 360 of 2018 replicates the provisions of Article 14 para. 1 and 2 of the NIS Directive in the exact same wording. It is then stated that

> "*(1) An operator of essential services shall— (a) take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems which it uses in its operations, and (b) take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used by it for the provision of the essential services in respect to which it is designated as an operator of essential services with a view to ensuring the continuity of the provision by it of those services. (2) The measures to be taken by an operator of essential services pursuant to paragraph (1) shall ensure, in regard to the state of the art, a level of security of network and information systems appropriate to the risks posed*".

While Irish NCSC of the Department of Communications, Climate Action & Environment published on August 2019 a NIS Compliance Guidelines for OES.[1] A document which offers a best practice framework for ensuring the protection of network and information systems.

Similarly to Ireland, Luxembourg replicates it with Article 8 para 1 and 2 of the Luxembourg Law of May 28th, 2019, the security requirements specified by NIS Directive in the same wording. It is however supplemented by a last sentence which is added to the European text, and which sets up the legal basis allowing the competent authorities concerned to specify a framework appropriate risk analysis for operators of essential services. Contrary to Ireland and Finland, it is indeed mentioned that the relevant to the essential sector competent authority (ILR or CSSF) may specify via a regulation the appropriate risk analysis framework in order to identify risks, regardless of the fact that the Council of State has been formally opposed to it because of the resulting legal uncertainty. This can result in a reading under the terms of which the said authority could sometimes have recourse to individual acts and sometimes to acts of a general normative nature. The provision was however adopted as such.

Although such regulations could be found for the identification of essential services, this was not the case for the risk analysis framework. Such regulation was impossible to be found neither from the ILS nor the CSSF. However, the ILR announced in a press release of July 31st, 2020, the launch of a new risk analysis platform (SERIMA -Security Risk Management) for telecommunications operators. The press release mentions that "*As part of the NIS Law, it will gradually be extended to the energy, transport, health, digital infrastructure, and*

[1] Department of the Environment, Climate and Communications, 'NIS Compliance Guidelines for Operators of Essential Service (OES)', August 2019 (updated on January 2021)

the supply and distribution of drinking water sectors. In this context, the NIS Security service of the ILR has set up working groups to adequately configure the platform by sector."[1] However, it might be considered that, even if any further detailed instruction in any kind of regulation could not be found, Luxembourg meets the criteria mentioned in Article 14, para. 1 and 2 of the NIS Directive. As the Member State of the EU provides requested insurances with its Law of May 28th, 2019, which also adds the requirement for the OES to notify risk management and prevention measures to the relevant competent authority, while the terms of this notification, the format, and the deadline, should be determined by the relevant competent authority by regulation (Article 8, para. 3).

Article 4, point 2 of the NIS Directive provides that the "*security of network and information systems means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems*". Based on this definition and on the content of the Reference document on security measures for the OES that was published by the NIS Cooperation Group. Poland further developed the criteria upon security measures mentioned by Article 14, para 1 and 2 of the NIS Directive. It is thus provided by Chapter 3, Article 8 of the National Cybersecurity System Act (NCSA) of July 5th, 2018, that

> "*The operator of the essential service shall implement in the information system used to provide this service a security management system that ensures:*
>
> *1) systematic incident risk assessment and risk management conduction*
>
> *2) implementation of technical and organisational measures appropriate and proportionate to the assessed risk, taking into account the latest state of knowledge, including: a) the maintenance and safe operation of the information system, b) physical and environmental security, including access control, c) security and continuity of the supply of services on which the provision of a key service depends, d) implementing, documenting and maintaining action plans to ensure the continuous and uninterrupted provision of the essential service and to ensure the confidentiality, integrity, availability and authenticity of information, (e) coverage of the information system used to provide the essential service with a continuous monitoring system;*
>
> *3) collecting information on cybersecurity threats and vulnerabilities of the information system used to provide the key service*
>
> *4) incident management*

[1] Gouvernement Luxembourgeois, 'L'ILR lance une nouvelle plateforme d'analyse de risques pour les opérateurs de télécommunications', [Prees Release] 31 July 2020, available at https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2020/07-juillet/31-ilr-analyse-risques.html (accessed on March 26th, 2021)

5) application of measures to prevent and limit the impact of incidents on the security of the information system used to provide the essential service, including: a) the use of mechanisms ensuring confidentiality, integrity, availability and authenticity of data processed in the information system, b) taking care to update the software, c) protection against unauthorised modification in the information system, d) immediately taking action upon noticing a vulnerability or threats to cybersecurity

6) use of means of communication enabling correct and secure communication within the national cybersecurity system."

A provision which exactly meets the criteria of the provisions of the NIS Directive. This provision does not however apply to operators who have facilities, installations, devices, or services included in the critical infrastructure and who have an approved plan for the protection of critical infrastructure along with documentation. Chapter 3, Article 10 of the NCSA goes deeper by requesting from the OES to "*develop, apply and update documentation on cybersecurity of the information system used to provide the essential service*" and "*to establish supervision*" over this documentation, "*ensuring 1) availability of documents only to authorised persons in accordance with their tasks; 2) protection of documents against misuse or loss of integrity; 3)the marking of successive versions of documents enabling the determination of changes made in these documents*". This documentation shall be kept "*for at least 2 years from the date of its withdrawal from use or termination of the provision of the essential service*" (Article 10, para 3).

To perform the tasks referred to in Art. 8 and 10, para. 1-3 the OES may establish internal structures responsible for cybersecurity or conclude an agreement with an entity providing cybersecurity services (Article 14, para. 1). The Ministry of Digital Affairs is responsible for defining, by way of a regulation, organisational and technical conditions for entities providing cybersecurity services for the OES and internal structures responsible for cybersecurity (Article 14, para. 4). Thus, a Regulation was published by the Ministry Digital Affairs on December 4th, 2019 relating the organisational and technical conditions for entities providing cybersecurity services and internal organisational structures of key service operators responsible for cybersecurity.[1] For example, a ministerial order from the Ministry of Maritime and Inland Navigation was also published on April 7th, 2020 relating the organisational and technical conditions and incident reporting under the national cybersecurity system in the water transport subsector and in the drinking water supply and distribution sector.[2] As it is the case for Finland, Ireland and Luxembourg, the implementation of Article 14, para 1 and 2 of the NIS Directive combines hard and soft law instruments. Since Article 42 of the NCSA

[1] Rozporządzenie Rady Ministrów z dnia 23 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz.U. 2019 poz. 2479

[2] Ministra Gospodarki Morskiej I Żeglugi Śródlądowej z dnia 7 kwietnia 2020 r. w sprawie warunków organizacyjno-technicznych oraz zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji, Dz.Urz.MGMiŻŚ.2020.20

provides that "*the authority competent for cybersecurity (…) prepares, in cooperation with the National CSIRT network,*[1] *recommendations regarding actions aimed at strengthening cybersecurity, including sectoral guidelines*[2] *for reporting incidents*".

Member States	Article 14§1 Compliance	Article 14§2 Compliance
Finland	Yes	Yes
France	Yes	Yes
Greece	Yes	Yes
Ireland	Yes	Yes
Luxembourg	Yes	Yes
Poland	Yes	Yes

Table 32: *Articles 14§1 and 14§2 Compliance*

(Table made by author)

6. OES Notification obligations (Art. 14)

Before continuing it is important to once again remind the OES obligation on incident notification as required by NIS Directive's provisions.The OES is obligated to "*notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide*"[3]. Two points stems from this obligation and should be kept in mind all along with the case study comparison which follow, the *undue delay* and the *significant impact* of the incident. *Undue delay* should be considered as soon as the operator is aware of the triggering event of the significant incident. While concerning the *significant impact*, the following parameters should be considered, "*(a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread regarding the area affected by the incident*" (Article 14, para 4 of the NIS Directive). If the incident has a cross-border dimension, 'the competent authority or the CSIRT shall inform the other affected Member State(s), "*by preserving 'the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification*"[4]. As stated in recital 32, it should be understood that the provision to authorise

[1] NASK, CSIRT GOV, CSIRT MON and sectoral cybersecurity teams.

[2] Ministerstwo Cyfryzacji, 'Materiały dla Operatorów Usług Kluczowych -Metodyka statycznej i dynamicznej analizy ryzyka', 30 May 2019, available at https://mc.bip.gov.pl/standaryzacja-bezpieczenstwa/materialy-dla-operatorow-uslug-kluczowych.html (accessed on March 26th, 2021)

[3] Article 14, para 3 of the NIS Directive

[4] Article 14, para 5 of the NIS Directive

Member States to choose between the recipients of notification and not to oblige them to offer an alternative to carry out the said notifications, so that the provision under notice and the subsequent provisions of the draft under notice, which fail to take up the alternative proposed by the directive, constitute a correct transposition. At last, Article 14, para 6 of the NIS Directive provides that "*after consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary to prevent an incident or to deal with an ongoing incident*".

To assess the Finnish implementation of the NIS Directive provision regarding the OES notification of incidents having a significant impact on the continuity of their services, it is important to once again compare the amending regulations of sectoral Acts (**Appendix 16:** OES Notification obligations by Finland). If we carefully examine the *undue delay* notification, all amending acts provides that the OES of each sector "*shall immediately notify*" to the Competent Authority for its sector "*any significant information security disruption to the communication networks or information systems used by it, as a result of which the [essential service] may be interrupted to a significant extent*" Therefore, the obligations of *undue delay* and *significant impact* are present for all sectors. This is also true for the cross-border information, as it stated that the sectoral Competent Authority "*shall assess whether the disturbance (...) affects other Member States of the European Union and, if necessary, notify the other Member States*". Confidentiality obligation is provided by sections 308 and 318 of the Information Society Act (917/2014). However, it should be noted that the criteria assessing the significant extent of an incident was not defined within legislative acts. The sectoral Competent Authority 'may issue more detailed regulations when the disturbance is significant, as well as the content, form and submission of the notification. Therefore, Finland meets all requirements of the NIS Directive on notification obligation of incidents.

In France, Article 7, para. 1 of Law 2018-133 provides that the OES shall "*declare, without delay [ANSSI] the incidents affecting the [NIS] necessary for the provision of essential services, when these incidents have or are likely to have, taking into account in particular the number of users and the geographical area affected as well as the duration of the incident, a significant impact on the continuity of these services*" and this, "*without prejudice to the sectoral provisions providing for other incident notification regimes*"[1].

Concerning *cross-border notification*, Article 7 of the aforementioned law continues mentioning that "*when an incident has a significant impact on the continuity of essential services provided by the operator in other Member States of the European Union, the administrative authority informs the competent authorities or bodies of these States*"[2]. While as soon as "*they become aware of additional information relating to the causes of the incident or its consequences, in particular, where applicable, (...) the operators shall communicate this*

[1] Article 11, para. 1 of the French Ministerial Decree 2018-384

[2] Article 7, para. 2 of the Law 2018-133

information to the agency. [OES] shall also 'respond to informational requests from ANSSI concerning incident evolution"[1].

Prime Minister's Ordinance of June 13th, 2018, sets out incident notification procedures, provided for in Articles 8, 11 and 20 of Decree No. 2018-384 of May 23, 2018, relating to the security of networks and information systems of operators of essential services and service providers digital. Notification requirement to the public is fulfilled by Article 7, para. 2 of Law 2018-133 and Article 12 of the Ministerial Decree 2018-384 ,while confidentiality obligation upon notification has been met by Article 3, para. 2 of Law 2018-133. It states that "*when informing the public or Member States of the European Union of incidents under the conditions provided for in Articles 7 and 13, the competent administrative authority shall consider the economic interests of these operators and digital service providers and ensure that they do not reveal information likely to endanger their security and commercial and industrial secrecy*". Thus, France exactly meets Article 14 requirements of the NIS Directive (**Appendix 17**: OES Notification obligations by).

In Greece, Article 9, para. 1(c), 2, 3,4 of Law 4577/2018 is perfectly duplicated meeting NIS Directive's requirements of incidents having a significant impact on the provisions of OES services. Article 9 of Ministerial Decision 1027/2019 of October 8th, 2019, further details the notification procedure. The initial report shall be provided to the Authority electronically or in writing, in the form which sets the relevant standard of the Authority, and within 24 hours after the entity became aware of the incident. The notification must contain at least the following information: a) the name or surname of the institution as well as the type of services it provides; the time at which the incident was diagnosed; the exact duration of the incident, from the moment it was diagnosed until its complete treatment, if it is considered over; information on the nature of the event, as well as a first impact assessment; information on the actions taken and the measures to limit the impact of the event that have already been taken; information on the likelihood of more Member States being affected by the incident; and any other information deemed to assist the work of the competent authorities. If the details of the incident change substantially, the OES may further submit an updated report, which will provide as much information as possible about it. Moreover, the final report is provided to the Authority in writing, in the form which sets out a relevant standard of the Authority and within one (1) month from the closing date of the security event.

After receiving the initial report, the competent authorities evaluate the incident and decide on the immediate actions to be taken. If the incident has a serious impact on the continuation of essential service in another Member State, the competent authorities shall inform the competent authorities of the Member State without delay. Upon receipt of the final report, the Competent Authorities evaluate the data, inform the entity of the effectiveness of incident management, and provide guidance on preventing or better managing future related

[1] Article 11, para. 2 of the French Ministerial Decree 2018-384

incidents.[1] Following article 11 of the Decision, after consulting the Agency, and when deemed necessary for the better management of the incident, the National Cybersecurity Authority shall ensure that the public enjoying the service affected by the incident is informed of its existence, its response and its possible disruption of the normal operation they suffered. Informing the public is not appropriate when it concerns sensitive or classified information, and it disproportionately affects the legitimate interests of the Organisation. In case the National Cybersecurity Authority deems that these both reasons do not exist, it can inform the public judging on a case-by-case basis and proportionally. Therefore, Greece also perfectly meets all incident notification requirements of the NIS Directive, as the same wording was used.

Irish Statutory Instrument No. 360 of 2018 provides that an OES shall "*notify the CSIRT of any incident concerning it that has a significant impact on the continuity of an essential service provided by it in respect of which it is designated as an OES*"[2]. The same applies for third-party digital service providers for the provision of an essential service for which it is designated as an operator of essential services.[3] Concerning the *undue delay*, notification in case of an incident shall be made not later than 72 hours the starting point being the moment when the OES becomes aware of the occurrence of that incident (Article 18, para. 2). Contrary to previously mentioned Member States, an indicative, sector specific Incident Reporting levels, according to which an incident has a significant impact on the continuity of the essential service, may be found in Appendix C of the NIS Compliance Guidelines for Operators of Essential Service (OES), which was edited in August 2019 by the Irish Department of Communications, Climate Action and Environment. A reproduction of the Appendix C may be found in annexed to the present study table (Table). In such cases, the "*CSIRT may inform the public about the incident to which the notification relates where the CSIRT considers that public awareness is necessary to deal with the incident*" (Article 18, para. 8). Concerning cross-border information, Regulation 18, para. 6 provides that "*the CSIRT shall (…) inform the single point of contact in the other Member State of the incident and may request the single point of contact to forward the notification made (…) to the single point of contact in the other member state*". Finally, Confidentiality is ensured by Regulation 5 of the Statutory Instrument. Therefore, Ireland also exactly meets NIS Directive's incident notification criteria, while a combination of hard and soft law is also made upon incident significant impact's criteria (**Appendix 18**: Security provisions by Ireland).

In Luxembourg, Article 8, para. 4 and following of the Law of May 28th, 2019, implements NIS Directive's incident notification requirements by using almost the same wording.

> "*Operators of essential services shall notify the relevant competent authority, without undue delay, of incidents which have a significant impact on the continuity of the essential services they*

[1] Article 10 of the Ministerial Decision 1027/2019 of October 8th, 2019

[2] Regulation 18, para. 1a, Irish Statutory Instrument No. 360 of 2018

[3] *Ibid*, Regulation 18, para. 1b

provide. These notifications are sent to the Governmental CERT and to the CIRCL according to their respective skills. The notifications contain information enabling the relevant competent authority to determine whether the incident has a cross-border impact. This notification does not increase the liability of the originating party" (Article 8, para. 4).

The relevant competent authority may specify, by regulation, the parameters, terms, and deadlines for notifications of incidents that have a significant impact on the continuity of the essential services they provide. A national public consultation is in progress from March 25th, 2021[1] on the ILR / N21 / 1 du DD-MM-YYYY regulatory project for the definition of criteria and their respective effects with respect to the impact on the continuity of essential services in the energy sector. Regulation 14/181 /ILR of August 28th, 2014[2] constitutes thus the only regulation, according to our research knowledge, providing criteria and thresholds in relation to the significant impact on the operation of networks or services that must be reported to the ILR in the event of a breach of security or loss of integrity of electronic communications networks and services. Finally, Article 8, para. 7 of the Law of May 28th, 2019, constitutes an addition to the Directive as it states that

"*Once a year, the relevant competent authority shall transmit to the single national contact point a summary report on the notifications received, including the number of notifications and the nature of the incidents notified (...). Every year, the single national contact point shall transmit to the cooperation group a summary report on the notifications received, including the number of notifications and the nature of the incidents notified (...)*".

In Poland, the NCSA provides that, "*driven by the need to ensure protection against threats to human life or health, significant property losses and deterioration of the quality of the key service provided*" (Article 11), the OES shall classify as serious any incident affecting the provision of its services on the basis of the incident serious thresholds, report a serious incident immediately, no later than 24 hours, starting from its detection, to the appropriate CSIRT MON, CSIRT NASK or CSIRT GOV; and interact with the relevant CSIRT MON, CSIRT NASK or CSIRT GOV during the handling of a serious incident and a critical incident, providing the necessary data, including personal data'.[3] Therefore,

"*The Council of Ministers shall define, by way of regulation, the thresholds for considering an incident as serious, by type of incident in individual sectors and subsectors specified in Annex 1 to the Act, taking into account 1) the number of users affected by the disruption of the essential*

[1] Retrieved from https://web.ilr.lu/fr/professionnels/niss/nis---securite-des-reseaux-et-systemes-dinformation/operateurs-de-services-essentiels-ose/_layouts/15/ilr.internet/nouveaute.aspx (accessed on March 28th, 2021)

[2] Institut Luxembourgeois de Régulation - Règlement 14/181/ILR du 28 août 2014 portant définition de critères et de seuils en relation avec l'impact significatif sur le fonctionnement des réseaux ou des services à signaler obligatoirement à l'Institut en cas d'atteinte à la sécurité ou à la perte d'intégrité de réseaux et de services de communications électroniques - Secteur Communications électroniques

[3] Article 11, para. 1 of the NCSA

service, 2) time of impact of the incident on the essential service provided, 3) the geographical scope of the area affected by the incident, 4) other factors specific to a given sector or subsector, if any - driven by the need to ensure protection against threats to human life or health, significant property losses and deterioration of the quality of the essential service provided"[1].

Entered into force on November 1st, 2018, a Regulation of the Polish Council of Ministers was published on October 31st, 2018, related to thresholds for categorising an incident as serious (**Appendix 19**: Security provisions by Poland). Therefore, the requirements of Article 6 of the NIS Directive were perfectly met by Poland.

The notification of any incident that has a significant impact should be provided in electronic form or any other available means of communication.[2] Regardless of the tasks specified in article 11, para. 1 of the NCSA the OES shall, in the case of establishing a sectoral cybersecurity team, "*simultaneously submit to this team in an electronic form the notification (...); interact with this team at the sector or sub-sector level during the handling of a serious incident or a critical incident by providing the necessary data, including personal data; and provide this team with access to information about registered incidents to the extent necessary to perform its tasks*". The NCSA further specifies the content contained in the notification, as in the data of the notifying OES, the description of the incidents having a significant impact or any other relevant information.[3] Confidentiality is ensured by Article 12, para. 2 and following of the NCSA, if the NCSA in Poland complies with the NIS Directive's provisions related to the *undue delay* criteria, the significant impact assessment, confidentiality preservation and finally the cross-border notification. The criterion of public information does not seem to have been reached contrary to other compared Member States as such provision does not figure within the NCSA. However, this criterion is not mandatory as NIS Directive provides it with the verb *may*. Finally, soft law instruments do not seem to be favoured.

[1] Article 11, para. 4 of the NCSA

[2] *Ibid*, Article 11, para. 2

[3] Article 12, para. 1 and 2 of the NCSA

Member States	Article 14§3 Compliance	Article 14§4 Compliance	Article 14§5 Compliance	Article 14§6 Compliance
Finland	Yes	Yes	Yes	Yes
France	Yes	Yes	Yes	Yes
Greece	Yes	Yes	Yes	Yes
Ireland	Yes	Yes	Yes	Yes
Luxembourg	Yes	Yes	Yes	Yes
Poland	Yes	Yes	Yes	Yes

Table 33: *Article 14§3, 14§4, 14§5 and 14§6 Compliance*

(Table made by author)

C. Comparative Results

Comparative analysis of Articles' 5, 6, 7, 8, 9, 14 and 21 transpositions of the NIS Directive, which corresponds to a selection of minimum harmonisation provisions, results in compliance among case studies. Selected articles were transposed using the same wording with the NIS Directive. The difference relies on the methodology employed for transposition. All Member States have transposed the provisions using the same wording with the NIS Directive, although compliance was not achieved on time for all Member States. But let us look first at the compliance outcome.

Following the transposition of the NIS Directive, the Commission sent on 19 July 2018 a notification to France and 16 other Member States asking them to *fully transpose* the NIS Directive.[1] A partial transposition had indeed been reported by the Commission to France, along with Denmark, Lithuania, and Hungary. In the absence of an official document explaining the Commission's motivation it could be speculated that further specification by a Ministerial Decree for provisions of the French NIS Directive transposition act (e.g., Article 6 on security rules necessary for the protection of OES networks and information systems) may explain the Commission's notification against France. Possible support for this hypothesis may be found in the French Decree n° 2018-384 adopted on 23 May 2018 relating to the networks and information systems security of essential and digital services providers. As Member States had to transpose the NIS Directive into national laws by 9 May 2018, the infringement proceeding against France was finally closed on January 24th, 2019.[2]

[1] Available at https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4486 (accessed on March 17th, 2021)

[2] Available at https://ec.europa.eu/commission/presscorner/detail/EN/MEMO_19_462 (accessed on March 17th, 2021)

Greece also appeared, along with France, on the notification sent by the Commission to 17 Member States on 19 July 2018 asking them to *fully transpose* the NIS Directive into their national legal framework.[1] In the absence of an official document one may only speculate about the Commission's motivations in notifying Greece with a partial transposition. It could be argued that the reason for the delayed transposition was the fault of the NIS Directive. As Law 4577/2018 transposing the NIS Directive was adopted on December 3rd, 2018, 6 months later after the transposition period. The infringement proceeding against Greece was closed on 7 March 2019.[2] The same goes for Ireland, Luxembourg and Poland which transposed NIS Directive on September 18th, 2018,[3] May 28th, 2019, and November 21st, 2018, respectively. Infringement proceedings were closed on January 24th, 2019,[4] for Ireland, on March 7th, 2021, for Luxembourg and Poland.[5] Finland was the only Member State of the EU among those selected for the current study, which has appeared on the letter of formal notice (Art. 258 TFEU) sent by the Commission for partial transposition of the NIS Directive.

Concerning the outcome upon the sample of seven provisions examined in the previous paragraph, the following applies; For the National strategy on NIS security all Member States of the present study have integrated the requirements of Article 7 into their legislative framework apart from Finland and France. However, it is worth mentioning that even if they have followed this practice, all of them have integrated NIS security objectives in a document defining broader objectives for cybersecurity in general.

Regarding the NIS governance framework's identification, all Member States have identified competent authority(-ies), CSIRT(s) and a Single Point of Contact through their respective implementing legislative acts. Finland and Poland adopted a more sectoral approach identifying competent authorities for each essential sector. France and Greece adopted a centralised approach making the ANSSI the unique competent authority and single point of contact of the country, while Luxembourg and Ireland opted for a hybrid approach by centralising at first OES and DSPs operations' supervision under two respective competent authorities and by designating secondly the competent authority for OES as Single point of contact and/or National Cybersecurity Authority. A perplex situation which may rise obstacles on the application of the NIS Directive. Communication from the Commission towards the effective implementation of Directive (EU) 2016/1148[6] states indeed that adopting a more decentralised approach and "*ensuring strong cooperative arrangements between numerous authorities and the single point of contact, would increase effectiveness of transposition and facilitate enforcement*". It

[1] Available at https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4486 (accessed on March 17th, 2021)

[2] Available at https://ec.europa.eu/commission/presscorner/detail/EN/MEMO_19_1472 (accessed on March 17th, 2021)

[3] S.I. No. 360/2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018

[4] Available at https://ec.europa.eu/commission/presscorner/detail/EN/MEMO_19_462 (accessed on March 17th, 2021)

[5] Available at https://ec.europa.eu/commission/presscorner/detail/EN/MEMO_19_1472 (accessed on March 17th, 2021)

[6] European Commission, Annex to the Communication on 'Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', COM(2017) 476 final/2.

could be thus considered that in terms of transposition efficiency the strategy of France and Greece seems to meet these criteria.

Concerning the CSIRT tasks, Finland, France, and Luxembourg met under broader terms NIS Directive's Annex I requirements, contrary to Greece, Ireland and Poland which exactly transposed the provisions using the same wording with the NIS Directive. The difficulty persists however on assessing if national CSIRTs dispose indeed of *adequate resources* to perform assigned tasks. There is no indication from the Commission or the ENISA on how to assess this criterion. But it is possible to consider that Annex I, para. 1 (c) criterion of the NIS Directive on *business continuity* may be of great help. It should be then reminded that, according to this criterion, CSIRTS should "*(i) be equipped with an appropriate system for managing and routing requests, to facilitate handovers; (ii) be adequately staffed to ensure availability at all times; and (iii) rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available*". Greece, Ireland, and Poland are legally bound unlike their counterparts, as they transposed this criterion into their respective national orders. The assessment will mostly rely on the case-by-case fruitful treatment of disruptive incidents upon NIS. An assessment which falls mostly under the administrative effectiveness hypothesis advanced by the present study and for which, a study will be provided in the next section.

On the OES identification criteria, it could be stated that all Member States used the NIS Directive's Annex II on the type of entities falling within the scope of the definition on the OES (Article 4, point 4 of the NIS Directive) as a common starting base. Greece and Luxembourg made no changes. Ireland only added the following type of entities in the Credit Institution subsector: Payment Services provided to non-Monetary Financial Institutions in the State, Cash Services provided in the State Access to retail payment systems provided to credit institutions in the State. While France and Poland further extended the NIS Directive's scope to further essential sectors and subsectors like insurance, education, or mining.

Finland has on the other hand drastically limited the OES falling the scope of the NIS Directive e.g., e only transmission system's operators in the electricity and natural gas subsectors or only TLD name registries in the Digital infrastructure sector, which is permissible as not all type of entities defined by Annex II of the NIS Directive operate in the country. For example, there are no Central counterparties (CCPs) in Finland. A divergent interpretation stems therefore by these differentiated approaches from Member States on what constitutes an essential service under the NIS Directive. In this way, the scope of the Directive risks being fragmented, with some operators being exposed to additional regulation (because they have been identified by their respective Member State) while others providing similar services remain excluded (because they have not been identified). To address these inconsistencies, a second proposal of December 16th, 2020, from the

Commission amending the NIS Directive should lead to a more aligned list of essential services by extending the scope of the Directive.[1]

Concerning the setting of the identification thresholds, Greece and Poland have made them public through secondary law instruments contrary to the other Member States. It is however interesting to note that while all Member States transposed the identification thresholds according to NIS Directive provisions, Poland considered only sector-specific factors applicable (Article 6, para. 2 of the NIS Directive) for most identified entities. The Directive mentions that "*Member States shall also, where appropriate, consider sector-specific factors*". Article 6, para. 2 of the NIS Directive does not offer thus an alternative. All factors need to be considered[2] and "*where appropriate"* sector-specific factors also. A situation which is interesting in relation to the terminology used by the directive and the one used upon transposition by Member States. The Commission states in its report assessing the consistency of the approaches taken by Member States in the identification of operators of essential services that, "*Member States have developed a variety of methodologies when it comes to the overall approach to the identification of OES (section 2.1) but also regarding the definition of essential services and the setting of thresholds*"[3]. It is stated for example that "*due to Finland's identification methodology, a very large number of OES [10897] were identified in the health sector*"[4]. A finding that may have "*a negative impact on the consistent application of the NIS provisions across the Union with possible consequences for the well-functioning of the internal market and the effective handling of cyber-dependencies*"[5].

Article 14, para. 1 and 2 of the NIS Directive imposes on Member States to ensure that OES risk management and prevention is "*appropriate and proportionate (…) to the security of network and information systems which they use in their operations*". The term appropriate and proportionate being not specified by the Directive, a dedicated work stream of the Cooperation Group offered non-binding guidelines concerning the security measures for OES.[6] Guidelines which were almost implemented from all Member States either using exclusively secondary law instruments (e.g., France or Greece) or combining them with soft law instruments (e.g., Finland or Ireland). As we know now Finland has adopted a sectoral approach upon NIS Directive transposition. There is not one central legislative act which amends sectoral acts. On the contrary, all sectoral

[1] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', 16 December 2020, COM(2020) 823 final

[2] European Commission, Annex to the Communication on 'Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', 13 September 2017, COM(2017) 476 final/2, 26

[3] European Commission, Report to the European Parliament and the Council 'assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems', 28 October 2019, COM(2019) 546 final, 22

[4] *Ibid*, p. 27

[5] *Ibid*, p. 22

[6] Cooperation Group, 'Reference document on security measures for OES', *CG Publication 01/2018*

acts regulating sectors falling within the NIS Directive's scope for OES were amended separately. Therefore, assessing NIS Directive provision transposition faced some difficulties, while not using the same wording with the NIS Directive has exacerbated them.[1] It is worth mentioning however that Greece has made the choice to unify the security measures requirements for OES and DSP's. Therefore, maximum harmonisation requirements for DSP's have also been transposed for OES security measures.

Concerning the rest of Article 14 of the NIS Directive on incident notification, all Member States studied by the present thesis have correctly transposed through primary law instruments the related provisions. The term of *undue delay* was however not specified letting enough room for interpretation by Member States, even though non-binding notification guidelines were once again published by the Cooperation Group.[2] Finland, France, Greece, and Luxembourg have maintained the same or approximate wording, while Ireland and Poland provided the *undue delay* as 72 and 24 hours, respectively. Greece further detailed the term through secondary law instrument[3] and retained same delay as Poland. In all cases, the delay starts running out the moment from which the incident is discovered. For Finland, France, and Luxembourg a recourse to soft law instruments may be expected. Cross border notification, information confidentiality clause and notification to the public were transposed accordingly to the NIS Directive by almost all Member States,[4] while significant impact determination offers once again a mitigate picture. In Finland, the sectoral Competent Authority may issue more detailed regulations on when the disturbance is significant, as well as on the content, form, and submission of the notification. The provision is thus ensured through hard law instruments. The same is also true for France, Greece, Luxembourg, and Poland. While Ireland had recourse to a combination of primary law and guidelines destinated to OES, Ireland and Poland, which used different implementation instruments, were the only ones publicly providing the thresholds above for when an incident should be considered as having a significant impact.

If the rest of minimum harmonisation provisions were assessed in detail the results would be the same. All Member States complied with NIS Directive requirements using more or less the same wording, while hard law instruments were the most used (**Table 34**).

Compliance with NIS Directive Articles (Hard / Soft law instruments)

[1] Contrary to Digital Infrastructures, there is no reference to 'appropriate' and 'proportionate' security measures for the rest of the OES.

[2] Cooperation Group, 'Reference document on Incident Notification for OES Circumstances of notification', *CG Publication 02/2018*

[3] Ministerial Decision 1097/2019

[4] In the case of Poland, it was impossible to find any provision related to public information. However, it should be stated once again that this provision is not mandatory.

Member States	Art. 5	Art. 6	Art. 7	Art. 8	Art. 9§1	Art. 9§2	Art. 14§1	Art. 14§2	Art. 14§3	Art. 14§4	Art. 14§5	Art. 14§6
Finland	Yes (Both)	Yes (Both)	Yes (Soft)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Both)
France	Yes (Both)	Yes (Both)	Yes (Soft)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Both)
Greece	Yes (Hard)	Yes (Hard)	Yes (Both)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)
Ireland	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Both)
Luxembourg	Yes (Both)	Yes (Both)	Yes (Both)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Both)	Yes (Both)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)
Poland	Yes (Hard)	Yes (Hard)	Yes (Both)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Both)	Yes (Both)	Yes (Hard)	Yes (Hard)	Yes (Hard)	Yes (Hard)

Table 34: *Compliance with NIS Directive Articles (Hard / Soft law instruments)*

(Table made by author)

The above comparative study on national transposition is leading to the following finding. Differences upon transposition outcomes may result because of the political interests pursued by Member States of the EU. Some states will put forward their national security, while others will transpose the directive with the only preoccupation of not being submitted to an infringement proceeding. A differentiated approach which is mostly allowed by the *regulatory flexibility* accorded by the EU NIS directive.

It is important to remember that the interest of the present study is to assess the effectiveness of EU law, specifically the NIS Directive, and not the legality of national transpositions. Neither the Commission nor the CJEU have initiated until today new compliance infringements against Member State(s) of the EU or any judicial rules on NIS Directive application, respectively. As mentioned in the introduction it is therefore important for the purposes of the present study to understand, what motivates Member States of the EU to make adopt different approaches upon transposition. Since the effectiveness of the NIS Directive may be jeopardised as the 2020 proposal repealing the NIS Directive tends to prove it.

On 25 June 2020, the European Commission published a combined evaluation roadmap/inception impact assessment on the revision of the NIS Directive (SWD/2020/345 final), according to which it planned to "*evaluate the functioning of the NIS Directive based on the level of security of network and information systems in the Member States*" Among others, the evaluation showed that regarding the discretion afforded to Member States, when laying down security and incident reporting requirements for OESs, led to an implementation in significantly different ways, creating an additional burden for companies operating in more than one Member State. The supervision and enforcement regime of the NIS Directive is ineffective. Member States do not share

information systematically with one another. The NIS Directive does not provide sufficient clarity as regards the scope criteria for OESs or the national competence over digital service providers.

In the next section, an explanatory overview of policy factors susceptible to affect transposition outcome across the EU will be then presented after testing hypothesis formulated in the present study.

§3. Extent of Usage of NIS Directive Regulatory Leeway

For the European Union the cybersecurity is understood as critical to individuals' privacy, business, and commerce. This falls under the broader European vision of the Digital Single Market that aims to integrate daily functions into the digital realm. Since the development of these asymmetric threats the EU has introduced directives such as the GDPR that aims at protecting privacy, the NIS Directive aims at securing operators of critical infrastructure and has established ENISA, the agency which is majorly responsible for cybersecurity directives. Adversely, the United States and the United Kingdom support a narrative which depicts cybersecurity as a danger to national security and stresses the need to employ military forces to deal with the issue. The EU does not completely reject this argument but prefers to conceptualise cybersecurity as a commercial problem that needs to be addressed by civilian authorities.

Definitions used to refer to cybersecurity by various actors, including EU Member States, bodies, and institutions, typically represent different perspectives, which can potentially be at odds with each other. For example, whereas ENISA often frames cybersecurity as a mere technical issue, some Member States in their national security strategies regard cybersecurity as an issue of national security (e.g., Estonia and Slovakia).[1] The possibility of attaching different meanings to the term *cybersecurity* has both advantages and disadvantages. It indicates the flexibility of the term that can adapt to changing circumstances. It opens therefore a space for friction between EU and Member States, powered around the national security notion.

EU Member States can be mostly inclined to make usage of discretionary room granted to them, to adapt NIS directive following objective pursued by national cybersecurity strategy. It should then be remembered that the present thesis assumes the usage of *discretionary room* as a dependent variable, which measures the degree to which Member States are willing to go beyond the required minimum thresholds set by NIS directive provisions. The higher the level of discretion granted to Member States by the NIS Directive, the greater the extent of the modifications by Member States and so, the divergences upon transposition outcome.

The extent of the *discretionary room* employed by Member States is measured here at the provision level. Only provisions that grant discretionary powers by allowing states to maximise directive's requirements on transposition process will be retained for the present study. Provisions delegating powers to the Commission

[1] G. G. Fuster and L. Jasmontaite, 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights', in M. Christen, B. Gordijn and M. Loi (eds), *The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology*, (Springer, 2020), 104

were thus excluded. Thus, the following values are used. When the provision of the NIS Directive is not transposed but national legislation complies with Directive in a different way (e.g., the competent authority is designated without using any legislative act), the value *low* is used. When the national rule is the same with the corresponding provision of the NIS Directive, the value *medium* is used. While the value *high* is used when the national rule meets and exceeds the provision of the NIS Directive.

Discretionary Deviation thresholds	
Low	*the provision of the NIS Directive is not transposed but national legislation complies with Directive in a different way*
Medium	*the national rule is exactly the same with corresponding provision of the NIS Directive*
High	*the national rule meets and exceeds the provision of the NIS Directive*

Table 35: *Discretionary Deviation thresholds*

(Table made by author)

From the comparative made between the six case studies I get the following results. Finland is making mostly a low to medium usage of the discretionary room let by the NIS Directive through both the usage of soft and hard law instruments. While France moves from medium to high usage of discretionary room and makes mostly usage of hard law instrument contrary to Finland. Greece appears to have adopted the same behaviour as France. Ireland and Luxembourg are presenting a medium usage of discreteness and a recourse to hard law instruments, as is the case for France and Greece. Unlike previous countries, Poland is pursuing for most provisions of the NIS Directive a high usage of the discretionary room by the Directive, followed by a recourse to hard law instruments.

The classification that stems from the aforementioned behaviour is categorised into three distinct groups: 1. Finland; 2. France, Greece, Ireland, Luxembourg and; 3. Poland seems to reside in the centralised versus sectoral approach on NIS Directive transposition. Indeed, Finland has opted for a transposition throughout a modification of its sectoral legislations. While the other 5 countries have opted in for a centralised approach by adopting one central regulatory framework. However, the combination of high usage of NIS Directive's flexibility followed by a high recourse to hard law by Poland is not allowing us to consider two groups. Therefore, the explanation should be found elsewhere.

The only plausible reason which may allow us to explain the outcome, is what Falkner called *the world of compliance*.[1] Indeed, according to Falkner typology, Finland belongs to the world of law Observance. While France, Greece, Ireland,[2] Luxembourg, belong to the world of transpositions neglect. Poland belongs to the world of dead letter.[3] According to Falkner, the states that belong to the world of law observance have a very good compliance record by transposing directives in a fully correct manner; and Finland is a such case since it had fully transposed the NIS Directive by May 9th, 2018. Same thing applies to the next group from the world of transposition neglect, France, Greece, Ireland, and Luxembourg having been the subject of a formal notice from the European Commission for fully complying. While Poland was part of this list, it belongs to a cluster in which states "*may transpose EU Directives in a compliant manner, depending on the prevalent political constellation among domestic actors*"[4]. At the time of transposition of the NIS Directive in Poland on August 13th, 2018, The First Cabinet of Mateusz Morawiecki formed the government of Poland between 2017 and 2019, following Szydło's cabinet. Both Prime Ministers Beata Szydło and Mateusz Morawiecki belonged to the same right-wing populist and national-conservative political party, the Law and Justice Party (Prawo I Sprawiedliwość).

Article	**Extent of Usage of 'Discretionary Room'**					
	Finland	**France**	**Greece**	**Ireland**	**Luxembourg**	**Poland**
Art. 5 §2	Low	Medium	High	High	Medium	Medium
Art. 5 §3	Low	High	Medium	Medium	High	High
Art. 6 §1	Medium	Medium	High	Medium	High	High
Art. 7 §1	High	Low	Medium	Medium	Medium	Medium
Art. 8 §1	High	Medium	Medium	High	High	High
Art. 8 §2	Medium	High	Medium	Low	High	Medium
Art. 8 §5 al. 1	Low	Low	Low	Low	Medium	Low
Art. 9 §2	Low	Low	Medium	Medium	Low	High
Art. 9 §3	Low	Low	Medium	Medium	Medium	High
Art. 14 §1	Low	High	High	Medium	Medium	High
Art. 14 §2	Low	High	High	Medium	Medium	High
Art. 14 §3	Medium	Medium	Medium	High	Medium	High
Art. 14 §4	Low	Medium	High	Medium	Medium	Medium
Art. 14 §5 Al. 2	Medium	Medium	High	Medium	Medium	High

[1] G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States*, (Cambridge University Press, 2005).

[2] It is interesting to note here that while in Falkner's original work Ireland was subsumed to belong in what he called the 'world of neglect' (Falkner, Treib, Hartlapp and Leiber, 2005, pp. 339-40). In his newer research work on Central and Eastern Europe, he decided to revise this assignment and include Ireland into the 'world of dead letter' (Falkner and Treib, 2007, pp. 4-5)

[3] See G. Falkner and O. Treib, 'Three Worlds of Compliance or Four? The EU15, Compared to New Member States', (2007) *Political Science Series* 112, Institute for Advanced Studies: Vienna, 22

[4] Ibid, p. 14

Art. 15 §2	Medium	High	High	Medium	Medium	High
Art. 15 §4	Medium	High	High	High	Medium	High

Table 36: *Extent of Usage of 'Discretionary Room'*

(Table made by author)

As already stated in the introduction of this section, only articles presenting an open statement were retained for the dependent variable meausrement. This means that the extent of usage of NIS Directive regulatory discreteness was only evaluated for articles that allow for a choice by the transposing authorities in the Member States and therefore delegate some policy-making power to Member States. Since the tested provisions offers a minimal threshold of harmonisation. The articles present a medium level of regulatory leeway granted to Member States. It is possible then to come up with the following results on the extent of usage of the *disrectionary room* let by the NIS Directive. (**Table 38**).

Regulatory Discreteness		
Member State	**Regulatory Discreteness**	**Extent of Usage of 'Discretionary Room' (highest score)**
Finland	Medium	Low (8)
France	Medium	Medium (6)
Greece	Medium	High (8)
Ireland	Medium	Medium (10)
Luxembourg	Medium	Medium (11)
Poland	Medium	High (11)

Table 37: *Regulatory Discreteness*

(Table made by author)

Section II. Assessing the Impact of Domestic Factors

The multitude of actors involved at the various levels and stages of an EU Directive's life cycle offer numerous possibilities for shortcomings in transposition and application. In this last section of the empirical Analysis, the relevance of three factors tested for explaining the methodological differences between the transposition outcomes that were put forward in the previous part.

The first paragraph tests the hypotheses formulated in the present study for the NIS Directive for assessing the relevance of their variation with the dependent variable of regulatory leeway (**§1**). The hypotheses cover factors known in implementation studies such as the misfit between European and domestic rules. They also include policy specific determinants, such as institutional setup of a political economy and the administrative effectiveness. The second paragraphe explains the transposition processes in for each of the six Member States throughout a national policy-making approach (**§2**).

§1. Testing Hypotheses

Departing from the Minimum Harmonisation Provisions of the NIS Directive's presented in previous section, we first determined for NIS directive the number articles that are relevant for our study and are providing requirements to Member States about how to transpose the content of the NIS Directive. I have not taken in consideration the final provisions such as the entry into force of the directive and transposition.

Secondly, I classified each article according to the type of statement it contained : closed or open statement. As closed statements have been considered those which bear an obligation of means for Member States, while open statements relate only obligations of means. While as open statements have been considered those delegating some policy-making power to Member States (**Table 35**).

NIS Directive's Provisions with an Opened Statement						
Art. 5 §2	Art. 6 §2	Art. 8 §3	Art. 9 §1	Art. 14 §1	Art. 14 §5 Al. 1	Art. 15 §2
Art. 5 §3	Art. 7 §1	Art. 8 §5 al. 1	Art. 9 §2	Art. 14 §2	Art. 14 §5 Al. 2	Art. 15 §4
Art. 5 §4	Art. 8 §1	Art. 8 §5 al. 2	Art. 9 §3	Art. 14 §3	Art. 14 §5 Al. 3	
Art. 6 §1	Art. 8 §2	Art. 8 §6	Art. 10 §3 Al. 1	Art. 14 §4	Art. 14 §5 Al. 4	

Table 38: *NIS Directive's Provisions with an Opened Statement*

(Table made by author)

It is upon those provisions that comparative analysis and hypotheses testing will be conducted in the following developments. There are two ways of looking for hypothesis validation. Either the hypothesis works for the 6 cases, and it is therefore validated. Either it does not work for the six cases and in this case it is not validated. As we will see in the following developments. Hypothesis which are not validated will lead to multi-factor explanations. In these cases, an attempt will be made to explain why a factor is explanatory in one Member State and not in the other.

Hypotheses Testing will depart from the aforementioned provisions, starting by the Policy (**A**) and Institutional (**B**) Misfit hypothesis and at last, ending with administrative effectiveness (**C**).

A. Policy Misfit

The first factor tested in this section is the policy misfit between NIS EU policy framework and national laws. It should be kept in mind that the policy misfit hypothesis is expressed in a way that the presence of an explanatory factor makes the result more likely. Therefore, the present thesis argues that the higher the policy misfit, the greater the extent of the modifications by Member States and the divergences upon transposition outcome. To measure and compare the policy misfit, I use three categories: a high, medium and low policy misfit (**Table 39**).

Policy misfit thresholds	
Low misfit	*e.g., security requirements and incident notification rules are the same or almost the same with the requirements already in place under national law*
Medium misfit	*e.g., security requirements and incident notification rules are not entirely new*
High misfit	*e.g., security requirements and incident notification provisions require completely new legal rules*

Table 39: *Policy misfit thresholds*

(Table made by author)

The following section applies this approach to the legislation in the six Member States. For allowing an ease comparability, I will regroup addressed provisions by the present study in three groups: the National strategy on the security of network and information systems, the Governance structure on NIS and the OES.

1. Finland

As stated in previous sections, Finland was the only State from the case studies of this thesis work, which has transposed the NIS Directive in due time without receiving any infringement notice from the Commission. Whenever we take the date of the NIS Directive proposal (2013) or the date of its adoption from the European

Parliament and the Council of the EU (2016), Finland had a Cybersecurity Strategy already in place.[1] The first cross-administrative strategy (Strategy for Securing the Functions Vital to Society) was presented in 2003. In January 2013, Finland's Cyber Security Strategy was published. While the Security Committee decided on March 14th, 2016, to update the Implementation Programme for Finland's Cyber Security Strategy 2017–2020. The early adoption of national strategies related to cybersecurity issuess was therefore supported by the adoption of a corresponding national legislative and governance framework. Therefore Article 7 of the NIS Directive transposition displays a low misfit regarding Finland's strategic.

Sectoral supervisory authorities were already present in Finland through sectoral legislations. Even so, they were not designated as competent authorities for the OES, as the designation of entities operating in critical sectors as OES was not done in the same way. The only exception was the designation of the Financial Supervisory Authority as competent authority for the financial market infrastructures. Therefore Finnish policy fits with National competent authorities' provisions of Article 8, para. 1 of the NIS Directive. But this is not true for the following provision of the NIS Directive on monitoring the application of this Directive at national level (Article 8, para. 2 of the NIS Directive). The NIS policy being newly implemented at EU level, the introduction of new obligations related to this policy was then deemed necessary for the competent authorities as also for the single point of contact (Article 8, para. 2 and 4 of the NIS Directive). The Finnish Transport and Communications Agency already had the role of single point of contact under its ancient denomination as *Finnish Communications Regulatory Authority (FICORA)* (Article 8, para. 3 of the NIS Directive). The current tasks of FICORA's CERT function are largely the same as those of a CSIRT but are not limited to the scope of the NIS Directive.

Since the Governmental Decision of 2008 amending the Act of December 18th, 1992, on Ensuring Security of Supply (1390/1992), Finland's had established precautionary measures to ensure the continuous functioning of the society and of critical production. Energy transmission and distribution networks, Electronic information, and communication systems (e.g., Information networks and systems or financial systems), Transport logistics systems, Water supply and other public utilities, Construction and maintenance of infrastructure, Food security, Energy production and Healthcare, figured among the sectors and services being deemed to be critical. A designation which fits with the essential services identification criteria and list under the NIS Directive. We should bear in mind that all these legislations date prior to the NIS directive proposal except for the Transport Services Act (2017) and the Financial Supervisory Authority Act (2017).

Concerning the significant disruptive effect of an essential service, Finland's does not provide specific criteria for all sectors. However, it is stated within the Governmental Decision of 2008 amending the Act of December 18th, 1992, that "*the most critical and key functions of society that rely on information technology must be identified and the related information system solutions and services must be ensured by arrangements*

[1] It should be reminded that NIS security is part of Cybersecurity matters.

that can withstand various serious disruptions and exceptional circumstances"[1]. If we take for example the Electricity Market Act, in its version prior to 2018's amendments, it was already stated in section 29a on the obligations of the network operator to co-operate in the event of disruption that "*in the event of a disruption, the network operator shall participate (...)*"[2]. The term *disruption* was thus already figuring in the Finnish legislative framework. A situation which fits with Article 6 of the NIS Directive. A non-publicity upon the identification thresholds does not necessarily entail a misfit. The majority of OES obligations upon risk management and incident notification were introduced in Finnish sectoral legislations. While measures to prevent and minimise the impact of incidents and cross-border notification were already present.

Summarising the observations, the hypothesis of the present study on policy misfit has been confirmed in Finland only for Articles 8§2, 15§2 and 15§4 of the NIS Directive. Those provisions are related to the monitoring, implementation and enforcement power of the competent authorities (**Appendix 20**: Policy Misfit in Finland).

2. France

France approach on NIS strategy follows the same paradigm as Finland with a low misfit value. France already has a policy in place upon critical infrastructures, as well as a competent cybersecurity authority (ANSSI).[3] However, France has made the choice to distinguish critical infrastructures from NIS Policy. Therefore, the majority of the NIS Directive's requirements on OES identification, risk management and incident notification were newly introduced in the French legislative framework.The only exceptions were the tasks of the French Cybersecurity Authority, ANSSI, which acts as competent authority for all OES and DSPs and as single point of contact and disposes of an integrated CSIRT. Most of the tasks provided by the NIS Directive figured already in the Decree n° 2009-834 of July 7th, 2009, which was then modified to adapt it to newly introduced NIS Policy.

Summarising the observations, the hypothesis of the present study on policy misfit has been confirmed in France for most of the provisions of the NIS Directive. Those provisions are related to the OES designation, security measures and incident notification, as well as the enforcement powers of the competent authority (**Appendix 21**: Policy Misfit in France).

[1] Kriittisimmät ja keskeisimmät tietotekniikan varassa olevat yhteiskunnan toiminnot tulee tunnistaa ja niihin liittyvät tietojärjestelmäratkaisut ja -palvelut tulee varmistaa erilaisia vakavia häiriöitä ja poikkeusoloja kestävillä järjestelyillä.

[2] Verkonhaltijan on toimittava häiriötilanteissa häiriöiden poistamiseksi ja niiden vaikutusten rajoittamiseksi yhteistyössä muiden sähköverkonhaltijoiden ja toiminta-alueensa pelastusviranomaisten, poliisin, kuntien viranomaisten ja tieviranomaisten sekä muiden yhdyskuntateknisten verkkojen haltijoiden kanssa.

[3] Interview 2

3. Greece

Greece has entirely introduced NIS Directive provisions resulting in a high overall policy misfit (Table). There were digital strategies prior to NIS Directive adoption but none of them was relating to cybersecurity matters.[1] Furthermore, the Presidential Decree 39-2011 was established since procedures related to the designation of European critical infrastructures according to Council Directive 2008/114/EC of December 8th, 2008. But it was limited only to a few entities in the field of energy and transport. In other words, Greece did not *take the chance* to further develop the potential offer by the Council Directive 2008/114/EC to other sectors. The same goes for the Communication of the European Commission on Critical Information Infrastructure Protection, COM(2009)149. A situation which explains the introduction of most NIS Directive's provisions. Concerning the national competent authority, this has been explicitly created for the purposes of the Directive. The only exception is the national CSIRT which has been attributed to the Cyber Defence Directorate of the General Staff of National Defence. An entity already in place at the time of the NIS Directive proposal. However, its tasks had to be adapted to the NIS Directive, which resulted in an introduction of the NIS Directive provision on CSIRTs with Greek law 4577/2018 (**Appendix 22**: Policy Misfit in).

4. Ireland

Ireland's first National Cyber Security Strategy was agreed by the Government and published in July 2015 and covers the period 2015 to 2017. Contrary to France and Finland, Ireland made the choice to introduce in its national legislation Article 7's requirements of the NIS Directive on NIS strategy.

Furthermore, the National Cyber Security Strategy was setting out a road map for the development of the National Cyber Security Centre (NCSC), which was established in 2011. The NCSC contains the State's national/governmental Computer Security Incident Response Team (CSIRT-IE), which was instituted in 2013. With the transposition of the NIS Directive, the CSIRT-IE became the single point of contact and national CSIRT. While the NCSC became the competent authority for the OES, except for the Banking and financial market infrastructure sectors. Designation of the NIS Governance in Ireland and tasks attribution were made through the Statutory Instrument 360/2018 implementing the NIS Directive. Finally, a CIIP or similar programmes were not in place at the time of the NIS Directive transposition. Which may once again explain the high degree of policy misfit in Ireland (**Appendix 23**: Policy Misfit in Ireland).

[1] Interview 3

5. Luxembourg

The National Cybersecurity Strategy of Luxembourg was announced by the Ministry of Justice in 2012, while an amended version of this Strategy was approved by the government in 2015, even though those strategies were related to democratising information security by promoting collaboration while reducing complexity and costs for all stakeholders. Luxembourg also made the choice to integrate the provisions of Article 7 of the NIS Directive contrary to Finland and France.

While the ILR and the CSSF were already in place at the time of the NIS Directive proposal, the Grand-Duchy's legislator made the choice to designate competent authorities in matters of network and information system security which are different according to the sector concerned: the CSSF has competence for the financial sector (including digital service providers to this sector), while ILR will deal with other sectors. Furthermore, the Law of May 28th, 2019, made of the ILR the single point of contact. However, the same is not true for the national CSIRT. As the CSIRT function is already performed by the Governmental Computer Emergency Response Team (GovCERT) and the Luxembourg Computer Incident Response Centre (CIRCL) responsible for incident management. Finally, a CIIP or similar programmes were not in place at the time of the NIS Directive transposition. Which may once again explain the high degree of policy misfit in Luxembourg (**Appendix 24**: Policy Misfit in Luxembourg).

6. Poland

Published in 2010, the *Polish Cyber Protection Program 2011-2016* was currently the most important document planning actions related to the Polish cyberspace. However, the first national cyber security strategy, entitled "*Cyberspace protection policy of the Republic of Poland*" was launched in 2013. While addressing almost all issues related to the NIS policy, the NIS strategy requirements of the NIS Directive were still introduced as such by the National Cybersecurity System Act (NCSA) of July 5th, 2018.

Concerning the NIS Governance framework, Poland followed the same sectoral approach as Finland (Article 41 of the NCSA). But contrary to Finland, Poland made the choice to appoint those responsibilities to Ministries and not Agencies, as Finland did. A situation which is interesting, since all Ministries were in place upon NIS Directive adoption. The Government Morawiecki was formed on December 11th, 2017, and ended on November 15th, 2019. Therefore, any change to Ministries would have already been made. However, Poland decided to introduce a new rule upon competent authorities' designation and responsibilities under the NIS Policy. Same thing goes for the single point of contact, appointed to the Ministry of Digital Affairs, with Article 49 of the NCSA; the national CSIRT tasks with the Chapter 6, Articles 26 to 36 of the NCSA; the OES designation with Chapter 2, Articles 5 to 7 of the NCSA; and the OES security measures and incident notification with Chapter 3, Articles 8 to 16 of the NCSA.

This high misfit with the NIS Policy in Poland is particularly interesting as the country had introduced in its national legislative order a Critical Infrastructure Policy with the Act of April 26th, 2007 on crisis management.[1] Those critical infrastructures were including systems for a) energy and fuel supply, b) communications and ICT networks c) financial, d) food and water supply, e) health protection, f) transport and communication, g) rescue, h) ensuring the continuity of public administration, i) production, storage, storage and use of chemical substances and radioactive substances, including pipelines of hazardous safe substances. Those provisions were also followed by protection measures. It worth noting that with such a transposition, Poland should have followed the same sectoral and low policy misfit approach as Finland, which was not the case (**Appendix 25**: Policy Misfit in Poland).

Summarising the comparative observations on testing the policy misfit hypothesis in the six selected case studies we end up with the following findings (**Appendix 26**: Cross Countries Policy Misfit Analysis). While hypothesis H1 is confirmed for France, Greece, Ireland, Luxembourg, and Poland, it is not the case for Finland, where the hypothesis was barely confirmed. Articles 8§5 al. 1 and 9 §2 on ensuring adequate resources for competent authorities, the single points of contact, and the CSIRT,[2] presented important inconsistencies among case studies. Therefore, they will be overshadowed by the final results; as they do not allow to draw up conclusions on common trends.

It is interesting to mention that it has not been possible to find a plausible theoretical explanation for this result. Netiher the concept of *Falkner et al.* on world of compliance,[3] nor the idea of Börzel on "leaders" and "laggards" in Europe are providing a theoretical explanation.[4] France, Greece, Ireland, Luxembourg, and Poland confirmed the policy misfit hypothesis test while they are belonging to different worlds of compliance. France, Greece and Luxembourg belong to the world of transposition neglect. While Ireland and Poland belong to the world of domestic politics and world of dead letter respectively. It is however possible to argue that the common tendency to non-compliance for France, Greece, Ireland, Luxembourg and Poland is a factor for confirming the hypothesis test for these countries. Since on time and correct (even where conflicting domestic) transposition is a central factor for the world of law observance to which, Finland is belonging. We should remind that Finland was the only Member State of the six case studies that transposed on time the NIS Directive and that, without receiving a forma notice (Art. 258 TFUE) from the Commission.

[1] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r. Nr 89, poz. 590

[2] A criterion for which it is believed that hypothesis assessment of administrative effectiveness will help explaining Article 8 §5 al. 1 implementation.

[3] G. Falkner and O. Treib, 'Three Worlds of Compliance or Four? The EU15, Compared to New Member States', (2007) *Political Science Series* 112, Institute for Advanced Studies: Vienna, 22; G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States*, (Cambridge University Press, 2005)

[4] T. A. Börzel, *Environmental Leaders and Laggards in Europe: Why there is (not) a 'Southern Problem'* (Aldershot, UK: Ashgate, 2003).

From a non-theoretical perspective, a second relevant explanation for this outcome may be the centralised versus sectoral implementation approach and more particularly, the appointment of implementation responsibilities to Agencies. France, Greece, Ireland and Luxembourg have followed a centralised approach by appointing the implementation duties to one central agency for all sectors falling within the scope of the NIS Directive. While Poland followed the same sectoral approach as Finland. Poland made however the choice to appoint those responsibilities to Ministries and not sectoral Agencies, as it was the case in Finland. The combined choice between a sectoral or centralized approach for the implementation of the directive may affect the transposition outcome and more particularly, the degree of policy misfit with the NIS Directive. Indeed, as it has been already explained, policy misfit is dependent on the policies already in place at the time of the directive transposition. In the case of the network and information systems security, Finland was already pursuing a sectoral regulatory approach throughout sectoral agencies. An approach which was repeated upon NIS Directive transposition.

B. Institutional Misfit

For the need of the present study, it has been argued that the higher the degree of corporatism, the greater the extent of the modifications by Member States and the divergences upon transposition outcome. *Siaroff* was the first to construct an index of corporatism.[1] By summarising the debate up to the late 1990s, *Siaroff* argues "*that an ideal type of corporatism involves structural features, functional role, behavioural patterns and favourable context*"[2]. However, *Detlef* turns to a concept of corporatism, which "*analytically separates the scope of corporatist agreements from organisational structures and the functional role in relation to the state*"[3]. The advantages of *Deltlef's* classification[4] are that he combines the insights of 42 countries covering the post-war period from 1960 to 2010 (**Appendix 27**: Average ranks and scores of corporatism in 42 countries).

For the purposes of the present thesis, I have classified the average scores from *Deltlef's* classification as follow. Negative average scores were accounted as low degree of corporatism. From the positive average scores, I have considered values between 0.09 and 0,96 as medium degree of corporatism. While average scores from 0.97 to 2.06 were accounted as high degree of corporatism. On Deltlef's scale, Finland has an average score of 0.99 which is the highest score of the six countries considered by the present study. Greece is almost as high as Finland with a score of 0.43. While Luxembourg and France have almost the same value near zero (0.24 and -

[1] See A. Siaroff, 'Corporatism in 24 industrial democracies: Meaning and measurement', (1999) 2 *European Journal of Political Research* 36

[2] *Ibid*

[3] See J. Detlef, 'Changing of the guard: trends in corporatist arrangements in 42 highly industrialized societies from 1960 to 2010', (2016) 1 *Socio-Economic Review* 14

[4] On an average scale between -1.65 and 2.06, higher values indicate a higher level of corporatism.

0.23 respectively). France's average score is however a negative value, which places it fourth after Luxembourg.[1] Both Ireland and Poland are found at the lower end of the scale. Ireland has a negative score of -0.46 and Poland a score of -1.03 (**Table 40**).

Average ranks and scores of corporatism in 6 selected case studies (indices are z-standardized)				
Rank	**Country**	**Mean**	**Years covered**	**Degree of Corporatism**
7	*Finland*	*0.99*	*1960- 2010*	*High*
13	*Greece*	*0.43*	*1974- 2010*	*Medium*
14	*Luxembourg*	*0.24*	*1960- 2010*	*Medium*
22	*France*	*-0.23*	*1960- 2010*	*Low*
25	*Ireland*	*-0.46*	*1960- 2010*	*Low*
37	*Poland*	*-1.03*	*1990- 2010*	*Low*

Table 40: *Average ranks and scores of corporatism in 6 selected case studies*

(Table made by author)

Based on the extent of usage of *discretionary room* from the six Member States studied here, the results upon corporatism relational hypothesis is mitigated. Following the hypothesis test's findings, the hypothesis is only confirmed for the case of Greece and Luxembourg. Both countries had a high or relatively high degree of corporatism and were followed respectively by a high and a medium degree of transposition extent. On the other hand, the two Member States placed at the extremities of the corporatism scale, Finland and Poland are not confirming the hypothesis test, as they present contradictory scores of usage of regulatory leeway upon transposition. A high corporatism with a low score of transposition extent for Finland and *vice versa* for Poland. France and Ireland also failed the hypothesis test, as both presented a low average degree of corporative followed by a medium score of transposition extent (**Tables 41 and 42**).

[1] Always among the six countries considered by the present study.

Member States	Extent of Usage of 'Discretionary Room'		
	Low	Medium	High
Finland	8	6	2
France	4	6	6
Greece	1	7	8
Ireland	2	10	4
Luxembourg	1	11	4
Poland	1	4	11

Table 41: *Extent of Usage of 'Discretionary Room'*

(Table made by author)

Institutional Misfit			
H2: *The higher is the degree of corporatism, the greater the extent of the modifications will be by Member States and the divergences upon transposition outcome.*			
Member State	**Degree of Corporatism**	**Extent of Usage of 'Discretionary Room' (highest score)**	**Hypothesis Test**
Finland	High	Low (8)	Rejected
France	Low	Medium (6)	Confirmed
Greece	Medium	High (8)	Confirmed
Ireland	Low	Medium (10)	Confirmed
Luxembourg	Medium	Medium (11)	Confirmed
Poland	Low	High (11)	Rejected

Table 42: *Institutional Misfit Results*

(Table made by author)

The hypothesis H2 on institutional misfit can be therefore considered as not validated. The degree of corporatism is not a common factor of influence on the extent of regulatory leeway usage by Member States as expected. Consedering again the theoretical approach of *Falkner et al.* on the worlds of compliance.[1] In the countries forming the world of neglect, those domestic actors that are calling for more obedience have even less of a sound cultural basis for doing so than in the world of domestic politics, where EU recommendations are

[1] G. Falkner and O. Treib, 'Three Worlds of Compliance or Four? The EU15, Compared to New Member States', (2007) *Political Science Series* 112, Institute for Advanced Studies: Vienna, 22; G. Falkner, O. Treib, M. Hartlapp and S. Leiber, *Complying with Europe: EU Harmonisation and Soft Law in the Member States*, (Cambridge University Press, 2005)

incorporated into domestic law if they fit in with the agendas of important political actors at the domestic level. For example, France, Greece and Luxembourg belong to the world of neglect. A positif degree of corporatism should have not influenced further the usage of the regulatory leeway provided by the NIS Directive. However, this was not the case for the three Member States of the EU, since higher was the degree of corporatism greater was the extent of the usage of the regulatory leeway. In the cas of Ireland, which belongs to the world of domestic politics, the presence of a high degree of corporatism should had influenced the extent of the regularoty leeway usage. The hypothesis test in Ireland confirms the application of this theoretical approach.

The case of Finland is much more interesting. According always to *Falkner et al.* Finland belongs to the world of law observance. As such, culture of good compliance works as a self-reinforcing social mechanism, that interrelates cultural and actor-related expectations and cost–benefit calculations. The well-established regulatory framework in Finland led the Government to formulate adaptations which was in line with all stakeholders' expectations for compliance.

Poland also shared a well-established regulatory framework with Finland. Even if Poland, who belongs to the world of dead letter, have failed to validate the hypothesis test, mosty due to the fact that the extent of the usage of the regulatory leeway was two times greater than the degree of corporatism. The expectations of national stakeholders for compliance, mostly motivated by cost-benefit calculation, may constitute a plausible explanation.

It stems from the above consideration that the variable of institutional misfit should be seen as a combination of behavioral factors. The capacity of the national society to force the adaptation upon directives transposal should be considered alongwih the expectation of the society for compliance. An expectation that should be measured on the base of a well-established regulatory framework at the time of the transposition and the cost-benefit calculations that may result from a such regulatory framework.

It should be reminded that the transposition of the NIS Directive involves a shift towards a more formal type of regulatory relationship in certain key industries.[1] No mandatory consultation is necessary within the framework of the NIS Directive's transposition. However, Member States of the EU such as France or Greece adopted regulatory texts that provide sectoral measures of a technical nature. In doing so, they had to be subject to certain mandatory consultations, regarding the security measures applicable to OES. Informal consultations with potentially nominating OES and DSP's have also been carried out. The capacity for national private stakeholders of affecting the transposition outcome should not be overlooked.

[1] Interview 5

C. Administrative Effectiveness

The administrative effectiveness hypothesis seeks controling the existence of an effective administration may (or not) hamper the transposition outcome. Administrative effectiveness has been operationalised using the *government effectiveness* indicator initially developed by *Kaufmann et al*.[1] The indicator captures "*perceptions of the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and transposition, and the credibility of the government's commitment to such policies*"[2]. The 2017 version of this indicator will be used, which is the newest (**Appendix 28**: 'Government effectiveness' indicator). The country score is ranged from -2.5 to 2.5.

Following Worldwide Governance Indicators, all six Member States present a high administrative effectiveness (**Table 43**). However, out of the six Member States, Greece and Poland show slightly lower scores than the other four. All six countries show well above zero, while Greece and Poland show above the EU average.

	Government Effectiveness Score											
Country/Territory	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**10years Average**
Finland	*2,23*	*2,23*	*2,24*	*2,22*	*2,17*	*2,00*	*1,81*	*1,83*	*1,94*	*1,98*	*1,93*	***2,05***
France	*1,48*	*1,43*	*1,36*	*1,34*	*1,48*	*1,40*	*1,44*	*1,41*	*1,35*	*1,48*	*1,38*	***1,41***
Greece	*0,62*	*0,56*	*0,51*	*0,32*	*0,46*	*0,40*	*0,26*	*0,23*	*0,31*	*0,34*	*0,41*	***0,40***
Ireland	*1,34*	*1,35*	*1,46*	*1,55*	*1,49*	*1,60*	*1,53*	*1,33*	*1,29*	*1,42*	*1,28*	***1,42***
Luxembourg	*1,75*	*1,72*	*1,75*	*1,67*	*1,63*	*1,65*	*1,72*	*1,69*	*1,68*	*1,78*	*1,73*	***1,71***
Poland	*0,53*	*0,64*	*0,62*	*0,68*	*0,72*	*0,83*	*0,80*	*0,71*	*0,64*	*0,66*	*0,60*	***0,68***
EU average (with the UK)	***1,081***	***1,088***	***1,073***	***1,080***	***1,095***	***1,086***	***1,092***	***1,062***	***1,048***	***1,049***	***1,041***	

Table 43: *Government Effectiveness Score for selected case studies*

Source: *World Bank (https://databank.worldbank.org/source/worldwide-governance-indicators#)*

The fit between the levels of administrative effectiveness and the transposition outcome is interesting. Since read in both ways, the hypothesis can be confirmed in all six cases. The two countries with low scores of administrative effectiveness, Greece, and Poland, also show high scores of transposition extent. While the rest of the countries, Finland, France, Ireland, and Luxembourg have high scores of administrative effectiveness and have low scores of transposition extent.

[1] D. Kaufmann, A. Kraay and M. Mastruzzi, 'Governance Matters VI: Governance Indicators for 1996–2006', (2006) *World Bank Policy Research Working Paper* 4280

[2] See D. Kaufmann, A. Kraay and M. Mastruzzi, 'The worldwide governance indicators: methodology and analytical issues', (2011) 2 *Hague Journal on the Rule of Law* 3

Administrative Effectiveness			
H3: *The higher the administrative effectiveness is, the lesser the extent of the modifications will be by Member States and the divergences upon transposition outcome.*			
Member State	**Administrative Effectiveness (10 years average)**	**Extent of Usage of 'Discretionary Room' (highest score)**	**Hypothesis Test**
Finland	2,05	Low (8)	Confirmed
France	1,41	Medium (6)	Confirmed
Greece	0,40	High (8)	Confirmed
Ireland	1,42	Medium (10)	Confirmed
Luxembourg	1,71	Medium (11)	Confirmed
Poland	0,68	High (11)	Confirmed

Table 44: *Administrative effectiveness results*

(Table made by author)

§2. Results Discussion

In the previous paragraph, the hypotheses formulated in Chap. 2 were tested. Findings showed that no hypothesis could be confirmed for all cases. The hypothesis on the administrative effectiveness (H3) could only be confirmed. It should be reminded that hypothesis H3 assesses the extent to which an effective administration may (or not) hamper the transposition result. This outcome confirms that transposition outcomes can be explained throughout a combination of factors. The following paragraph explains at first the country-specific transposition processes (**A**) before proceeding to cross-country transposition patterns (**B**).

A. Country-Specific Transposition Patterns

1. Finland

The proposal for transposing the NIS Directive was submitted to the Finnish Parliament (Eduskunta) on December 19th, 2017, by the Ministry of Transport and Communications. According to the proposal, Finnish legislation concerning information security has not been consolidated into a single law, but it is included in

several regulations concerning both public administration and certain private services providers'.[1] Therefore, obligations related to information security risk management include general administrative laws (e.g., Act on Public Access to Government Activities - 621/1999[2] or Personal Data Act - 523/1999),[3] general legislation on quality requirements or security obligations of services providers (e.g., provisions of the Information Society Act - 917/2014),[4] business risk management legislation (e.g., regulation of credit institutions' operational risk management) and disruption preparedness legislation (e.g., water utility emergency preparedness obligation).

The Government had indeed issued a decision on the securitisation of the country's supply (VNp 857/2013)[5] in accordance with section 2 of the Supply Security Act (1390/1992).[6] According to this decision, disruption of information and communication systems and networks, interruption of energy supply, serious disruption of the health and functioning of the population, and natural and environmental disasters had been defined as the main threats to the functioning of society. The decision divided critical infrastructure security as follows: Energy production, transmission, and distribution systems; Information and communication systems, networks, and services; Financial services; Transport and logistics; Water supply; Construction and maintenance of infrastructure and Waste management in special situations. Therefore, the Government stated in the proposal for transposing the NIS Directive that "*the security risk management obligations under existing legislation in the areas covered by the NIS Directive will be examined in more detail below*"[7]. The title of the proposal, "*the Government's proposal to Parliament to amend the laws related to the transposition of the European Union's Network and Information Security Directive*" and the transposition extent corroborate the negative result from the policy misfit hypothesis test. The existence of widely deployed legislation on critical sectors, among which also figures the information and communication systems and networks, led to a low degree of transposition intervenention. It should be reminded that only the energy and transports sectors were falling within the scope of the Council Directive 2008/114/EC on the identification and designation of European critical infrastructures (ECI). While the communication on extending the critical sectors to Information Infrastructure was published three months later.[8] The promotion of digitalisation and the insurance of digital security by improving the level

[1] Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta (HE 192/2017 vp), p. 10

[2] Laki viranomaisten toiminnan julkisuudesta (621/1999) 21/05/1999

[3] Henkilötietolaki (523/1999) 22/04/1999

[4] Tietoyhteiskuntakaari (917/2014) 07/11/2014

[5] Valtioneuvoston päätös huoltovarmuuden tavoitteista (857/2013) 05/12/2013

[6] Laki huoltovarmuuden turvaamisesta (1390/1992) 18/12/1992

[7] Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta (HE 192/2017 vp), p. 11

[8] European Commission, Communication on Critical Information Infrastructure Protection (CIIP) – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', 30 March 2009, COM(2009)149 final

of information security of services that are important to society and citizens, figured among the government's goals which justifies this early and widely developed policy.

The Finnish parliamentary Committee on Transport and Communications was charged on February 7th, 2018, to study the proposal[1] and presented its reports on April 3rd, 2018.[2] In its report, the Committee expressed the view that it might be appropriate to extend similar information security obligations to some other actors important for the functioning of society, such as service providers responsible for intelligent traffic control. But this opinion was not taken into consideration. The Committee also considered that the activities of FICORA's (now TRAFICOM) cybersecurity centre is particularly important for the overall security of society. Therefore, it should be ensured in the future that FICORA is also provided with sufficient resources to carry out and develop these tasks for the benefit of all sectors of society.Finally, the Committee proposed a new bill amending section 6 of the Act on the Licensing and Supervision Agency for the Social and Health Sector (669/2008). A bill which was approved on April 4th, 2018 by the Parliament on first reading along with the Government's amendments on sectoral laws.[3] After a second reading on April 10th, 2018[4] the Parliament submitted its response to the Government on April 13th, 2018.[5] The President of the Finnish Republic approved on May 4th, 2018[6] the bills contained in the Parliament's response to the government's proposal to amend the laws relating to the transposition of the European Union Directive on network and information security and ordered the entry into force of these laws on May 9, 2018.

During the legislative process and specially the Committee's work, 21 expert opinions were heard. Most of the opinions emanated from the national administration sector, including ministries and national regulatory agencies. While representantives from identified private sectors falling within the scope of the transposing bills (e.g. energy, transport, digital infrastructure or water) expressed their comments.[7] Elisa, a Finnish company specializing in telecommunications, acknowledged in its letter of March 1st, 2021 that "*the current Finnish*

[1] Eduskunta, Pöytäkirjan asiakohta PTK 2/2018 vp, Täysistunto, '7. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta', Keskiviikko 7.2.2018 klo 14.05—15.55

[2] Eduskunta, Pöytäkirjan asiakohta PTK 28/2018 vp, Täysistunto, '15. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta', Tiistai 3.4.2018 klo 14.00—16.34

[3] Eduskunta, Pöytäkirjan asiakohta PTK 29/2018 vp, Täysistunto, '11. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta', Keskiviikko 4.4.2018 klo 14.00—18.19

[4] Eduskunta, Betänkande KoUB 6/2018 rd, RP 192/2017 rd, 'Regeringens proposition till riksdagen med förslag till lagar om ändring av lagar som har samband med genomförandet Europeiska unionens av direktiv om nät- och informationssäkerhet', Kommunikationsutskottet, 8 May 2021

[5] Eduskunta, Eduskunnan vastaus EV 25/2018 vp, 'Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta', 29 January 2021, HE 192/2017 vp

[6] Valtioneuvosto, Tasavallan presidentin esittely 4.5.2018 TP 30/2018

[7] Eduskunta, Asian käsittelytiedot HE 192/2017 vp, 'Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta', 29 January 2021

legislation provides a sufficient framework for ensuring information security"[1]. A Finnish telecommunications group providing voice, data and television services (DNA) sent its own expert for a hearing to support the statement of the Finnish Federation for Communications and Teleinformatics (FiCom),[2] which supports the proposal as being in line with Sipilä's Government program[3] and considers provisions on the submission of incident reports and FICORA's procedures appearing to be appropriate.[4] Pursuing on corporatist opinions, the Finnet Association of the local telecommunications businesses stated that the sector of digital infrastructures was already regulated by the Information Society Act (917/2014) and that no further regulation was required. It has however supported the government's proposal to harmonise the regulation of digital services and further requested to add to FICORA's (now TRAFICOM) tasks the investigation of offenses and threats.[5] The Finnish Ports Association (Suomen Satamaliitto ry) requested further clarifications.[6] Finland's Intelligent Transportation Society (ITS)[7] considered that the proposal was not bringing significant new requirements to the industry, as information security issues have been part of the operation of various modes of transport as well as international agreements and legislation in the past. However, it was neglecting that urban street traffic, or the regional traffic control of the largest cities, which play a very important role in the functioning of the transport system were not figuring among the subsectors falling within the scope of the NIS Directive; and that road traffic control was not considered as an essential service.[8] After highlighting the important of maintaining a centralised legislation for the air transport sector, the Air Navigation Services of Finland (ANS Finland) supported the information security requirements including the Aviation Act (864/2014).[9] Finally, the Helsinki Region Environmental Services Consortium (Helsingin seudun ympäristöpalvelut -kuntayhtymä HSY) for the water sector highlighted "*the importance of defining within the law what should constitute a significant impact upon water supply within the meaning of section 15 b of the proposed Water Supply Act (290/2018); as*

[1] Security Director Jaakko Wallenius, Elisa Corporation Expert opinion, available at https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-173859.pdf (accessed on April 5th, 2021)

[2] DNA Oy Expert opinion, available at https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-173451.pdf (accessed on April 5th, 2021)

[3] It should be reminded that the Government program aims to promote the resilience of key societal functions in the face of various cyber threats.

[4] Lawyer Jussi Mäkinen, Confederation of Finnish Telecommunications and Information Technology FiCom ry Expert opinion, available at https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-174121.pdf (accessed on April 5th, 2021)

[5] Marko Vuorinen, General Counsel, Finnet Association Expert opinion, available at https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-174122.pdf (accessed on April 5th, 2021)

[6] Deputy Director Kirsti Tarnanen-Sariola, Finnish Ports Association Expert opinion, available at https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-174123.pdf (accessed on April 5th, 2021)

[7] Älykkään liikenteen verkosto ITS Finlandin

[8] Intelligent Transportation Society - ITS Finland Expert opinion, available at https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-175871.pdf (accessed on April 5th, 2021)

[9] Air Navigation Services Finland Oy (ANS Finland) Expert opinion, available at https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-175972.pdf (accessed on April 5th, 2021)

significant impacts in water supply must be limited and defined with sufficient precision by law to ensure uniform operation"[1]. It has furthermore noted that the law should provide "*the kind of information [that] should be provided in the notification (e.g., quality of the disturbance, time of occurrence of the disturbance, measures taken to eliminate the disturbance)*"[2].

Most of the opinions noted that the proposal was in line with the already in place regulatory framework created, for most sectors, following the Council Directive 2008/114/EC on the identification and designation of European critical infrastructures (ECI). However, neither the opinion of the Intelligent Transportation Society of Finland nor the one of the Region Environmental Services Consortium HSY were taken into consideration. As only the Operators of Intelligent Transport Systems were considered as OES and as no definition of the significant impact upon water supply was included by the respective amending bills. It should be mentioned, considering the latter, that the Government placed the responsibility for defining the significant impact thresholds by decree on the Ministry of Agriculture and Forestry.

2. France

In France, the transposition process for the NIS Directive was conducted in a quick and transparent fashion. In French constitutional law, the *fast-track* procedure or accelerated legislative procedure is the possibility of having a bill adopted after a single reading by the Chambers of Parliament (National Assembly then Senate), thus reducing the duration of the *parliamentary shuttle*. Provided for by article 45, para. 2 of the Constitution, it allows the Government since the constitutional reform of 2008[3] to shorten the parliamentary discussion on certain bills or proposals of law. At a first reading from the Senate on November 22nd, 2017[4] the Law 2018-133 transposing the NIS Directive was adopted in a mere 3 months. The *fast-track* procedure being initiated by the Government the proposed bill was debated after a first reading in both French Parliament's Chambers before an agreement was reached within a Joint Committee on February 6th, 2018.

[1] Helsinki Region Environmental Services Consortium of Experts Expert opinion, available at https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-176683.pdf (accessed on April 5th, 2021)

[2] *Ibid*

[3] Loi constitutionnelle du 23 juillet 2008 de modernisation des institutions de la Vème République, available at https://www.vie-publique.fr/loi/269792-loi-constitutionnelle-23-juillet-2008-de-modernisation-des-institutions (accessed on April 1st, 2021)

[4] Sénat, 'Projet de Loi (Procédure Accélérée) portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', *Présenté au nom de M. Édouard PHILIPPE, Premier ministre, Par M. Gérard COLLOMB, Ministre d'État, Ministre de l'Intérieur*, Texte n° 105 (2017-2018), déposé le 22 Novembre 2017

The impact assessment[1] clearly states that the country already has "*a national authority competent*" in matters of NIS security, the ANSSI, which acts as "*an authority for the defence and security of information systems*" and "*a security incident response and handling centre (CSIRT)*". There are moreover provisions in national law intended to strengthen the security of the information systems for electronic communications operators[2] and the operators of vital importance (OVI).[3] Considering however that the directive excludes, on the one hand, the electronic communications sector from its scope, because it is already the subject of equivalent European regulations in this area; and that the framework applicable to operators of vital importance is based, on the other hand, on legal foundations and pursues purposes different from those of the directive which the bill intends to transpose.[4] It has been considered therefore that in the absence of applicable provisions in national law the transposition of Chapter V of the Directive should be operated through the adoption of new legislative provisions applicable to essential service operators and to digital service providers.[5]

M. Christophe Euzet, Member of the National Assembly, confirmed it in a report (n° 530) published on 17 January 2018 on behalf of the Commission for Constitutional Laws, Legislation and General Administration of the French Republic. M. Euzet wrote that, "*depending to the information systems concerned, some companies are likely to meet both the definition of OVI and that of OSE. . . OVIs being subject to particularly strict rules on information system security, which do not necessarily appear justified for all business information systems and networks*"[6]. Therefore, the policy misfit is justified by the necessity of preserving national security interests related framework, which is of a national prerogative and should be not combined with EU's NIS security matters. This despite the preference mentioned in both the impact study of the bill and in legislative debates "*to avoid gold plating*"[7].

According to impact assessment relating the transposition of the NIS security framework, it has been considered that ANSSI "*will be able to rely on the means already put in place for the system relating to*

[1] Gouvernement, Etude d'Impact relative au 'Projet de Loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', 17 Novembre 2017, INTX1728622L/Bleue-1, p. 13

[2] Articles L. 33-10, L. 33-1, and D. 98-5 of the 'Code des postes et des communications électroniques', which transposes the Directive 2002/21 / EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24.4.2002, p. 33–50

[3] Articles L. 1332-6-1 and following of the 'Code de la défense', introduced by the 'Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n°0294', pp. 13-14

[4] Interview 2

[5] Gouvernement, Etude d'Impact relative au 'Projet de Loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', 17 Novembre 2017, INTX1728622L/Bleue-1, p. 18

[6] Assemblée Nationale, 'Rapport sur le projet de loi, adopté par le Sénat après engagement de la procédure accélérée, portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (n°530)', par M. Christophe EUZET – Député, 17.02.2018, available at https://www.senat.fr/dossier-legislatif/pjl17-105.html (accessed on April 1st, 2021)

[7] Over-transposition in French: '*surtransposition*'.

operators of vital importance. However, depending on the number of essential service operators potentially affected by the new system, additional human resources may be necessary"[1]. Furthermore, it has been considered that "*the ministries which oversee the sectors of the activity concerned, (...), will naturally be involved, in relation with ANSSI, in the transposition of this new system. However, this will only generate a marginal workload for the ministries concerned*". Therefore, neither in the rapport of the Senate[2] nor in the one of the National Assembly[3] was the question of the NIS Governance framework addressed further. The existence of a wide administrative structure like ANSSI, with 500 agents dispersed across 5 branches, confirm the test of the administrative effectiveness hypothesis.

3. Greece

In Greece, the transposition process for the NIS Directive was conducted in a quick and transparent fashion, as Law 4577/2018 was adopted in a mere 10 days from the deposit of the bill to the Greek Parliament.

The European Commission published a Communication on Critical Information Infrastructure Protection (CIIP) in 2009, "*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*"[4]. However, Greece did not have any similar policy already in place at the time of the NIS Directive adoption. The reasons may be related to the national economy. As it must be reminded that the public deficit climbed in 2010 to 12.7% of GDP and it is only after the consolidation of its public finances in 2018, that the country resumed regular refinancing on the markets.

When Law 4577/2018 was adopted, the report of the General Accountant of the Hellenic State refered to possible expenditure from any measures taken for the transposition of the National Cyber Security Authority, preparedness measures, education and training programs, supply of the competent service with the appropriate infrastructure, equipment and personnel.[5] However, the amount of this expenditure is not specified. The

[1] Gouvernement, Etude d'Impact relative au 'Projet de Loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', 17 Novembre 2017, INTX1728622L/Bleue-1, p. 23

[2] Sénat, 'Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le projet de loi (Procédure Accélérée) portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', M. Philippe Bonnecarrère, Sénateur, N° 161, 13.01.2017

[3] Assemblée Nationale, 'Rapport sur le projet de loi, adopté par le Sénat après engagement de la procédure accélérée, portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (n°530)', par M. Christophe EUZET – Député, 17.02.2018

[4] European Commission, Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', 30 March 2009, COM(2009) 149 final.

[5] Interview 3

rapporteur of the New Democray Party, Andreas Katsaniotis,[1] stated during the joint meeting of the Standing Committee on Public Administration, Public Order and Justice, and the Standing Committee on Production and Trade on November 15th, 2018 that

> "*according to the joint statement of 4/5/2018 of the Vice President Mr. Ansip and the Commissioners Mr. Avramopoulos and King, and Mrs. Gabriel, according to the new Cyber Security rules at EU level, so that the Member States can quickly transfer the NIS Directive in their national law and to develop their capabilities, the program of the mechanism, connecting Europe, provides the funding of 38,000,000 euros by 2020 to support national CSIRTs as well as other stakeholders under the NIS Directive, such as essential service operators and digital service providers. The aforementioned joint statement also emphasises that Member States should make the most of the opportunities provided by this source of funding*"[2].

While the bill for the transposition of the NIS Directive was followed by an explanatory memorandum, a session report from the Commission of the Hellenic Parliament, as well as a report on the scientific service of the Hellenic Parliament, there was no mention of the current situation in Greece prior to the NIS Directive adoption. Therefore, it may be considered that the absence of a similar policy followed by the provision of financial incentives from EU have forced Greece to introduce as such the NIS Directive's provisions into its national law order. The adoption of Law 4577/2018 transposing the provisions of the NIS directive intended thus mostly to comply with EU law.

4. Ireland

The transposition process in the Republic of Ireland offers a particularity which is interesting to highlight. As it has been mentioned above, the transposition of the NIS Directive was made using a Statutory Instrument. Under the Statutory Instruments Act 1947[3] a statutory instrument is defined by the Republic of Ireland as being

[1] It should be noted that the New Democracy Party is not part of the Government during this period. However, the statements of the rapporteur were not refuted by the responsible Minister who was present during the joint meeting.

[2] Βουλή των Ελλήνων, 'Επεξεργασία και εξέταση του σχεδίου νόμου του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης "Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση"', Διαρκής Επιτροπή Δημοσίας Διοίκησης, Δημόσιας Τάξης και Δικαιοσύνης Και η Διαρκής Επιτροπή Παραγωγής και Εμπορίου, Εισηγητές: Αναστασία Γκαρά και Ανδρέας Κατσανιώτης, 15.11.2018

[3] Statutory Instruments Act, 1947, Number 44 of 1947

"*an order, regulation, rule, scheme or bye-law made in exercise of a power conferred by statute*". Therefore, a statutory instrument is a form of secondary law.[1]

Statutory Instruments have a wide variety of functions. They may allow persons or bodies – to whom legislative power has been delegated by statute – to legislate in relation to detailed day-to-day matters arising from the relevant primary legislation. Statutory instruments are used, for example, for transposing European Council Directives of for delegating the powers of Ministers. This explains why no legislative process could be found and why it is stated at the beginning of S.I. 360 of 2018 that, "*I, DENIS NAUGHTEN, Minister for Communications, Climate Action and Environment, in exercise of the powers conferred on me by section 3 of the European Communities Act 1972 (No. 27 of 1972) and for the purpose of giving effect to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, hereby make the following regulations*".

Following Section 3 of the European Communities Act 1972, a Minister of State may make regulations to give full effect to "*treaties governing the European Communities and the existing and future acts adopted by the institutions of those Communities*" and make them thus part of domestic law. The Communication of the European Commission on Critical Information Infrastructure Protection (CIIP)[2] being not a binding act requiring from the Republic of Ireland to give full effect, it could be understood why there was not a CIIP or similar policy in place. Therefore, the binding effect of an EU's soft law instrument (e.g., communications) may influence the transposition extent of a future related directive, which was confirmed in the case of the Irish transposition of the NIS Directive. As it has been transposed by introducing mostly new rules in the Irish national legal order.

5. Luxembourg

Bill transposing the NIS Directive and amending 1° the amended law of April 20th, 2009, establishing the Information Technology State's Centre and 2° the law of July 23rd, 2016, establishing a High Commission for National Protection, was deposited on the Deputies' Chamber of the Grand Duchy on June 6th, 2018. While a referral for an opinion[3] to the Council of State was made on September 5th, 2018. The legislative process lasted

[1] Revenu Legislation Services, 'Guide to the Legislative Process', May 2016, Dublin, Published by the Revenue Commissioners, RPC009237_EN_WB_L_1, available at https://www.revenue.ie/en/tax-professionals/documents/legislative-process.pdf (accessed on April 2nd, 2021)

[2] European Commission, Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', 30 March 2009, COM(2009) 149 final.

[3] (1) Chambre Des Députés, Session ordinaire 2017-2018, Projet de Loi No 73141 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, Avis Du Conseil D'Etat (10.7.2018); (2) Chambre Des Députés, Session ordinaire 2018-2019, Projet de Loi No 7314 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun

almost 12 months. The bill was amended twice by the Government (02/10/2018) as well as the Deputies (03/13/2019).

As in the case of Ireland, here also there was no CIIP[1] or similar policy in Luxembourg. It should be noted once again that the notion of OSE should not be confused with the notion of operator of a critical infrastructure (Opérateur d'infrastructures Critiques - OIC), as provided for by the law establishing a High Commission for National Protection, although partial overlaps cannot be ruled out and an entity could be considered both an OSE and an OIC. Therefore, the binding effect of an EU's soft law instrument (e.g., communications) may influence the transposition extent of a future related directive, which was confirmed in the case of the Luxembourg transposition of the NIS Directive. As it has been transposed by introducing mostly new rules in the Irish national legal order. It is also worth noting that the Bill was passed unanimously with 60 votes.[2]

According to the explanatory memorandum accompanying the submission of the bill,[3] it is recognised that

> "*the ILR already regulating a large part of these sectors at the national level, while having a confirmed expertise in regulation, as well as an independent status, it seems coherent to entrust to it the role of competent authority within the meaning of the NIS directive, with the exception of the banking and financial market infrastructure sectors, where the CSSF will remain the regulatory authority. Entrusting the task of competent authority to a new entity, foreign to the sectors defined in the NIS directive, would necessarily have resulted in interference with the powers of the existing regulatory authorities*".

Furthermore, it should be noted that "*the competence of ILR to carry out this new mission is confirmed all the more by its current competence in the field of electronic communications*".

---

de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, Avis Complémentaire Du Conseil D'Etat (27.11.2018); (3) Chambre Des Députés, Session ordinaire 2018-2019, Projet de Loi No 7314 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, Deuxième Avis Complémentaire Du Conseil D'Etat (26.04.2019).

[1] European Commission, Communication on Critical Information Infrastructure Protection – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', 30 March 2009, COM(2009) 149 final.

[2] Chambre des Députés du Grand-Duché de Luxembourg, Séance publique n° 24, Point d'ordre du jour n° 4, Compte rendu de la Séance (15.05.2019)

[3] Chambre des Députés, Session ordinaire 2017-2018, Projet de Loi N° 7314 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, Dépôt le 6.6.2018, p. 16

6. Poland

The bill for the transposition of the NIS Directive in Poland was submitted to the SEJM,[1] which is the lower house of the Parliament, on April 30th, 2018. The parliament of Poland is the bicameral legislature of Poland. It is composed of an upper house (the Senate) and a lower house (the Sejm). The Constitution of Poland does not refer to the Parliament as a body, but only to the Sejm and Senate. Compared to France and Luxembourg, the transposition process lasted 3 months.

Extensive documentation of the consultation processes, as well as documents on impact assessments and explanatory memoranda, are found on the site of the SEJM.[2] In the reasoned opinion of the Government following the bill submission to the SEJM, it is stated that at the time of the transposition of the NIS Directive the issues of securing ICT systems are regulated in Poland by sectors according to the tasks of various entities. These regulations regard the provision of an information security management system to public entities, combating cybercrime, preventing terrorist threats or crisis management. But none of these regulations addresses the problem. It is emphasised that "*the legal basis of Directive 2016/1148, which is Article 114 of the Treaty on the Functioning of the European Union, relating to the common market, is different*"; and that the protection of national critical infrastructure is an exclusive competence of Member States, closely related to the sphere of national security, not covered by the EU treaties. Furthermore, it is indicated that "*there are no provisions in Polish law aimed at establishing obligations in the field of risk management, application of safeguards, incident reporting and handling, or covering the provided services with a continuous monitoring system.' The bill transposing the NIS Directive aimed thus at providing the first document that 'comprehensively defines the principles of the national cybersecurity system*". The need for distancing national security interests as an individual state from the common market's interest as a Member State of the EU prevailed then in introducing new rules within the Polish legal order. However, the choice of creating a national cybersecurity system based on existing infrastructures explains the confirmation of the policy misfit hypothesis test. The extended amendments considered by the Digitisation, Innovation and Modern Technologies Committee and the National Defence Committee attest to this extensive transposition.[3]

Contrary to the other five countries, the bill was made available on the website of the Public Information Bulletin of the Ministry of Digital Affairs and on the website of the Government Legislation Centre, according to Article 5 of the Act of July 7th, 2005, on Lobbying Activities in the Law-making Process.[4] The consultations

[1] Rzeczypospolitej Polskiej. Available at http://www.sejm.gov.pl/ (accessed on April 3rd, 2021)

[2] SEJM Rzeczypospolitej Polskiej, Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa, druk nr 2505, 30.04.2018, available at http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2505 (accessed on April 3rd, 2021)

[3] SEJM Rzeczypospolitej Polskiej, 'Dodatkowe sprawozdanie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Komisji Obrony Narodowej o rządowym projekcie ustawy o krajowym systemie cyberbezpieczeństwa, Druk nr 2659-A, available at http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2659-A (accessed on April 3rd, 2021)

[4] Ustawa z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, Dz.U. 2005 nr 169 poz. 1414

took place from October 31 to November 21st , 2017.[1] The bill was thus sent to 34 entities for consultation and 58 for opinion. From those entities 44 submitted comments on the bill. From the 205 comments expressed 51 were taken in consideration, while 20 comments were partially considered and 134 were omitted.

Most of the proposals considered focused on the interest of protecting classified information, the extension of the entities' list authorised to request support from the CSIRT on serious incidents handling cooperation, removing *public universities* from the regulation, detailing the scope of the OES under local government structures, the person responsible for keeping the list of OES, the reporting process of incidents between national CSIRTs within the EU, on OES obligations and finally on the bill's wording. However, none of the 51 comments taken into consideration were transmitted by corporatist representatives (e.g., Polish Chamber of Maritime Economy or Liquid Fuels), while extensive modifications were made upon submitting the bill.

Following the explanatory memorandum comments on the governance framework states that the competences regarding cybersecurity may be exercised by the Minister of National Defence, the Head of the Internal Security Agency, the Minister of Internal Affairs and Administration, the Police, the Government Center for Security, or the Minister of Digitisation. Cyberspace protection system in Poland being decentralised, the above-mentioned entities perform tasks in the field of cybersecurity, combating cybercrime, preventing terrorist events and national defence.

B. Cross-Country Impact Analysis of Internal Factors on Transposition Patterns

Drawing from the above country-specific analysis of the transposition patterns, the purpose of the following developments will be to examine how internal factors – such as the transposition process, the existence of a well-established regulatory framework prior to transposition or even the expectation of the national stakeholders – have affected the transposition outcome across the 6 case studies. Analysis is presented by independent variables.

Regarding the policy misfit variable, the existence of widely deployed legislation in Finland on critical sectors, among which also figures the information and communication systems and networks, led to a low degree of transposition intervention. While the promotion of digitalisation and the insurance of digital security figured among the government's goals by improving the level of information security of services that are important to society and citizens. A situation which justifies this early and widely developed policy. It is

[1] SEJM Rzeczypospolitej Polskiej, 'Raport z konsultacji publicznych i opiniowania projektu ustawy o krajowym systemie cyberbezpieczeństwa', Druk nr 2505 cz. II, 30.04.2018, available at https://orka.sejm.gov.pl/Druki8ka.nsf/0/6624C41DF04E6186C1258287003D9163/%24File/2505%20cz%20II.pdf (accessed on April 3rd, 2021)

important to note however that this result is justified by the fact that the well-established regulatory framework in Finland led the Government to formulate adaptations which was in line with all stakeholders' expectations.

In France, the transposition process for the NIS Directive was conducted in a quick and transparent way. The impact assessment clearly states that the country already has *a competent national authority* on matters of NIS security, the ANSSI, which acts as "*an authority for the defence and security of information systems*" and "*a security incident response and handling centre (CSIRT)*". Therefore, the policy misfit is thus justified by the necessity of preserving national security interests related framework, which is of a national prerogative and should be not combined with EU's NIS security matters. And this, despite the preference mentioned in both the impact study of the bill and in legislative debates on avoiding "*gold plating*".

In the case of Greece, it may be thus considered that the absence of a similar policy followed by the provision of financial incentives from the EU have forced Greece to introduce as such the NIS Directive's provisions into its national law order. The adoption of Law 4577/2018 transposing the provisions of the NIS directive tended thus mostly to comply with EU law. Transposition process in the case of Ireland and Luxembourg revealed that the binding effect of an EU's soft law instrument (e.g., communications) may influence the transposition extent of a future related directive, which was confirmed in the case of the Irish transposition of the NIS Directive. It has been implemented by introducing mostly new rules in the Irish national legal order, while the need for distancing the national security interests as an individual state from the common market's interest as a Member State of the EU prevailed in introducing new rules within the Polish legal order. However, the choice of creating a national cybersecurity system based on existing infrastructures explains the confirmation of the policy misfit hypothesis test.

Regarding the institutional misfit, the preservation of the French national economy from considerable financial impacts also prevailed upon corporatism consideration, leaving enough discretionary room for the executive power. This is reinforcing the fact that the expactations of compliance based on cost-benefits calaculation has prevailed. An expacation which is shared by Finland which, a high degree of corporatism alongwith a low transposition extent rejected the Institutional misfit hypothesis test. It is important to note however that this result is justified by the fact that the well-established regulatory framework in Finland led the Government to formulate adaptations which were in line with all stakeholders' expectations upon compliance. This proves so in the case of Finland that even if the state displays a high score of corporatism, the adaptation of the private stakeholders to long lasting rules may reduce the need for the state to further add a whole set of new rules while similar rules are already present. It is possible to presume that defining minimal thresholds for the identification of the OES could confirm a possible presence of corporatism influence, which was confirmed by the institutional misfit hypothesis test in the case of Greece.

According always to the statement provided by the rapporteur of the New Democratic Party, Andreas Katsaniotis, to the joint meeting of the Standing Committee on Public Administration, Public Order and Justice, and the Standing Committee on Production and Trade, we infer that "*the bill was not put to public consultation,*

as the Ministry claimed". The fact that there was no modification seems to confirm this statement. A situation which does not coincide with the positive result of the institutional misfit hypothesis test, as Greece figures among the countries with the highest corporatism score. The only reasonable explanation is that of *patronage*. Takis S. Pappas and Zina Assimakopoulou's work on "*Party Patronage in Greece: Political Entrepreneurship in a Party Patronage Democracy*" shows indeed that the scope and reach of patronage in Greece has been the highest in Europe, and points to several state-related mechanisms that have facilitated such growth.[1] The introduction of new rules in the national law order using the same wording as the NIS Directive does not match however with patronage assertation during the legislative process, since the Hellenic Parliament adopted the bill without any amendment. The only point of influence would have been the OES identification criteria where theresholds were specificly defined in order either to limit or to enhance the extent of the transposition, as a high threshold entails low entries within the scope of the NIS Directive. The absence of a well-established regulatory framework in Greece on NIS security have thus led the Governement meeting the expectations of national stakeholder for compliance throught the leverage of the national cybersecurity awarness. To comply the Governenment "copy-pasted" the NIS directive provisions to meet compliance, lowering the cost of a non-compliance. But it has taken the in consideration the national stakeholders cost-benefit calculation by adaptating further the national law transposing the NIS Directive throughout ministerial decrees.

Concerning the French consultation processes with national stakeholders, the Movement of French companies,[2] insisted on the fact that "*most small and medium-sized enterprises were slow to put in place an ambitious policy in this area and to make the necessary investments*"[3]. However, the choice of maintaining a broader definition of the OES than that provided for by the directive, opened up to the executive power the possibility of extending the scope of the provisions of the law to a larger number of OES than what the directive provides. Which was finally done by extending the list of OES provided in the Annex II of the NIS Directive. Same thing with the security measures for the OES for which a *free of movements* has been opened up to the executive power. Taking into consideration the fact that "*the Government points out that the costs generated by an incident affecting the information systems generally turn out to be much higher than the costs incurred for protection devices*"[4], neither the Senate nor the National Assembly have amended this article of Law 2018-133. Thus, extensive measures have been adopted through Decree 2018-384 and the Ordinance of September 14th,

[1] See T. Pappas and Z. Assimakopoulou, 'Party Patronage in Greece: Political Entrepreneurship in a Party Patronage Democracy. In Party Patronage and Party Government in European Democracies', (Oxford University Press, 2012)

[2] Mouvement des entreprises de France – MEDEF

[3] Sénat, 'Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le projet de loi (Procédure Accélérée) portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', M. Philippe Bonnecarrère, Sénateur, N° 161, 13.01.2017, p. 11. Available at https://www.senat.fr/rap/l17-161/l17-1611.pdf (accessed on April 1st, 2021)

[4] Sénat, 'Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le projet de loi (Procédure Accélérée) portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', M. Philippe Bonnecarrère, Sénateur, N° 161, 13.01.2017, p. 11. Available at https://www.senat.fr/rap/l17-161/l17-1611.pdf (accessed on April 1st, 2021)

2018. Therefore, the preservation of the national economy from considerable financial impacts prevailed upon corporatism consideration, leaving enough discretionary room for the executive power.

Contrary to France and Greece, extensive documentation of the consultation processes, as well as documents on impact assessments and explanatory memoranda, can be found. Therefore, there are no documents able to give insights into the political context. Applying however a deductive reasoning it is possible to assert that, the unchanged transposition of the NIS Directive by the Irish Minister for Communications, Climate Action and Environment may not give place to any corporatist influence. Identifications criteria for the OES were maintained as such. Notification thresholds and proposed security measures figure in detail within a non-binding document, the "*NIS Compliance Guidelines for Operators of Essential Service (OES)*". Therefore, the unchanged transposition of the NIS Directive followed by the attribution of the transposition responsibility to the Minister for Communications, Climate Action and Environment confirm the hypothesis test result of the Institutional Misfit.

In the case of Luxembourg, it was not possible to find an announcement for public consultations. However, the publication of the opinions from the professional chambers during the transposition process reveals relevant information. In its opinion of August 29, 2018, the Chamber of Works (Chambre des Métiers) had no comments to make.[1] While the Chamber of Commerce issued its opinion dated November 14th, 2018.[2] In it, the Chamber of Commerce refers to the importance of faithfully transposing the directive according to the principle "*the whole directive, nothing but the directive*" in order to guarantee that Luxembourg companies are not faced with stricter obligations than those valid for companies in other Member States. Because, contrary to the obligations arising from the NIS Directive, Article 8, para. 3 of the Bill aims to impose on the OSE an additional burden of notifying to the competent authority of all the measures taken in terms of risk management or prevention of incidents. It states that, according to Article 8, para. 8 of the bills the competent authority is empowered "*requiring the OES to inform the public themselves of reported incidents and notifying the public of specific incidents where 'disclosure of the incident is to other respects in the public interest'*". A situation which constitutes a potentially significant risk for the OES in terms of commercial image to the public. Therefore, the corporate awareness upon their obligations as OES and DSPs prevailed on corporatism interests, which confirms once again that the society expectations for compliance pressured the government to adapt the transposition of the NIS Directive while observing compliance. Finally, extensive modifications were made upon submitted the Bill in Poland. But the existence of a well-established regulatory framework seems to support the idea of an adaptation based on the expectations of the national stakeholders to comply at the least cost.

Regarding the administrative effectiveness hypothesis test, the long-lasting governance framework of Finland in the field of information security led most sectoral agencies to develop significant knowledge on the

[1] Avis de la Chambre des Métiers, Dépêche du Directeur Général de la Chambre des Métiers au Premier Ministre, Ministre d'Etat (29.8.2018)

[2] Avis de la Chambre de Commerce sur le projet de loi et les amendements gouvernementaux y relatifs, (14.11.2018)

matter. Therefore, the existence of an effective administration capable of also supervising the transposition of the NIS Directive facilitates the choice of the Government to adopt a sectoral approach, while keeping a centralised governance for each sector. It is however worth noting that contrary to other Member States of the EU, such as France or Poland, the National Cyber Security Centre was occupying only 70 employees in 2017. While Finnish Communications Regulatory Authority – FICORA, which became TRAFICOM in 2019, today occupies almost 900 employees. A situation which proves that even with a small number of employees an administration may be more effective within a sectoral approach. Therefore, the transposition choice may also rely on the centralised approach which a state wishes to bring forward. Compared to the French ANSSI with 500 agents being dispersed across 5 branches, the Greek General Directorate of Cybersecurity is a part of the Ministry, which counts 366 employees and was established in 2016, while in France, the ANSSI counts approx. 500 employees and was established in 2009. The administrative effectiveness relies on the number of employees or the years of establishment for the responsible entity, factors which could thus affect the extent and technicity of the transposition which was confirmed by the administrative effectiveness hypothesis test. Contrary to France and Greece, the Republic of Ireland has chosen to transpose the NIS Directive provisions relying partially on services of the National Cyber Security Centre (NCSC) and to the Central Bank of Ireland. As in Greece, the NCSC is an operational arm of the Department of the Environment, Climate and Communications. However, the NCSC was founded in 2011 and counts 201-500 employees, contrary to the Greek General Secretariat of the Ministry of Digital Policy, Communication and Media which was founded in 2016 and counts almost 370 employees. Contrary to earlier states, the ILR and the CSSF count 11-50 employees and 501-1.000 employees respectively in Luxembourg. The number of employees does not correspond to the extent of the sector supervised by ILR. Therefore, the factor of the national interests should be taken in consideration along with the number of employees allocation, when determining the relationship between the administrative effectiveness and the transposition outcome. In Poland, along with the amendment of the Act of 4 September 1997 on government administration departments in December 2015, competences in the field of cybersecurity were assigned to the Ministry of Digital Affairs for undertaking activities related to the regulation of cybersecurity issues for the administration and for the entire civil part of the country.

	Cross Comparative Hypothesis Results		
	H1	**H2**	**H3**
Member States	*The higher the policy misfit is, the greater will be the extent of the modifications by Member States and the divergences upon transposition outcome.*	*The higher the degree of corporatism is, the greater will be the extent of the modifications by Member States and the divergences upon transposition outcome.*	*The higher the administrative effectiveness is, the lesser will be the extent of the modifications by Member States and the divergences upon transposition outcome.*
Finland	Rejected	Rejected	Confirmed

France	Confirmed	Confirmed	Confirmed
Greece	Confirmed	Confirmed	Confirmed
Ireland	Confirmed	Confirmed	Confirmed
Luxembourg	Confirmed	Confirmed	Confirmed
Poland	Confirmed	Rejected	Confirmed

Table 45: *Cross comparative hypothesis results*

(Table made by author)

***

In the introduction of part II, it was argued that Member States can perfectly be compliant with regulations, without their effectiveness being insured. Effectiveness may refer not only to compliance but also to transposition, enforcement, and impact. The obligation of transposition incumbent on the States is a condition of the effectiveness of EU law but the effectiveness of hard regulation to foster compliance, especially of those actors that face heavy costs, is still questionable.

Member State's compliance with their EU legal obligations stays an unresolved issue. As Treib puts it, "*we have as yet comparatively little evidence on the extent to which there is non-compliance beyond transposition and on the factors that are conducive to effective application and enforcement*".[1] A statement which has also been confirmed by the empirical research made in Section II. Future legal research has to go beyond legal transposition of European directives and integrate variables in their research frameworks related to domestic factors. Simply studying the legally, the transposition of European measures is not enough for explaining non-compliance behaviours across the EU. Domestic factors, such as national ongoing policies or strategies, must be taken into consideration as explicative factors.

Following the empirical results of the present thesis, every Member State has sooner or later successfully transposed the NIS Directive but not in the same way. Some States have made extensive usage of the regulatory leeway left by the Directive (e.g., Finland), while others have made the choice of transposing Directive's content as such (e.g., Greece). In most cases, behaviours in transposing the NIS Directive were motivated by domestic's politics and policies. Policy and Institutional fits, as well administrative effectiveness had an impact on the way in which the NIS Directive was transposed.

[1] Retrieved from O. Treib, 'Implementing and complying with EU governance outputs', (2014) 1 *Living Reviews in European Governance* 9

Three hypotheses have been formulated (H1, H2, H3). All of them were confirmed in the case of France, Greece, Ireland, Luxembourg while Finland and Poland offered a mitigated landscape. From a cross-country point of view on the other hand, hypothesis H3 on administrative effectiveness was confirmed for all six case studies. In the less prepared States on cybersecurity preparedness and awareness like Greece and Poland, transposed rules have met and exceeded the provisions of the NIS Directive. The variation between a unified and sectoral regulatory approach may also be considered as a factor of influence of the transposition outcomes. A positiveness, which has been noticed when testing the second hypothesis on policy misfit. Finland was the only country applying a sectoral approach in which the policy misfit hypothesis was rejected. On the other hand, variables such as the institutional setup of the political economy or the oldness of countries' membership in the EU have not affected the hypotheses results. From the three-hypothesis test conducted in this part, it possible to argue that the existence of a well-established regulatory framework prior to directive's transposition may affect the expectation of compliance among national stakeholder, which may ask a pressure to the government to comply by adapting the transposition outcome based on the cost-benefit calculation. In a such context the EU should consider the promotional function of law through incentives. incentives should be considered therefore, along with coercion, as alternative means of influence for achieving a uniform transposition of EU's directives. Prior to the adoption of directives in fields – such as cybersecurity – the Commission should thus undertake a cost-benefit assessment in order to evaluate the risks of usage of the regulatory leeway by the Member States. In such sensistive domains as cybersecurity, where some Member States (of the EU) are more advanced than others, the combination of the NIS directive with sectoral focused strategies with economic incentives should have been priviledged.

General Conclusion

Through the era of digitalisation, more and more sectors of modern society nowadays operate on the basis of digital technologies. Although sectors such as the economy, health and transport took advantage of digitisation, they continue to be exposed to cyber threats. The same goes for the European Union which, adapting to international developments, is actively working for cybersecurity, making it a priority in its policies. Since the beginning of 2000, the EU has been fully engaged in the protection against cyberattacks, but a substantial development has taken place since 2004. At that time, the European Union Network, and Information Security Agency (ENISA) was established, in accordance with Regulation 460/2004. Two years later, the EU launched the first Network Security Initiative, which was replaced in 2013 by the Cyber Security Strategy. The latter was the product of long-term processes and was based on the 2010 Digital Agenda for Europe. The aim of the strategy - which is the foundation of European cybersecurity - was to prevent and address the failures of European telecommunications systems.

The strategy tried setting up a coherent Union cyber policy across a three-fold approach through cyber resilience, cybercrime, and cyber defence. Each of these approaches refers however to domains with different types of legal and institutional governance, the internal single market, the area of Freedom, Security and Justice and the external policies of the CSDP/CFSP. Developments of Part I highlighted the *hybridity* of the legal framework of the EU, which oscillates between the hard and the soft legal and institutional governance across the European cyber policy mix. A restricted transfer of competences to the EU and the cross-sectoral nature of cybersecurity led the EU to apply different modes of governance in cybersecurity policy.

Regarding the legal framework, the EU is following the ordinary legislative process for issues linked to the security of the DSM. However, it has been seen that before adopting hard legal instruments the EU forwards harmonising national legislations throughout soft legal documents. Since 1999, the Commission adopted a series of communications in the field of network and information security such as the e-Europe initiative, the i2010 initiative, the Digital Agenda for Europe, the strategy for a Secure Information Society - Dialogue, partnership, and empowerment or even Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP). But even if the European Union has promoted cooperation between Member States in different areas since 1999, it has not truly enhanced the collaboration in cybersecurity domain. The EU's cybersecurity policy was thus marked by a limited and irregular application of Commission's recommendations.

The external action of the EU forms a paradigm of the Union's scattered approach on cyber legal related issues. The EEAS uses the term of *cybersecurity* regardless of referring to civilian or military context. The Commission uses the term of *cybersecurity* as a general term primarily related to the civilian context, whereas *cyber defence* is generally used for military cyber aspects. A situation which may be caused by the fact that contrary to NATO, where cyber defence has evolved into a crucial action in the last decade, the EU seems to have failed until 2013 to appreciate how catalytic cyber warfare can be for business development. NATO was

thus the first to adopt a Cyber Defence Policy in January 2008, five years before the EU, the latter having started to implement concrete policies and to create cyber defence capabilities with its European Cybersecurity Strategy, published in 2013. It should not be overlooked that the CSDP and EU's defence dimension in general have neither the degree of NATO maturity nor the real permanent staffing force. The sensitivity and reluctance of certain Member States to participate in a common defence policy in the field of cybersecurity, given their own cyberdefence strategies, has forced the development of a Common Cyberdefence Policy which is a rarely addressed issue marked by the existence of a number of instruments of soft law (e.g., strategies) and of a soft institutional governance. For example, concepts such as *strategic autonomy* are sometimes employed that are differently defined by Member States either because they still prefer other frameworks for security and defence issues (the United States and NATO), "*or because initiatives, such as PESCO, includes too many objectives that are not sufficiently strategically prioritised and lacking strong compliance mechanisms*". Therefore, the current thesis showed that the CSDP Decision-Making Process is generally marked to cyber related issues by intergovernmental procedures with supranational practice. On the other hand, while constituting an obstacle to their effective implementation by EU Member States' policies, the non-binding nature of the norms and principles of international law is accentuating the soft nature of the cybersecurity policy when it comes to defence matters, since it is does not offer a comprehensive framework able to serve as a set-up base for the EU to harden its cybersecurity/defence related policy.

The cybersecurity policy mix in the EU involves various modes of institutional governance. Over the last fifteen years, the EU has created several institutions providing to their Member States with adequate cybersecurity and cyberdefence ressources. The reinforced role of the Commission in EU's tradition model of hard governance, the coordination through intergovernmentalists mechanisms within the Council of the EU workplace, the partial-fledged co-decisive European Parliament, and the judicial review of national measures by the Court of Justice of the EU on the preservation of the fundamental rights of European citizens synthetise the governance landscape of the EU in the field of cybersecurity. The EU practice of *agencification* has resulted in an expediential development of EU's cybersecurity *soft* networked governance, with horizontal cooperation and information exchange between the various agencies being often limited. Yet cybersecurity governance is fragmented at the EU level.

The adoption of the NIS Directive in 2016 on the basis of Article 114 TFEU, marked the first step for an EU-wide cybersecurity legislation harmonising national cybersecurity capabilities, cross-border collaboration, and the supervision of critical sectors across the EU. The main objectives of the Directive are the management of security risks, the protection against cyber-attacks, the detection of cyber-security incidents and the minimisation of the impact of cyber-security incidents. The analysis of the provisions of the NIS directive revealed that digitalazing the European single market still requires moving from individual national markets to one single EU-wide rulebook.

Therefore, Member States were obliged to work with the EU in harmonising their national legislation on NIS security. The measures stemming from the NIS Directive apply to private actors, Member States' public authorities and intergovernmental relations, since the NIS Directive must be transposed in domestic law. Domestic actors may however create many difficulties of a legal, economic as well as of a technical nature. The present thesis argues that the limits of the EU Law should be searched not only in the nature of EU law but also within domestic policies and politics.

Following the *Most Similar Systems Design* strategy the choice was made to analyse NIS Directive transposition by France, Finland, Greece, Ireland, Luxembourg and Poland. This selection of case studies was based on the EU Enlargement round they belong to, their cybersecurity preparedness and awareness, and the institutional setup of their political economy. Throughout a qualitative based analysis, it has furthermore been revealed that the adoption of the NIS Directive, a hard instrument with a soft dimension, was also marked from a fragmented approach within the selected case studies. Althought there was no problem of legal compliance, since the six Member States have finally transposed the NIS Directive without making the finally the object of an infringement procedure (Art. 258 TFEU). These Member States have made however the use of the Directive's regulatory leeway to adjust its content to the domestic *reality*.

For assessing the discretionary use of the regulatory leeway by the Finland, France, Greece, Ireland, Luxembourg and Poland three hypothesis have been tested regarding the degree of policy misfit, of institutional misfit and the administrative effectiveness. Firstly, the degree of policy misfit with the NIS Directive was affected by the combined choice between a sectoral or centralized approach for the implementation of the directive. Secondly, it was revealed that the variable of institutional misfit should be seen as a combination of behavioral factors. The capacity of the national society to force the adaptation upon directives transposal should be considered alongwith the expectation of the society for compliance. An expectation that should be measured on the base of a well-established regulatory framework at the time of the transposition and the cost-benefit calculations that may result from a such regulatory framework. Thirdly, the degree of administrative effectiveness was confirmed in all six cases as having an influence on the transposition outcome. From the aforementioned results an overall statement could be drawn. The NIS directive landscape stays largely fragmented mostly due to the preservation of domestic interests by Member States of the EU, a fragmentation that has also been seen by the European Commission.

On January 19th, 2020, the European Commission's new work programme was published. Under the second priority – A Europe fit for the digital age – the Commission announced its intention to launch a review of the NIS Directive to further strengthen overall cybersecurity in the Union. On 7 July 2020 the Commission opened a period of public consultation on revisions to the NIS Directive. The President of the European Commission Ursula von der Leyen explained that the strategic objective of the revision was to make Europe suitable for the digital age. At the end of 2020, the European Commission published a proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive), to update and replace Directive (EU)

2016/1148, which entered into force in 2016. In the explanatory memorandum following the NIS2 Directive proposal, it is acknowledged that "*cybersecurity requirements imposed on entities providing services or economically relevant activities vary considerably among Member States in terms of type of requirement, their level of detail and the method of supervision*". It is also acknowledged that this fragmentation stems from the unclear delimitation of the NIS Directive's scope of application, "*which was largely left to the discretion of Member States*". In the same way, the NIS Directive allowed the Member States of the EU with a significant leeway in the transposition of security and incident reporting obligations, as well as on supervision and enforcement requirements. These statements confirm the relevant work's results conducted along with the present thesis without having access to the same sources of information.

To conclude, the State's obligation of result implies that it uses its internal law to fulfil it. Thus, the obligation of transposition incumbent on the States is a condition of the effectiveness of EU law but the effectiveness of hard regulation in fostering compliance, especially of those actors that face heavy costs, is still questionable. All Member States have sooner or later transposed the provisions of the NIS Directive but as we have seen this was not conducted in the same manner in each case. The Member State's compliance with their EU legal obligations certainly stays an unresolved issue. But the following research work showed that future legal studies would benefit from going beyond legal transposition of European directives and from integrating framework variables related with domestic policies and politics.

Bibliography

Books:

- Amselek, P. (1964), *Perspectives critiques d'une réflexion épistémologique sur la théorie du droit*. Paris: LGDJ.

- Andenas, M. and Andersen, C. (2011), *Theory and Practice of Harmonisation*. Cheltenham: Edward Elgar Publishing.

- Andréani, G. (2002), *What Future for Federalism ?*. London: Centre for European Reform.

- Andreasson, Kim J. (2012), *Cybersecurity: Public Sector threats and Responses*, CRC Press

- Arpagian, N. (2015), *La cybersécurité*, « Que sais-je ? », n° 3891. Presses Universitaires de France.

- Aubert, J.-L. (1984), *Introduction au droit et thèmes fondamentaux du droit civil*. Paris : Armand Colin

- Bache, I.; George, S.; Bulmer, S. and Parker, O. (2011), *Politics in the European Union.* Oxford: Oxford University Press.

- Bannelier, K. and Christakis, T. (2017), *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*, Paris, Les Cahiers de la Revue Défense Nationale.

- Bergé, J.-S. and Robin-Olivier, S. (2011), *Droit européen* (2nd ed.). Paris : Thémis.

- Bickerton, Christopher J.; Hodson, Dermot; Puetter, Uwe (2015), *The New Intergovernmentalism. States and Supranational Actors in the Post-Maastricht Era.* Oxford, Oxford University Press.

- Blatter, J. and Haverland, M. (2012), *Designing case studies : explanatory approaches in small-n research*. Palgrave Macmillan UK.

- Bloch, O. and von Wartburg, W. (2004), *Dictionnaire étymologique de la langue française*. Paris : PUF

- Börzel, T.A. (2003), *Environmental Leaders and Laggards in Europe: Why there is (not) a 'Southern Problem'*. Aldershot, UK: Ashgate.

- Börzel, T. (2001), *States and Regions in the European Union. Institutional Adaptation in Germany and Spain*. Cambridge: Cambridge University Press.

- Bouveresse, A. and Ritleng, D. (2018), *L'effectivité du droit de l'Union européenne*, Bruylant Edition.

- Buzan, B. and Hansen, L. (2009), *The evolution of international security studies*. Cambridge: Cambridge University Press.

- Cairns, W. (2002), *Introduction to European Law*. London: Cavendish.

- Carbonnier, J. (1998), *Flexible droit. Pour une sociologie du droit sans rigueur*. Paris: LGDJ

- Chamon,M. (2016), *EU Agencies: Legal and Political Limits to the Transformation of the EU Administration*. Oxford University Press.

- Cherrier, E. and Guérard, S. (2014), 'La régionalisation en Europe', *Regards croisés*. Bruylant Edition.

- Christou, G. (2016), *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. London, Palgrave MacMillan

- Chryssochoou, D. N.; Tsinisizelis, M. J.; Stavridis, S. and Ifantis, K. (2003), *Theory and Reform in the European Union*. Manchester University Press.

- Cohendet, M.-A. (2001), 'Légitimité, effectivité et validité'. In : *Mélanges Pierre Avril, La république*. Montchrestien.

- Coombes, D. (1970), *Politics and Bureaucracy in the European Community*. London: George Allen and Unwin

- Cornu, G. (2004), *Vocabulaire juridique*. Paris : PUF.

- Copsey, N. (2015), *Rethinking the European Union*. Basingstoke: Palgrave Macmillan.

- Cowles, M.G.; Caporaso, J. and Risse, T. (2001), *Transforming Europe: Europeanization and Domestic Change*. Ithaca: Cornell University Press.

- Davies, K. (2001), *Understanding European Union Law.* London: Cavendish Publishing

- De Búrca, G.; J. Scott (2006), *Law and New Governance in the EU and the US*. Dublin: Irish Academic Press.

- Delerue, F. (2020), *Cyber Operations and International Law. In Cyber Operations and International Law*. Cambridge: Cambridge University Press.

- Demers, V. (1996), *Le contrôle des fumeurs: Une étude d'effectivité du droit*. Montréal: Thémis.

- Denzin, N.K.; Lincoln, Y.S. (2000), *Handbook of Qualitative Research*. London: SAGE Publications

- Deschaux-Dutard, D. (2018), *Introduction à la sécurité internationale*. Presses Universitaires de Grenoble.

- Duina, F. G. (1999), *Harmonizing Europe: Nation-States Within the Common Market*. Albany, NY: State University of New York Press.

- Dür, A. and Mateo, G. (2016), *Insiders versus Outsiders: Interest Group Politics in Multilevel Europe*. Oxford: Oxford University Press.

- Drahn P. (2020), Theoretical Explanations for the Domestic Impact of EU Law, *Adoption of EU Business and Human Rights Policy. Contributions to Political Science*. Springer, Cham.

- Epstein, D. and O'Halloran, S. (1999), *Delegating Powers. A Transaction Costs Politics Approach to Policy Making under Separate Powers*. Cambridge: Cambridge University Press.

- Fabbrini, S. (2015). *Which European Union? Europe after the Euro Crisis*. Cambridge University Press.

- Falkner, G.; Treib, O.; Hartlapp, M. and Leiber, S. (2005), *Complying with Europe: EU Harmonization and Soft Law in the Member*. New York: Cambridge University Press

- Featherstone, K. and Papadimitriou, D. (2008), The Limits of Europeanization: Reform Capacity and Policy Conflict in Greece, *Palgrave Studies in European Union Politics*. UK: Palgrave Macmillan.

- Gercke, M. (2012), *Understanding cybercrime: Phenomena, challenges, and legal response*. Geneva: ITU.

- Gerring, J. (2007), *Case study research : principles and practices*. Cambridge University Press.

- Gesualdi-Fecteau, D. and Visotzky, M. (2020), 'La notion d'effectivité du droit'. In : Blais Y. (Ed.), *Approches et fondements du droit*. Canada : Thomson Reuters, pp. 327 – 362.

- Ghernaouti, S. (2016), *Cybersécurité* (5th ed.). Sécurité informatique et réseaux, Malakoff :Editions Dunod.

- Guillien, R., Vincent, J. (1995), *Lexique des termes juridiques*. Paris: Dalloz.

- Guiora, A.N. (2017), *Cybersecurity: Geopolitics, law, and policy* (1st ed.). New York :Routledge.

- Hass, Ernst B. (1958), *The Uniting of Europe: Political, Social, and Economic Forces 1950-1957*. Stanford: Stanford University Press.

- Héritier, A., Kerwer, D., Knill, C., Lehmkuhl, D., Teutsch, M., and Douillet, A-C. (2001), *Differential Europe: New opportunities and restrictions for policymaking in the Member States*. Lanham, MD: Rowman and Littlefield.

- Hix, S., Hoyland, B. (2011), *The Political System of the European Union* (3rd ed.). Houndmills: Palgrave Macmillan.

- Hix, S. (2005), *The political system of the European Union* (2nd ed.). Palgrave Macmillan, Basingstoke

- Hofmann S. (2012), 'CSDP: Approaching Transgovernmentalism?' In: Kurowska X., Breuer F. (Ed.) *Explaining the EU's Common Security and Defence Policy*, London: Palgrave Macmillan, pp. 41 – 62

- Hofmann, S. (1995), *The European Sisyphus: Essays on Europe, 1964-94*. New York: Routledge.

- Hooghe, L. and Marks, G. (2001), *Multi-Level Governance and European Integration*. Lanham, MD: Rowman and Littlefield Publishers.

- Jans, J.H., de Lange, R., Prechal, S. and Widdershoven, R.J.G.M. (2015), *Europeanisation of Public Law*. Groningen: Europa Law Publishing.

- Kelsen, H. (1962), *Théorie pure du droit*. Paris : Dalloz.

- Kelsen, H. (1996), *Théorie générale des normes.* Paris : PUF

- Klüver, H. (2013), *Lobbying in the European Union*. Oxford: Oxford University Press.

- Knill, C.; Lenschow, A. (2000), *Implementing EU Environmental Policy : New Directions and Old Problems*. Manchester : Manchester University Press.

- Lenaerts, K. and Van Nuffel, P. (2005), *Constitutional law of the European Union* (2nd ed.). London: Sweet & Maxwell.

- Leuffen, D. Rittberger, B. and F. Schimmelfennig (2012), *Differentiated Integration: Explaining Variation in the European Union*. Basingstoke: Palgrave Macmillan.

- Lewis, J. (2003), *Qualitative Research Practice - A Guide for Social Science, Students and Researchers*. London: SAGE Publications, Inc.

- Lindberg, Leon N. (1963), *The political dynamics of european economic integration*. Stanford: Stanford University Press.

- Lobell, S., Ripsman, N. and Taliaferro, J. (2009), *Neoclassical Realism, the State, and Foreign Policy*, Cambridge: Cambridge University Press.

- Malinvaud, P. (1992), *Introduction à l'étude du droit. Cadre juridique des relations économiques.* Paris : Litec

- Mallet, J.-C. (2008), *Défense et Sécurité nationale – Le Livre Blanc*. Paris : La documentation Française.

- Missiroli A. (2015), *Towards an EU global strategy – Background, process, references*. EU Institute for Security Studies (EUISS), Paris

- Monjal, P.-Y. (2006), *Le droit communautaire applicable aux collectivités territoriales. Les nouveaux enjeux*. Editions Territorial.

- Moravcsik, A. (1998), *The Choice for Europe: Social Purpose and State Power from Rome to Maastricht*. Ithaca, NY: Cornell University Press

- Majone, G. (2009), *Europe as the Would-be World Power – The EU at Fifty*. Cambridge University Press.

- March, J. and Olsen, J. (1989), *Rediscovering Institutions. The Organizational Basis of Politics. The Free Press*. Cambridge University Press.

- Marsden, C. (2011), *Internet co-regulation: European law, regulatory governance, and legitimacy in cyberspace*. Cambridge University Press.

- Montaldo, S., Costamagna, F. and Miglio, A. (2021), *EU Law Enforcement: The Evolution of Sanctioning Powers*. New York:Routledge.

- Mörth, U. (2004), *Soft law in governance and regulation: an interdisciplinary analysis*. Edward Elgar Publishing

- Nugent, N. (2017), *The Government and Politics of the European Union* (8th ed.). London: Red Globe Press.

- Ost, F. and Van De Kerchove, M. (2002), *De la pyramide au réseau. Pour une théorie dialectique du droit*. Bruxelles : Publications des Facultés universitaires Saint-Louis.

- Pelkmans, J. (2006), *European Integration: Methods and Economic Analysis* (3rd ed.). London: Pearson Education Limited.

- Przeworski, A. and Teune, H. (1970), *The Logic of Comparative Social Inquiry*. New York: Wiley.

- Puetter, Uwe. (2014), *The European Council and the Council. New Intergovernmentalism and Institutional Change*. Oxford: Oxford University Press.

- Preston C. (1997), *Enlargement and Integration in the European Union*. London: Routledge

- Prevedourou, E. (1999), *L'évolution de l'autonomie procédurale des états membres de l'Union Européenne : recherches sur le pouvoir du juge administratif d'apprécier d'office la compatibilité du droit national avec le droit européen*. Esperia Publications.

- Quemener, M. and Pinte, J.-P. (2013), *Cybersécurité des acteurs économiques - risques, réponses stratégiques et juridiques*. Cachan: Edition Lavoisier.

- Rangeon, F. (1989), *Réflexions sur l'effectivité du droit*. Les usages sociaux du droit. PUF.

- Rasmussen, H. (1986), *On Law and Policy in the European Court of Justice: A Comparative Study in Judicial Policymaking*. Leiden: Martinus Nijhoff Publishers

- Rasmussen, H. (1998), *The European Court of Justice*. Copenhagen: Gadjura

- Rawls, J. (1987), *Théorie de la Justice*. Paris: Seuil.

- Richardson, J. (1996), 'Eroding EU politics: Implementation gaps, cheating and re-steering'. In: Richardson, J. (Ed.), *European Union: Power and Policymaking*. London: Routledge, pp. 278 – 294.

- Rosamond, B. (2000), *Theories of European Integration. Basingstoke*. UK: Palgrave MacMillan.

- Risse, T., Ropp, S.C. and Sikkink, K. (2001), *The power of human rights: International norms and domestic chance*. Cambridge: Cambridge University Press.

- Ross, A. (1959), *On law and justice*. Berkeley & Los Angeles: University of California Press.

- Salisbury, R. (1992), *Interests and Institutions*. Pittsburgh: University of Pittsburgh Press.

- Saurugger, S. (2014), *Theoretical approaches to European integration*. Basingstoke: Palgrave Macmillan

- Saurugger, S. (2010), *Théories et concepts de l'intégration européenne*. Paris: Presses de Sciences Po.

- Scholten, M. and Luchtman, M. (2017), *Law Enforcement by EU Authorities: Implications for Political and Judicial Accountability*. Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing.

- Schön-Quinlivan, E. (2011), *Reforming the European Commission*. Basingstoke: Palgrave Macmillan.

- Schwarze, J.; Becker, U. and Pollak, C. (1993), 'Die Implementation von Gemeinschaftsrecht', *Untersuchungen zur Gesetzgebungs- und Verwaltungspolitik der Europäischen Gemeinschaft und ihrer Mitgliedstaaten*. Baden-Baden: Nomos.

- Senden, L. (2004), *Soft Law in European Community Law*. Oregon: Hart Publishing.

- Siedentopf, H. and Ziller, J. (1988), *Making European policies work: The implementation of community legislation in the Member States*. London: Sage.

- Slaughter, A.-M. (2004) *A New World Order*. Princeton: Princeton University Press.

- Tallberg, J. (1999). *Making States Comply. The European Commission, the European Court of Justice, and the Enforcement of the Internal Market*. Lund: Studenlitteratur.

- Thibierge, C. (2009), *La Force Normative. Naissance d'un Concept*, Paris: LGDJ Hors collection.

- Thomas, J. R. and Nelson, J. K. (1996), *Research Methods in Physical Activity*. Champaign: Human Kinetics Publishers.

- Troper, M. (2003), *La philosophie du droit*, coll. « Que sais-je ? », Paris : PUF.

- Tropina, T. and Callanan, C. (2015), *Self-and Co-regulation in Cybercrime, Cybersecurity and National Security*. Heidelberg: Springer.

- Tsagourias, N. and Buchan, R. (2015), *Research Handbook on International Law and Cyberspace*. UK: Edward Elgar Publishing.

- Tsebelis, G. (2002), *Veto Players: How Political Institutions Work*. Princeton University Press.

- Van Keulen, M. (2006), *Going Europe or Going Dutch: How the Dutch Government Shapes European Union Policy*. Amsterdam University Press

- Versluis, E. (2003), *Enforcement matters enforcement and compliance of European Directives in four Member States*. Utrecht.

- Vervaele, J. (1999), *Compliance and Enforcement of European Community Law*, The Hague: Kluwer.

- Vigour, C. (2005), *La comparaison dans les sciences sociales: Pratiques et méthodes*. Paris: La Découverte.

- Wiener, A., Diez, T. (2009), *European Integration Theory* (2nd ed.). Oxford University Press.

Chapters:

- Alberti, J. (2021), 'New Actors on the Stage: The Emerging Role of EU Agencies in Exercising Sanctioning Powers'. In: Montaldo, S., Costamagna, F., and A. Miglio (Ed.), *EU Law Enforcement: The Evolution of Sanctioning Powers*. New York: Routledge, pp. 25 – 46.

- Beaud, O. (2004), 'Préface'. In : Beaud, O. (Ed.), *René Capitant, Écrits d'entre-deux-guerres : 1928-1940*. Paris : Panthéon-Assas

- Blumann, C. ; Bertrand, B. ; Grard, L. ; Peraldi-Leneuf, F. ; Petit, Y. and Soulard, C. (2015), 'Introduction au marché intérieur. Libre circulation des marchandises'. In: C. Blumann (Ed.), *Commentaire J. Mégret* (3rd ed.), Éditions de l'Université de Bruxelles, pp. 9–23.

- Börzel, T. A. (2008), 'Environmental Policy'. In: Graziano, P. and M. Vink (Ed.), *Europeanization: New Research Agendas*. New York: Palgrave Macmillan, pp. 226 – 238

- Börzel, T. and Risse, Th. (2007), 'Europeanization: The European Impact of EU Politics'. In: Joergensen, K.; Pollack, M., and B. Rosamond (Ed.), *Handbook of European Union Politics*. London, Sage, pp. 483 – 504.

- Börzel, T. and Risse, Th. (2003), 'Conceptualizing the domestic impact of Europe'. In: Featherstone, K., and C. Radaelli (Ed.), *The Politics of Europeanization*, Oxford: Oxford University Press, pp. 57 – 82.

- Bruni, A. (2019), 'Promoting Coherence in the EU Cybersecurity Strategy'. In: Vedder, A.; Schroers, J.; Ducuing, C. and P. Valcke (Ed.), *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, pp. 253-276.

- Buchen C. (2007), 'Estonia and Slovenia as Antipodes'. In: Lane, D., and M. Myant (Ed.), *Varieties of Capitalism in Post-Communist Countries. Studies in Economic Transition*. Palgrave Macmillan, London, pp. 65 – 89.

- Bulmer, S. (2007), 'Theorizing Europeanization'. In: Graziano, P. and M. P. Vink (Ed.), *Europeanization: New Research Agendas*, New York: Palgrave Macmillan, pp. 46 – 58.

- Cardwell, P.J. (2020), 'Governance as the meeting place of EU law and politics'. In Cardwell, P.J. and Granger, M.-.P. (Eds.), *Research Handbook on the Politics of EU Law*. Cheltenham, UK: Edward Elgar Publishing, 10–30.

- Cardwell, P.J. (2011), 'Institutional balances, competences and restraints: The EU as an autonomous foreign policy actor'. In Collins, R. and N. D. White (Eds), *International Organizations and the Idea of Autonomy: Institutional Independence in the International Legal Order*. London: Routledge, 353–365.

- Christakis, T. (2018), 'The relations between cybersecurity, data protection and privacy: a european perspective'. In Pernice, I. and J. Pohle (Ed.), *Privacy and Cyber Security on the Books and on the Ground*, Berlin: Alexander von Humboldt Institute for Internet and Society, pp. 26-30.

- Ciavarini Azzi, G. (2000), 'The slow march of European Legislation: The implementation of directives'. In: Neunreither, K. and A. Wiener (Ed.), *European integration after Amsterdam: Institutional dynamics and prospects for democracy*. Oxford: Oxford University Press, pp. 52 – 67

- Collins, H. (2011), 'The constitutionalization of European private law as a path to social justice ?' In: Micklitz, Hans-W. (Ed.), *The Many Concepts of Social Justice in European Private Law*. Edward Elgar Publishing Ltd, Cheltenham, pp. 133 – 166.

- Dewar, R. S. (2017), 'The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern'. In: O'Neill, M. Swinton, K. (Ed.), *Challenges and Critiques of the EU Internal Security Strategy*. Cambridge Scholars Publishing, pp. 113 – 148.

- Duez, D. (2014), 'L'européanisation au prisme de la science politique. Un nouveau regard sur l'Europe'. In : Duez, D., Paye, O. and C. Verdure (Ed.), *L'européanisation. Sciences humaines et nouveaux enjeux*. Collection « Idées d'Europe ». Bruxelles: Bruylant.

- Featherstone, K. (2004), 'The political dynamics of external empowerment: The emergence of EMU and the challenge to the European Social Model'. In: Martin, A., and G. Ross (Ed.), *Euros and the Europeans*. Cambridge: Cambridge University Press, pp. 226 – 247.

- Featherstone, K. and Radaelli, C. (2003), 'A conversant research agenda'. In: Featherstone, K. and C. Radaelli (Eds), *The Politics of Europeanization*. Oxford: Oxford University Press, pp. 331 – 341.

- Fuster, G. & Jasmontaite, L. (2020), 'Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights'. In: Christen, M.; Gordijn, B.; Loi, M. (Ed.), *The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology*. Vol 21. Cham: Springer, pp. 97 – 118.

- Giuliani, M. (2003), 'Europeanization in Comparative Perspective: Institutional Fit and National Adaptation', In: Featherstone, K. and C. Radaelli (Ed.), *The Politics of Europeanization*. Oxford: Oxford University Press, pp. 134 – 155.

- Goetz, K.H. (2001), 'European Integration and National Executives: A cause in search of an effect ?' In: Goetz, K.H. and S. Hix (Eds), *Europeanized Politics? European Integration and National Political Systems*. Portland: Frank Cass, pp. 211 – 231.

- Hall, P. A. and Soskice, D. (2001), 'An Introduction to Varieties of Capitalism'. In: Hall, P. A., and D. Soskice (Ed.), *Varieties of Capitalism: The Institutional Foundations of Comparative Advantage*. Oxford: Oxford University Press, pp. 1–68.

- Hartlapp, M. (2019), 'Soft Law Implementation in the EU Multilevel System Legitimacy and Governance Efficiency Revisited'. In: Behnke, N.; Broschek, J. and J. Sonnicksen (Ed.), *Configurations, Dynamics, and Mechanisms of Multilevel Governance*. Cham: Springer International Publishing, pp. 193-210.

- Hartlapp, M. (2015), 'Politicization of the European Commission: When, How, and with What Impact ?' In: Bauer, Michael W., and J. Trondal (Ed.), *The Palgrave Handbook of the European Administrative System*. London: Palgrave Macmillan UK, pp. 145–160.

- Haverland, M. (2008), 'Methodology'. In: Graziano, P. and M. Vink (Ed.), *Europeanization: New Research Agendas*. New York: Palgrave Macmillan, pp. 59 – 70.

- Haverland, M. (2003), 'The Impact of the European Union on Environmental Policies'. In: Featherstone, K., and C. Radaelli (Ed.), *The Politics of Europeanization*. Oxford: Oxford University Press, pp. 203 – 221.

- Héritier, A. and Knill, C. (2001), 'Differential responses to European policies: A comparison'. In: Heritier, A.; Kerwer, D.; Knill, C.; Lehmkuhl, D.; Teutsch, M. and A-C. Douillet (Ed.), *Differential Europe: The European Union Impact on National Policy Making*. New York and Oxford: Rowman and Littlefield, pp. 257– 294.

- Héritier, A. (1995), ' "Leaders" and "laggards" in European clean air policy'. In: van Waarden, F. and B. Unger (Ed.), *Convergence or Diversity ? Internationalization and Economic Policy*. Avebury: Hampshire, pp. 278-305.

- Heukels, T. and Tib, J. (2002), 'Towards Homogeneity in the Field of Legal Remedies: Convergence and Divergence'. In: Beaumont, P.; Lyons, C., and N. Walker (Ed.), *Convergence and Divergence in European Public Law*. London: Hart Publishing, pp. 111 – 128.

- Hillion, C. (2008), 'Tous pour un, un pour tous! Coherence in the External Relations of the European Union'. In: Cremona, M. (Ed.), *Developments in EU External Relations Law*, Oxford: Oxford University Press, pp. 10-36.

- Kilpatrick, C. (2001), 'Turning remedies around: a sectoral analysis of the Court of Justice'. In: De Burga, G. and J.H.H. Weiler (Ed.), *The European Court of Justice*. New York: Oxford University Press, pp. 143 – 176.

- Knockaert, M. (2019), 'La sécurité dans le marché unique numérique européen: le Règlement 2019/881 ('Cybersecurity Act')'. In : Dumortier, F. and V. Vander Geeten (Ed.), *Les obligations légales de cybersécurité et de notifications d'incidents*. Bruxelles: Politeia, pp. 157-180.

- Krislov, S., Ehlermann, C. and Weiler, J.H. (1986), 'The Political Organs and the Decision-Making Process in the United States and the European Community', In: Cappelletti, M.; Secombe, M. and Joseph H. Weiler (Ed.), *Integration through Law, Volume 1: Methods, Tools and Institutions, Book 2: Political Organs, Integration Techniques and Judicial Process*, Berlin: Walter de Gruyter, pp. 3 – 112.

- Lascoumes, P. (1993), 'Effectivité', in A.-J. Arnaud (ed.), *Dictionnaire encyclopédique de théorie et de sociologie du droit*. Paris: LGDJ

- Marti, G. (2019), 'Les conflits de base juridique'. In: Clément-Wilz, L. (ed.), *Le rôle politique de la Cour de justice de l'Union européenne*, Bruxelles: Bruylant, pp. 73-100.

- Marti, G. (2019), 'L'intégrité du droit de l'Union européenne. Recherches sur l'effectivité et les potentialités d'un principe matriciel du droit de l'Union européenne'. In: Blumann, Cl. and F. Picod (Ed.), *Annuaire de droit européen 2017*, Panthéon-Assas Paris II: Paris, pp. 99-118.

- Mastenbroek, E. and Van Keulen, M. (2005), 'Beyond the goodness of fit: A preference-based account of Europeanization'. In: Haverland, M. and R. Holzhacker (Ed.), *European Research Reloaded: Cooperation and Integration among Europeanized States*. Springer: Netherlands, pp. 19 – 42.

- Millard, E. (2008), 'Effectivité des droits de l'homme'. In: Andriantsimbazovina, J. ; Gaudin, H. ; Marguenaud, J.-P.; Rials, S. and F. Sudre (Ed.), *Dictionnaire des droits de l'homme*. Paris : PUF, pp. 349-352.

- Moravcsik, A. and Schimmelfennig, F. (2009), 'Liberal Intergovernmentalism'. In: Diez, T. and A. Wiener (Ed.), *European Integration Theory*. Oxford: Oxford University Press, pp. 67 – 90.

- Oppermann, K. and De Vries, C. (2011), 'Analysing issue salience in international politics: Theoretical foundations and methodological approaches. In: Oppermann K. and H. Viehrig (Ed.), *Issue Salience in International Politics*. London: Routledge, pp. 3–22.

- Pappas, T. and Assimakopoulou, Z. (2012), 'Party Patronage in Greece: Political Entrepreneurship in a Party Patronage Democracy'. In: Kopecký, P.; Mair, P. and M. Spirova (Ed.), *Party Patronage and Party Government in European Democracies*. Oxford: Oxford University Press, pp. 144–161.

- Pellet, A. (2012), 'Les sanctions de l'Union Européenne'. In: M. Benlolo-Carabot, U. Candas, and E. Cujo (Ed.), *Union européenne et droit international. En l'honneur de Patrick Daillier*. Paris: Pedone, pp. 451-455.

- Pernice, I. (2018), 'E-Government and E-Democracy: Overcoming Legitimacy Deficits in a Digital Europe?'. In: Papadopoulou L.; Pernice I. and J.H.H. Weiler (Ed.), *Legitimacy Issues of the European Union in the Face of Crisis*. Nomos. pp. 287–316.

- Perrin, J.-F. (1977), 'L'effectivité de l'ordonnance du 10 mars 1975'. In : Morand C. A. ; Perrin J.-F. ; Robert C.-N. and R. Roth (Ed.), *Le port obligatoire de la ceinture de sécurité. Hypothèses et données pour l'étude des effets d'une norme*, Genève : CETEL, Université de Genève.

- Pollack, M. (2012), 'Realist, Intergovernmentalist and Institutionalist Approaches'. In: Jones, E.; Menon, A. and S. Weatherill (Ed.), *The Oxford Handbook of the European Union*. Oxford University Press, pp. 3 – 17.

- Pollack, M. (2007), 'Rational Choice and EU Politics'. In: Jorgenson, K. E.; Pollack, M. and B. Rosamond, (Ed.), *Handbook of European Union Politics*. London: Sage, pp. 31–56.

- Pridham, G. and Cini, M. (1994), 'Enforcing Environmental Standards in the European Union: Is There a Southern Problem ?' In: Faure, M.; Vervaele, J. and A. Waele (Ed.), *Environmental Standards in the EU in an Interdisciplinary Framework*. Antwerp: Maklu, pp. 251–277.

- Procedda, M. (2014). 'Public-Private Partnerships: A soft approach to cybersecurity? Views from the European Union'. In G. Giacomello (Ed.), *Security in Cyberspace: Targeting Nations, Infrastructures, Individual*. New York, London: Bloomsbury Academic, pp. 183 – 212.

- Radaelli, C. and Pasquier, R. (2008), 'Conceptual issues'. In: Graziano, P. and M. Vink (Ed.), *Europeanization: New Research Agendas*. New York: Palgrave Macmillan, pp. 35 – 45.

- Radaelli, C. (2003), 'The Europeanization of Public Policy'. In: Featherstone, K., and C. Radaelli (Ed.), *The Politics of Europeanization*. New York: Oxford University Press, pp. 27 – 56.

- Raustiala, K. and Slaughter, A.-M. (2002), 'International Law, International Relations and Compliance'. In: Carlsnaes, W.; Risse, T. and B.-A. Simmons (Ed.), *Handbook of International Relations*. London : Sage, pp. 538–558.

- Reincke, W. and Witte, J. M. (2000), 'Interdependence, Globalization and Sovereignty: The Role of Non-binding International Legal Accords'. In: Dinah Shelton (Ed.), *Commitment and Compliance. The Role of Non-Binding Norms in the International Legal System*. Oxford: Oxford University Press, pp. 75–100.

- Risse, T.; Green Cowles, M. and Caporaso, J. (2001), 'Europeanization and Domestic Change: Introduction'. In: Cowles, M.G.; Caporaso, J., and T. Risse (Ed.), *Transforming Europe: Europeanization and Domestic Change*. Ithaca: Cornell University Press, pp. 1–20.

- Salamon, L. M. (2002), 'The tools approach and the new governance: Conclusion and implications. In: Salamon, L. M. (Ed.), *The tools of government: A guide to the new governance*. Oxford: Oxford University Press, pp. 600–610.

- Santos Vara, J. (2018), 'The EU's agencies. Ever more important for the governance of the Area of Freedom, Security and Justice'. In: Trauner, F. and Ripoll Servent (Ed.), *Routledge Handbook of Justice and Home Affairs Research*. UK: Routledge, pp. 445-455.

- Santos Vara, J. (2014), 'Transatlanctic counter-terrorism cooperation agreements on the transfer of personal data: a test for democratic accountability in the EU'. In: Deirdre C. and E. Fahey (Ed.), *A Transatlantic Community of Law. Legal Perspectives on the Relationship Between the EU and US Legal Orders*. Cambridge: Cambridge University Press, pp. 256-288.

- Scelle, G. (1936), 'Le rôle et le risque des sanctions'. In: Mestre, A.; Le Fur, L. and G. Scelle (Ed.), *Les sanctions internationales, trois opinions de juristes*. Paris: Pedone.

- Schmitter, P.C. (2002), 'Participation in Governance Arrangements: Is there any reason to expect it will achieve "Sustainable and Innovative Policies in a Multi-Level Context" ?' In: Grote J.R. and B. Gbikpi (Ed.), *Participatory Governance*. VS Verlag für Sozialwissenschaften: Wiesbaden, pp. 51 – 70.

- Shapiro, M. (2011), 'Independent agencies'. In: Craig, P. and G. De Burca (Ed.), *The evolution of EU Law*. New York: Oxford University Press, pp. 111 – 120.

- Smith, M.P. (1997), 'The Commission made me do it: The European Commission as a strategic asset in domestic politics'. In: Nugent, N. (Ed.), *At the Heart of the Union: Studies of the European Commission*. Basingstoke: Macmillan, pp. 167 – 186.

- Snape, D. and Spencer, L. (2003), 'The Foundations of Qualitative Research'. In: Ritchie, J., and J. Lewis (Ed.), *Qualitative Research Practice - A Guide for Social Science Students and Researchers*. London: SAGE Publications, Inc, pp. 1 – 23.

- Streeck, W. and Kenworthy, L. (2005), 'Theories and Pratices of Neocorporatism'. In: Janoski, T. (Ed.), *The Handbook of Political Sociology: States, Civil Societies, and Globalization*. New York: Cambridge University Press, pp. 441–460.

- Sverdrup, U. (2008), 'Implementation'. In: Graziano, P. and M. Vink (Ed.), *Europeanization: New Research Agendas*. New York: Palgrave Macmillan, pp. 197 – 211.

- Sztucki, Jerzy (1990), 'Reflections on international 'soft law'". In: Ramberg, L.; Bring, O. and Saaid Mahmoudi (Ed.), *Festskrift till Lars Hjerner*. Stockholm; Norstedts, pp. 549-575.

- Vink, M. and Graziano, P. (2008), 'Challenges of a new research agenda'. In: Graziano, P. and M. Vink, (Ed.), *Europeanization: New Research Agendas*. New York: Palgrave Macmillan, pp. 3 – 20.

- Weiler, J. (1988), 'The White Paper and the application of Community law'. In: Bierber, R., Dehousse, R., Pinder, J. and J. Weiler (Ed.), *One European Market*. Baden-Baden: Nomos, pp. 337–58.

- Wessel, R. A. (2020), 'Cybersecurity in the European Union: Resilience through Regulation?'. In: Conde, E.; Yaneva, Z. and M. Scopelliti (Ed.), *The Routledge Handbook of European Security Law and Policy*. London: Routledge.

- Wessel, R. A. (2015), 'Towards EU Cybersecurity Law: Regulating a New Policy Field'. In: Tsagourias, N. and R. Buchan (Ed.), *Research Handbook on International Law and Cyber Space*. Cheltenham: Edward Elgar Publishing, pp. 403–425.

- Wiseman, G., and Sharp, P. (2017). 'Diplomacy'. In: Devetak, R.; George, J., and S. Percy (Ed.), *An Introduction to International Relations*. Cambridge: Cambridge University Press, pp. 296 – 308.

Articles:

- Abbott, K. W., and Snidal, D. (2000), 'Hard and Soft Law in International Governance', *International Organization*, 54(3), 421–56.

- Acceto, M. and Zleptnig, S. (2005), 'The principle of effectiveness: rethinking its role in Community Law', *European Public Law*, 11(3), 375-403.

- Anckar, C. (2008), 'On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research', *International Journal of Social Research Methodology*, 11(5), 389-401.

- Andone, C. and Greco, S. (2018), 'Evading the Burden of Proof in European Union Soft Law Instruments: The Case of Commission Recommendations', *International Journal for the Semiotics of Law*, 31(1), 79-99.

- Angelet, B., and Vrailas, I. (2008), 'European Defence in the wake of the Lisbon Treaty', *Egmont Paper*, 21.

- Aspinwall, M. and Schneider, G. (2000), 'Same menu, separate tables: The intuitionalist turn in Political Science and the study of European Integration', *European Journal of Political Research*, 38(1), 1-36.

- d'Aspremont, J. (2008), 'Softness in International Law: A Self-Serving Quest for New Legal Materials', *The European Journal of International Law*, 19(5). 1075–1093.

- Bannelier-Christakis K. (2017), 'Rien que la Lex Lata ? Etude critique du Manuel de Tallinn 2.0 sur le droit international applicable aux cyber-opérations', *Annuaire Français de Droit International*, CNRS, 121-160.

- Bannelier-Christakis, K. (2017), 'Obligations de diligence dans le cyberespace : qui a peur de la cyber-diligence?' Revue belge de droit international 2, 612–665

- Bannelier-Christakis, K. (2015), 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?', *Baltic Yearbook of International Law Online*, 14(1), 23-39.

- Barrinha, A. and Carrapico, A. (2017), 'The EU as a Coherent (cyber)Security Actor ?', *Journal of Common market*, 55(6), 1254-1272.

- Barrinha, A. and Renard, T. (2017), 'Cyber-diplomacy: the making of an international society in the digital age', *Global Affairs*, 3(4-5), 353-364.

- Bauer, Michael W. and Becker, S. (2014), 'The Unexpected Winner of the Crisis: The European Commission's Strengthened Role in Economic Governance', *Journal of European Integration*, 36(3), 213-229.

- Bátora, J. (2009), 'European Defence Agency: A Flashpoint of Institutional Logics', *West European Politics* 32(6), 1075–1098.

- Baumgartner, F.R. and Mahoney, C. (2008), 'The two faces of framing – individual level framing and collective issue definition in the European Union', *European Union Politics*, 9(3), 435–49.

- Beach, D. (2005), 'Why governments comply: An integrative compliance model that bridges the gap between instrumental and normative models of compliance', *Journal of European Public Policy*, 12(1), 113 – 142.

- Bendiek, A. and Porter, L. (2013), 'European Cyber Security Policy within a Global Multistakeholder Structure', *European Foreign Affairs Review*, 2, 155–180.

- Bickerton, C. J., D. Hodson, and U. Puetter. (2014), 'The New Intergovernmentalism: European Integration in the Post-Maastricht Era', *Journal of Common Market Studies*, 53(4), 703–722.

- Biener, C., Eling, M. and Wirfs, J. (2015), 'Insurability of cyber risk: An empirical analysis', *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1), 131-158.

- Błachucki, M. (2020), 'The Role of Soft Law in Functioning of Supranational Competition Networks', *Contemporary Central & East European Law*, 1(133), 33-42.

- Blockmans, S. (2018), 'The EU's modular approach to defence integration: An inclusive, ambitious and legally binding PESCO ?' *Common Market Law Review*, 55, 1785–1826.

- Blutman, L. (2010), 'In The Trap of A Legal Metaphor: International Soft Law', *International and Comparative Law Quarterly*, 59(3), 605-624.

- Bonichot J.-C. (2014), 'A propos de l'attribution du pouvoir réglementaire a l'Autorité européenne des marchés financiers', *RFDA*, 325–330.

- Börzel, T. A. and Sedelmeier, U. (2017), 'Larger and more law abiding? The impact of enlargement on compliance in the European Union', *Journal of European Public Policy*, 24(2), 197-215.

- Börzel, T. A. and Risse, T. (2012), 'From Europeanisation to diffusion: introduction', *West European Politics*, 35(1), 1–19.

- Börzel, T. A. (2001), 'Non-Compliance in the European Union: Pathology or Statistical Artefact?', *Journal of European Public Policy*, 8(5), 803–24.

- Börzel, T. A. and Risse, T. (2000), 'When Europe Hits Home: Europeanization and Domestic Change', *European Integration online Papers*, 4(15).

- Börzel T. A. *et al.*, (2010), 'Obstinate and Inefficient: Why Member States Do Not Comply with European Law', *Comparative Political Studies*, 43(11), 1363–1390.

- Börzel, T. A. (2002), 'Pace-Setting, Foot-Dragging, and Fence-Sitting: Member State Responses of Europeanization', *Journal of Common Market Studies*, 40(2), 193 – 214.

- Börzel, T. A. (2000), 'Why there is no "southern problem": On environmental leaders and laggards in the European Union', *Journal of European Public Policy*, 7(1), 141 – 162.

- Börzel, T. A. (1999), 'Towards convergence in Europe? Institutional adaptation to Europeanization in Germany and Spain', *Journal of Common Market Studies*, 37(4), 573 – 596.

- Boulet M. (2012), 'I. Les collectivités territoriales françaises dans le processus d'intégration européenne', *Droit et gestion des collectivités territoriales. Transports et politiques locales de déplacement*, 32, 785–799.

- Bourgeois M., Tanguy A., (2015), '3 questions Sécurité des données et cybermenaces : les armes pour s'en protéger', *La Semaine Juridique Entreprise et Affaires*, n° 50, 927.

- Brantly, Aaron F. (2014), 'The Cyber Losers', *Democracy and Security*, 10(2), 132 – 155.

- Brauch H. G. (2010), 'Concepts of Security Threats, Challenges, Vulnerabilities and Risks', *Coping with Global Environmental Change, Disasters and Security: Threats, Challenges, Vulnerabilities and Risks*, 5, 61 – 106.

- Breeman G. and Zwaan P., (2009), 'Domestic Change and EU Compliance in the Netherlands: Policy Feedback during Enforcement', *European Integration*, 31(3), 349 – 367.

- Brisse, M. (2007), 'La jurisprudence européenne sur les discriminations fondées sur l'âge', *Retraite et société*, 51(2), 286–291.

- Brunessen B., (2021), 'Chronique Droit européen du numérique - La volonté de réguler les activités numériques', *RTDeur. Revue trimestrielle de droit européen* 1, 160

- Brunessen, B. (2021), 'Chronique Droit européen du numérique - Perfectibilité de la protection des données personnelles', *RTDeur. Revue trimestrielle de droit européen* 1, p. 143

- Brunessen B., Bosse-Platière I., (2014), 'La soft law en droit de l'Union européenne', *Revue de l'Union Européenne* 575, *Revue de l'Union Européenne*, p. 72

- Brunessen B., (2014), 'Rapport introductif : Les enjeux de la Soft Law dans l'Union européenne', *Revue de l'Union Européenne*, Dalloz, 73-84

- Bursens, P. and Deforchea, J. (2008), 'Europeanization of Subnational Polities: The Impact of Domestic Factors on Regional Adaptation to European Integration', *Regional & Federal Studies*, 18(1), 1 – 18.

- Caranta, R. (1995), 'Judicial Protection Against Member States: A New Jus Commune Takes Shape', *Common Market Law Review*, 32, 703 – 726.

- Carbonnier, J. (1957), 'Effectivité et ineffectivité de la règle de droit, *L'année sociologique*.

- Carrapico, H. and Barrinha, A. (2017), 'The EU as a Coherent (Cyber)Security Actor? , *Journal of Common Market Studies*, 55(6), 1254– 1272.

- Chayes, A. and Handler Chayes, A., (1993), 'On Compliance', *International Organization*, 47(2), 175 - 205.

- Checkel, J.T. (2001), 'Why comply? Social learning and European identity change', *International Organization*, 55(3), 473 – 495.

- Chopin, T. and Lequesne, C. (2016), '"Differentiation as a double-edged sword: Member States" practices and Brexit', *International Affairs* 92(3), 531 – 545.

- Cini, M. (2001), 'The Soft Law Approach: Commission Rule-Making in the EU's State Aid Regime', *Journal of European Public Policy*, 8(2), 192–207.

- Coen, D. and Thatcher, M. (2008), 'Network Governance and Multi-level Delegation: European Networks of Regulatory Agencies', *Journal of Public Policy*, 28(01), 49–71.

- Collins, K. and Earnshaw, D. (1992), 'The implementation and enforcement of European Community legislation', *Environmental Politics*, 1(4), 213 – 249.

- Craig, P. (2009), 'The Legal Effects of Directives: Policy, Rules and Exceptions', *European Law Review*, 34(3), 349 – 377.

- Cremona, M. (2008), 'Coherence through Law: What Difference will the Treaty of Lisbon Make?', *Hamburg Review of Social Sciences*, 3(1), 11–36.

- Davies, G. (2006), 'Subsidiarity: The wrong idea, in the wrong place, at the wrong time', *Common Market Law Review*, 43(1), 63–84.

- De Bruycker, I. (2016), 'Pressure and expertise: explaining the information supply of interest groups in EU legislative lobbying', *Journal of Common Market Studies*, 54(3), 599–616.

- Dehousse, R. (1992), 'Integration v. Regulation? On the dynamics of regulation in the European Community', *Journal of Common Market Studies*, 30(4), 383-402.

- De Silva, K. (2013), 'Europe's fragmented approach towards cyber security', *Internet Policy Review*, 2(4), 1-8

- Detlef, J. (2016), 'Changing of the guard: trends in corporatist arrangements in 42 highly industrialized societies from 1960 to 2010', *Socio-Economic Review*, 14(1), 47–71.

- Dimitrakopoulos, D. G. (2001), 'The transposition of EU law: "post-decisional politics" and institutional economy', *European Law Journal*, 7(4), 442–58.

- Dimitrova, A. and Steunenberg, B. (2017), 'The power of implementers: a three-level game model of compliance with EU policy and its application to cultural heritage', *Journal of European Public Policy*, 24(8), 1211-1232.

- Dimitrova, A. and Steunenberg, B. (2000), 'The search for convergence of national policies in the European Union: an impossible quest?', *European Union Politics*, 1(2), 201–26.

- Dinan, D. (2016). 'Governance and Institutions: A More Political Commission', *Journal of Common Market Studies*, 54 (Annual Review), 101–116.

- Dougan, M. (2000) 'Minimum Harmonization and the Internal Market', *Common Market Law Review*, 37(4), 853-885.

- Downs, G. W.; David, M. R. and Peter, N. B. (1996),' Is the Good News about Compliance also Good News about Cooperation?', *International Organization*, 50(3), 379–406.

- Dubout, E. (2007), 'La procéduralisation des obligations relatives aux droits fondamentaux substantiels par la Cour européenne des droits de l'homme', *RTDH*, n° 70, 397–425.

- Duina, F. (1997), 'Explaining Legal Implementation in the European Union', *International Journal of the Sociology of Law*, 25(2), 155-179.

- Egan, M. and Wolf, D. (1998), 'Regulation and Comitology: The EC Committee System in Regulatory Perspective', *Columbia Journal of European Law*, 4, 499–523.

- Ellis, J. (2012), 'Shades of Grey: Soft Law and the Validity of Public International Law', *Leiden Journal of International Law*, 25(2), 313-334.

- Eising, R., Rasch, D. and Rozbicka, P. (2015), 'Institutions, policies, and arguments: context and strategy in EU policy framing', *Journal of European Public Policy*, 22(4), 516–33.

- Fasone, C. (2014), 'The European Parliament in the Economic Governance', *European Law Journal*, 20 164-185.

- Falkner, G., Hartlapp, M. and Treib, O. (2007), 'Worlds of compliance: Why leading approaches to European Union implementation are only "sometimes-true theories"', *European Journal of Political Research*, 46(3), 395–416.

- Falkner, G. (2003), 'Comparing Europeanization effects: from metaphor to operationalization', *European Integration online Papers*, 7(13), 1-18.

- Faqir, RSA (2013), 'Cyber crimes in Jordan: a legal assessment on the effectiveness of information system crimes law no (30) of 2010', *International Journal of Cyber Criminology*, 7(1), pp. 81–90.

- Fahey, E. (2014), 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security', *European Journal of Risk Regulation*, 5(1), 46-60.

- Fjelstul, J. C. and Carruba, C. J. (2018), 'The Politics of International Oversight: Strategic Monitoring and Legal Compliance in the European Union', *American Political Science Review*, 112(3), 429–445.

- Finke, D. and Dannwolf, T. (2015), 'Who let the dogs out? The effect of parliamentary scrutiny on compliance with EU law', *Journal of European Public Policy*, 22(8), 1127-1147.

- Franchino, F. (2004), 'Delegating powers in the European community', *British Journal of Political Science*, 34(2), 269–93.

- Furnell, S.M. *et al.* (1996), 'Assessing staff attitudes towards information security in a European healthcare establishment', *Medical Informatics*, 21(2), 105–112.

- Garrett, G.; Keleman, R. D. and Schulz, H. (1998), 'The European Court of Justice, National Governments, and Legal Integration in the European Union', *International Organization*, 52(1), 149–76.

- Gautier, L. (2018), 'Cyber : les enjeux pour la défense et la sécurité des Français', *Politique étrangère*, 2018/2, 29–42.

- Geradin, D. and Petit, N. (2005), 'The development of agencies at EU and national levels: conceptual analysis and proposals for reform, Yearbook of European Law', 23(1), 137-197.

- Ghernaouti, S. & Aghroum, C. (2012), 'Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cyber-sécurité', *Sécurité et stratégie*, 11(4), 74-83.

- Gijsbers, K. and Veenendaal, M. (2011), 'Protecting the National Interest in Cyberspace', *Georgetown Journal of International Affairs*, 191–196.

- Giliker, P. (2015) 'The Transposition of the Consumer Rights Directive into UK Law : Implementing a Maximum Harmonization Directive', *European Review of Private Law* 23(1), 5-28

- Gomez F. and Ganuza, J.J. (2011), 'An Economic Analysis of Harmonization 359overei : Full Harmonization, Minimum Harmonization or Optional Instrument ?', *European Review of Contract Law*, 7(2), 275-294

- Gray, V. and Lowery, D. (1993), 'The diversity of state interest group systems', *Political Research Quarterly*, 46(1), 81–97.

- Grosswald, L. (2011), 'Cyberattack Attribution Matters Under Article 51 of the U.N. Charter', *Brook. J. Int'l L.*, 36(3), 1151–1181.

- Guitton, C. (2013), 'Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?' , *European Security*, 22(1), 21–35.

- Hall, P. and Taylor, R. (1996), 'Political Science and the three New Institutionalisms', *Political Studies*, 44(4), 936–957.

- Hall, P. (1993), 'Policy Paradigms, Social Learning and the State. The case of economic policy making in Britain', *Comparative Politics*, 25(3), 275 – 296.

- Hansche, S. (2008), 'Designing a security awareness program: part I', *Information System Security*, 10(1), 14–22

- Hansen, L. and Nissenbaum, H. (2009), 'Digital disaster, cyber security, and the Copenhagen school', *International Studies Quarterly*, 53(4), 1155–1175.

- Haroche, P. (2020), 'Supranationalism strikes back: a neofunctionalist account of the European Defence Fund', *Journal of European Public Policy* 27(6), 853–872.

- Haverland, M. (2000), 'National adaptation to European integration: The importance of institutional veto points', *Journal of Public Policy*, 20(1), 83–103.

- Haverland, M. and Romeijn, M. (2007), 'Do Member States Make European Policies Work ? Analysing the EU Transposition Deficit', *Public Administration*, 85(3), 757–778.

- Hathaway, O.; Crootof, R.; Levitz, P.; Nix, H.; Nowlan, A.; Perdue, W. and Spiegel, J. (2012), 'The law of cyber-attack', *California Law Review*, 817–885.

- Hartlapp, M. and Falkner, G. (2009), 'Problems of operationalization and data in EU compliance research', *European Union Politics*, 10(2), 281–304.

- Heidbreder Eva G., (2017), 'Strategies in multilevel policy implementation: moving beyond the limited focus on compliance', *Journal of European Public Policy*, 24(9), 1367–1384.

- Hoerbelt, C. (2017), 'A Comparative Study: Where and why does the EU impose sanctions', *Research Unit on International Security and Cooperation (UNISCI) Journal*, 43, 53–71.

- Hoffmann, S. (1964), 'The European Process at Atlantic Cross-purposes', *Journal of Common Market Studies*, 3(2), 85–101.

- Jasiecki, K. (2017), 'The Nature of Capitalism in Poland. Controversy over the Economy since the end of 2015: The Prospects of Business Elite and Employer Associations', *Corvinus Journal of Sociology and Social Policy*, 8(3), 171–193.

- Jeammaud, A. (1990), 'La règle de droit comme modèle', *Revue interdisciplinaire d'études juridiques*, 25, 125–164.

- Jensen, C. (2007), 'Implementing Europe: A question of oversight', *European Union Politics*, 8(4), 451–477.

- Kaeding, M. (2006), 'Determinants of transposition delay in the European Union', *Journal of Public Policy*, 26(3), 229–253.

- Kaeding M., (2007), 'Active transposition of EU legislation', *EIPASCOPE*, 3, 27–34.

- Kassim, H. and Menon, A. (2003), 'The principal-agent approach and the study of the European Union: Promise unfulfilled?', *Journal of European Public Policy*, 10(1), 121-139.

- Kaufmann, D., Kraay, A. and Mastruzzi, M. (2011), 'The worldwide governance indicators: methodology and analytical issues', *Hague Journal on the Rule of Law*, 3(2), 220–246.

- Kinderman, D. (2015), 'Corporate social responsibility–Der Kampf um die EU-Richtlinie', *WSI Mitteilungen*, 2015/8.

- Kitchen, N. (2010), 'Systemic pressures and domestic ideas: a neoclassical realist model of grand strategy formation,', *Review of international studies*, 36(1), 117–143.

- Kjaer, PF. (2017), 'European crises of legally-constituted public power: From the "law of corporatism" to the "law of governance"', *European Law Journal,* 23, 417–430.

- Klimburg, A. (2010), 'The Whole of Nation of Cyberpower', *Georgetown Journal of International Affairs*, 11, 171–179.

- Knill, C. and Lehmkuhl, D. (1999), 'How Europe Matters. Differents Mechanism of Europeanisation', *European Integration Online Papers*, 3(7), 1–17.

- Koelble, T. A. (1995), 'The New Institutionalism in Political Science and Sociology', *Comparative Politics*, 27(2), 231–243.

- König, T. and Mader, L. (2014), 'The Strategic Nature of Compliance: An Empirical Evaluation of Law Implementation in the Central Monitoring System of the European Union', *American Journal of Political Science*, 58(1), 246–263.

- König T., Luetgert T. and Luetgert B. (2009), 'Troubles with Transposition ? Explaining Trends in Member-State Notification and the Delayed Transposition of EU Directives', *British Journal of Political Science*, 39(1), 163–194.

- Korkea-Aho, E. (2009), 'EU Soft Law in Domestic Legal Systems: Flexibility and Diversity Guaranteed?', *Maastricht Journal of European and Comparative Law*, 16(3), 271–290.

- Knill, C. (1998), 'European Policies: The Impact of National Administrative Traditions', *Journal of Public Policy*, 18(1), 1 – 28.

- Knill, C. and Lenschow, A (1998), 'Coping with Europe: The Impact of British and German Administrations on the Implementation of EU Environmental Policy', *Journal of European Public Policy*, 5(4), 595-614.

- Krahmann, E. (2003), 'Conceptualizing security governance', *Cooperation and Conflict*, 38, 5–26.

- Krzysztof Feliks Sliwinski (2014), 'Moving beyond the European Union's Weakness as a Cyber-Security Agent', *Contemporary Security Policy*, 35(3), 468–486.

- Kutay, A. (2015), 'Limits of Participatory Democracy in European Governance', *European Law Journal*, 21, 803–818.

- Láncos, P. L. (2018), 'A Hard Core Under the Soft Shell: How Binding Is Union Soft Law for Member States?', *European Public Law*, 24(4), 755–784.

- Lampinen, R. and Uusikylä, P. (1998), 'Implementation Deficit — Why Member States do not Comply with EU directives?', *Scandinavian Political Studies*, 21(3), 231-251.

- Lang, R. (2013) 'The EU's New Victims' Rights Directive : Can Minimum Harmonization Work for a Concept Like Vulnerability ?', *Nottingham LJ*, 90(22)

- Lascoumes, P. and Severin, E. (1986), 'Théories et pratiques de l'effectivité du droit', *Droit et société*, n°2, 101–124.

- Leroy, Y. (2011), 'La notion d'effectivité du droit', *Droit et société*, 79(3), 715–732.

- Lieberman, E. (2005), 'Nested Analysis as a Mixed-Method Strategy for Comparative Research', *The American Political Science Review*, 99(3), 435-452.

- Maggetti, M. (2014), 'The Politics of Network Governance: The Case of Energy Regulation', *West European Politics*, 37(3), 497–514.

- Maggetti, M. and Gilardi, F. (2011), 'The Policy-Making Structure of European Regulatory Networks and the Domestic Adoption of Standards', *Journal of European Public Policy*, 18(6), 830–847.

- Major, C. (2005), 'Europeanisation and Foreign and Security Policy – Undermining or Rescuing the Nation State?', *Politics*, 25(3), 175–190.

- Makridis, C.A. and Smeets, M. (2019), 'Determinants of cyber readiness', *Journal of Cyber Policy*, 4(1), 72–89.

- March, J. and Olsen, J. (1998), 'The Institutional Dynamics of International Political Orders', *International Organization*, 52(4), 943–969.

- March, J. and Olsen, J. (1984), 'The New Institutionalism: Organizational Factors in Political life', *American Political Science Review*, 78(3), 734–749.

- Margulies, P. (2013), 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility', *Melb. J. Int'l L.*, 14, 496–522.

- Mastenbroek, E. (2017), 'Guardians of EU law? Analysing roles and behavior of Dutch legislative drafters involved in EU compliance', *Journal of European Public Policy*, , 24(9), 1289–1307.

- Mastenbroek, E. (2005), 'EU compliance: Still a "black hole"?', *Journal of European Public Policy*, 12(6), 1103-1120.

- Mastenbroek, E. (2003), 'Surviving the deadline: The transposition of EU directives in the Netherlands', *European Union Politics*, 4(4), 371-395.

- Mastenbroek, E. and Kaeding, M. (2006), 'Europeanization beyond the goodness of fit: domestic politics in the forefront', *Comparative European Politics*, 4(4), 331–354.

- Mbaye, D.H.A. (2001), 'Why National States Comply with Supranational Law: Explaining Implementation Infringements in the European Union, 1972-1993', *European Union Politics*, 2(3), 259–281.

- McGowan, F., and H. Wallace (1996), 'Towards a European regulatory state', *Journal of European Public Policy*, 3(4), 560–576.

- McKay, C. (2013), 'Diminishing Sovereignty: How European Privacy Law Became International Norm', *Santa Clara Journal of International Law*, 11(2), 421–453.

- Mendrinou, M. (1996), 'Non – Compliance and the European Commission's Role in Integration', *Journal of European Public Policy*, 3(1), 1 – 22.

- Michael, S. E. (2018), 'Transatlantic security relations since the European security strategy: what role for the EU in its pursuit of strategic autonomy?', *Journal of European Integration*, 40(5), 605–620.

- Mincke, C. (1998), 'Effets, effectivité, efficience et efficacité du droit : le pôle réaliste de la validité', *Revue interdisciplinaire d'études juridiques* 40(1), 115–151.

- Moravcsik, A. (1993), 'Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach', *JCMS: Journal of Common Market Studies*, 31, 473–524.

- Mounier, G. (2009), 'Europol: A New Player in the EU External Policy Field?', *Perspectives on European Politics and Society* 10(4), 582-602.

- Müller, P. and P. Slominski (2019), 'Legal framing and the EU's external relations: how NGOs shaped the negotiations for an Israel-Europol cooperation agreement', *Journal of European Public Policy* 26(6), 906-926.

- Myriam Dunn Cavelty. (2018), 'Europe's cyber-power', *European Politics and Society*, 19(3), 304–320.

- Naert, F. (2013), 'Observance of international humanitarian law by forces under the command of the European Union', *International Review of the Red Cross*, 95 (891/892), 637–643.

- Naert, F. (2011), 'Legal aspects of EU operations', *Journal of International Peacekeeping*, 15, 218–242.

- Nicole S. van der Meulen (2013), 'Following in the footsteps of terrorism? Cybersecurity as a crowded policy implementation space', *Canadian Foreign Policy Journal*, 19(2), 123–126.

- Nissenbaum, H. (2005), 'Where computer security meets national security', *Ethics and Information. Technology*, 7(2), 61–73.

- Nivet, B. (2015), 'Les sanctions internationales de l'Union européenne : soft power, hard power ou puissance symbolique ?', *Revue internationale et stratégique*, 97(1), 129–138.

- Norgaard, A.S. (1996), 'Rediscovering Reasonable Rationality in Institutional', *Analysis, European Journal of Political Research*, 29(1).

- Nugent, N. and Rhinard, M. (2019), 'The "political" roles of the European Commission', *Journal of European Integration*, 41(2), 203–220.

- Olsen, J.P. (2002), 'The many faces of Europeanization', *JCMS: Journal of Common Market Studies*, 40(5), 921–952.

- Pegasiou, A. (2013), 'The Cypriot Economic Collapse: More Than a Conventional South European Failure', *Mediterranean Politics*, 18(3), 333-351.

- Pereira, B. (2016), 'La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité', *Revue internationale de droit économique*, 3(3), 387-409.

- Peterson, J. (1995), 'Decision-Making in the European Union: Towards a framework for analysis', *Journal of European Public Policy*, 2(1), 69–93.

- Pierson, P. (1996), 'The Path to European Integration: A Historical Institutionalist Analysis', *Comparative Political Studies*, 29(2).

- Pircher B., (2017), 'Member States' opposition in the Council of the European Union and its impacts on the implementation of directives', *Austrian Journal of Political Science*, 46(3).

- Pisani, E. (1956), 'Administration de Gestion, Administration de Mission'. *Revue Française de Science Politique*, 2 (Avril-Juin), 315–331.

- Pollack, M. (1997), 'Delegation, agency, and agenda setting in the European Community', *International Organization*, 51(1), 99–134.

- Portela, C. (2005), 'Where and why does the EU impose sanctions ?', *Politique Européenne*, 17(3), 83–111.

- Pridham, G. (1996), 'Environmental policies and problems of European legislation in Southern Europe', *South European Society & Politics*, 1(1), 47 – 73.

- Pridham, G. (1994), 'National Environmental Policy-making in the European Framework: Spain, Greece, and Italy in Comparison', *Regional Politics and Policy*, 4(1), 80-101.

- Purnhagen, K. P. and Wesseler J.H. (2019), 'Maximum vs minimum harmonization : what to expect from the institutional and legal battles in the EU on gene editing technologies', *Pest Management Science*, 75(9) , 2310-2315.

- Putnam, R. D. (1988), 'Diplomacy and Domestic Politics: The Logic of Two-Level Games', *International Organization*, 42(3), 427–460.

- Patterson, D.M. (1990), 'Law's pragmatism: law as practice & narrative', *Virginia Law Review*, 76(5), 937–996.

- Quemener M., (2016), 'La directive NIS, un texte majeur en matière de cybersécurité', *Sécurité et stratégie*, 3(23), 50–56.

- Radaelli, C. M. (2004), 'Europeanization: Solution or problem?', *European Integration online Papers*, 8(4).

- Raustiala, K. (2000), 'Compliance & Effectiveness in International Regulatory Cooperation', *Case Western Reserve Journal of International Law*, 32(3), 387–440.

- Riddervold, M. (2016), '(Not) in the Hands of the Member States: How the European Commission Influences EU Security and Defence Policies', *JCMS: Journal of Common Market Studies*, 54(2), 353–369.

- Rott, P. (2003), 'Minimum harmonization for the completion of the internal market ? The example of consumer sales law', *Common Market Law Review*, 40(5), 1107-1135

- Rhodes, R.A.W. (1996), 'The New Governance: Governing Without Government', *Political Studies*, 44, 652–667.

- Rizcallah, C. (2019), 'The challenges to trust-based governance in the European Union: Assessing the use of mutual trust as a driver of EU integration', *European Law Journal*, 25, 37–56.

- Ross, M. (2006), 'Effectiveness in the European Legal Order(s): Beyond Supremacy to Constitutional Proportionality?', *European Law Review*, 31(4), 474- 496.

- Rossi, C. R. (2015), 'The club within the club: the challenge of a soft law framework in a global Arctic context', *The Polar Journal*, 5(1), 8–34.

- Sabatier, P. (1998), 'The advocacy coalition framework: Revisions and relevance for Europe', *Journal of European Public Policy*, 5(1), 98–130.

- Sandholtz, W. (1996), 'Membership matters: limits of the functional approach to European institutions', *Journal of Common Market Studies*, 34(3), 403–429.

- Santos Vara, J. (2011), 'The Consequences of Kadi: Where the Divergence of Opinion between EU and International Lawyers Lies?', *European Law Journal*, 17(2), 252 – 257.

- Santos Vara, J. (2011), 'The Establisment of the European External Action Service: The EU in Search of a Stronger Role on the International Stage', *Croatian Yearbook of European Law*, 109 – 134.

- Saurugger, S. and Terpan, F. (2021), 'Normative Transformations in the European Union: On Hardening and Softening Law', *West European Politics*, 44(1), 1-20.

- Saurugger, S. and Terpan, F. (2021), 'Soft and hard law in times of crisis: budget monitoring, migration and cybersecurity', *West European Politics*, 44(1), 21–48.

- Saurugger, S. and Terpan, F. (2020), 'Understanding Normative Change in the European Union', *West European Politics*, 44(1), 1-20.

- Saurugger, S. and Terpan, F. (2016), 'Resisting 'new modes of governance': An agency-centred approach', *Comparative European Politics*, 14, 53–70.

- Saurugger, S. and Terpan, F. (2015), 'Resisting EU Norms. A Framework for Analysis', *Comparative European Politics,* 14, 53–70.

- Scharpf, F.W. (1994), 'Community and Autonomy: Multi-Level Policy-Making in the European Union', *Journal of European Public Policy*, 1(2), 219–242.

- Schimmelfennig, F. and Winzen, T. (2014), 'Instrumental and constitutional differentiation in the European Union', *JMCS: Journal of Common Market Studies*, 52(2), 354–370.

- Schimmelfennig, F. (2014), 'EU enlargement and differentiated integration: discrimination or equal treatment?', *Journal of European Public Policy*, 21(5), 681–698.

- Schmidt, S.K. (2008), 'Beyond compliance: the Europeanization of Member States through negative integration and legal uncertainty', *Journal of Comparative Policy Analysis: Research and Practice*, 10(3), 299–308

- Schmidt, Vivien A. (2016), 'Reinterpreting the rules 'by stealth' in times of crisis: a discursive institutionalist analysis of the European Central Bank and the European Commission', *West European Politics*, 39(5), 1032-1052.

- Siaroff, A. (1999), 'Corporatism in 24 industrial democracies: Meaning and measurement', *European Journal of Political Research*, 36(2), 175–205.

- Snyder, F. (1993), 'The Effectiveness of European Community Law: Institutions, Processes, Tools and Techniques', *The Modem Law Review*, 56(1).

- Spendzharova, A. and Versluis, E. (2013), 'Issue salience in the European policy process: What impact on transposition?', *Journal of European Public Policy*, 20(10), 1499–1516.

- Steunenberg, B. and Toshkov, D. (2009), 'Comparing transposition in the 27 Member States of the EU: The impact of discretion and legal fit', *Journal of European Public Policy*, 16(7), 951–970.

- Steunenberg, B. (2007), 'A policy solution to the European Union's transposition puzzle: interaction of interests in different domestic arenas', *West European Politics*, 30(1), 23–49.

- Steunenberg B., (2006), 'Turning Swift Policymaking into Deadlock and Delay', *European Union Politics*, 7(3), 293–319.

- Sverdrup, U. (2004), 'Compliance and Conflict Management in the European Union: Nordic Exceptionalism', *Scandinavian Political Studies*, 27(1), 23–43.

- Tallberg, J. (2003), 'Paths to compliance: enforcement, management, and the European Union', *International Organization*, 56(3), 609–643.

- Terpan, F. (2020), 'La relance du projet européen de défense au-delà du contrôle des États', *Politique européenne*, 70(4), 40-69.

- Terpan, F. (2015), 'Soft Law in the European Union – The Changing Nature of EU Law', *European Law Journal*, 21(1), 68–96.

- Tesauro, G. (1992), 'La sanction des infractions au droit communautaire (Report presented to the 15th FIDE Conférence, 1992)', *Rivista de diritto Europeo*, n°32, 447.

- Thomann, E. and Sager, F. (2017), 'Moving beyond legal compliance: Innovative approaches to EU multilevel implementation', *Journal of European Public Policy*, 24(9), 1253–1268.

- Thomann, E. and Zhelyazkova, A. (2017), 'Moving beyond (non-)compliance: the customization of European Union policies in 27 countries', *Journal of European Public Policy*, 24(9), 1269–1288.

- Thomann, E. (2015), 'Customizing Europe: Transposition as bottom-up implementation', *Journal of European Public Policy*, 22(10), 1368–1387.

- Thomas M., (2018), 'The efficiency of ministries in transposing EU directives: Evidence from Ireland', *Public Policy and Administration*, 33(2), 190–215.

- Thomson, R. (2010), 'Opposition through the back door in the transposition of EU directives', *European Union Politics*, 11(4), 577–596.

- Thomson, R. (2009), 'Same effects in different worlds: The transposition of EU directives', *Journal of European Public Policy*, 16(1), 1–18.

- Thomson, R., Torenvlied, R. and Arrequi, J. (2007), 'The paradox of compliance: infringements and delays in transposing European Union directives', *British Journal of Political Science*, 37, 685–709.

- Töller, A.E. (2010), 'Measuring and comparing the Europeanization of national legislation: a research note', *JCMS: Journal of Common Market Studies*, 48(2), 417–444.

- Toshkov, D. (2012), 'Compliance with EU Law in Central and Eastern Europe. The Disaster that Didn't Happen (Yet)', *L'Europe en Formation*, 364, 91–109.

- Treib, O. (2014), 'Implementing and Complying with EU Governance Outputs, Living Reviews in European Governance', 9(1), 1-46.

- Treib, O. (2008), 'Implementing and Complying with EU Governance Outputs', *Living Reviews in European Governance*, 3(5), 1–30.

- Treib, O.; Bähr, H. and Falkner, G. (2007), 'Modes of governance: Towards a conceptual clarification', *Journal of European Public Policy*, 14, 1–20.

- Treib, O. (2003), 'Die Umsetzung von EU-Richtlinien im Zeichen der Parteipolitik: Eine akteurszentrierte Antwort auf die Misfit-These', *Politische Vierteljahresschrift*, 44(4), 506–528.

- Trondal J. and Jeppesen L. (2008), 'Images of Agency Governance in the European Union', *West European Politics*, 31, 417–441.

- Trstenjak, V. (2013), 'National 368overeignty and the Principle of Primacy in EU Law and Their Importance for the Member States', *Beijing Law Review*, 4(2), 71–76.

- Trubek, D. M., and L. G. Trubek (2005), 'Hard and Soft Law in the Construction of Social Europe: The Role of the Open Method of co-Ordination', *European Law Journal*, 11(3), 343–364.

- Tsebelis G., (1995), 'Decision- Making in Political Systems!: Veto Players in Presidentialism, Parliamentarism, Multicameralism and Multipartyism', *British Journal of Political Science*, 25(3), 289-325.

- Van Wolleghem P. G., (2017), 'Why Implement without a Tangible Threat? The Effect of a Soft Instrument on National Migrant Integration Policies', *JCMS: Journal of Common Market Studies*, 55, 1127–1143.

- Versluis, E. (2007), 'Even rules, uneven practices: Opening the 'black box' of EU law in action', *West European Politics*, 30(1), 50–67.

- Virally, M. (1960), *La pensée juridique*, coll. « Les introuvables » des éditions Panthéon-Assas, rééd. 1998, Droit et Société Année 1999 42-43 pp. 577-580

- Von Solms, R., Van Niekerk, J. (2013), 'From information security to cyber security', *Computers & Security*, 38, 97–102.

- Weber, V. (2018), 'Linking cyber strategy with grand strategy: The case of the United States', *Journal of Cyber Policy*, 3, 236–257.

- Wenander, H. (2020), 'Administrative Constitutional Review in Sweden: Between Subordination and Independence', *European Public Law*, 26(4), 987–1010.

- Wessel, R. A. (2003), 'The State of Affairs in EU Security and Defence Policy: The Breakthrough in the Treaty of Nice', *Journal of conflict and security law*, 8(2), 265–288.

- Winter, J. A. (1972), 'Direct Applicability and Direct Effect Two Distinct and Different Concepts in Community Law', *Common Market Law Review*, 9(4), 425–438.

- Wolff, J. (2016), 'What we talk about when we talk about cybersecurity: security in internet governance debates', *Internet Policy Review*, 5(3).

- Zhelyazkova, A.; Kaya, C. and Schrama, R. (2016), 'Decoupling practical and legal compliance: Analysis of Member States' implementation of EU policy', *European Journal of Political Research*, 55(4), 827–846.

- Zhelyazkova, A. (2013), 'Complying with EU directives' requirements: the link between EU decision-making and the correct transposition of EU provisions', *Journal of European Public Policy*, 20(5), 702–721.

- Zhelyazkova, A. and Torenvlied, R. (2011), 'The successful transposition of European provisions by Member States: Application to the Framework Equality Directive', *Journal of European Public Policy*, 18(5), 690–708.

- Zhelyazkova, A. and Torenvlied, R. (2009), 'The time-dependent effect of conflict in the council on delays in the transposition of EU directives', *European Union Politics*, 10(1), 35–62.

Working/Research Paper:

- Bannelier-Christakis, K. (2019), 'Laws of Gravitation. Due diligence Obligations in Cyberspace', in P. Pawlak, T. Biersteker eds., Guardian of the Galaxy. EU Cyber Sanctions and Norms in Cyberspace, Chaillot Paper 155, oct. 2019, 62-69

- Bendiek, A. (2018), 'The EU as a force for peace in international cyber diplomacy', SWP Comment, 19/2018, Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit.

- Berglund, S., Gange, I., and Van Waarden F. (2005), 'Taking institutions seriously: a sociological institutionalist approach to explaining transposition delays of European food safety and utilities directives'. Paper presented at the Joint Sessions of Workshops, European Consortium for Political Research, 14–19 April, Granada.

- Blauberger, M. (2008) From Negative to Positive Integration? European State Aid Control Through Soft and Hard Law, MaxPlanck-Institut für Gesellschaftsforschung, Discussion Paper 08/4

- Börzel, T.A. (2003). Shaping and Taking EU Policies: Member States Responses to Europeanization, Queen's Papers on Europeanization, 2.

- Börzel, T. A.; Dudziak, M.; Hoffman, T.; Panke, D.; Sprungk, C. (2007), Recalcitrance, Inefficiency, and Support for European Integration: Why Member States Do (Not) Comply with European Law, Harvard University Working Paper

- Börzel, T. A.; Hofmann, T.: Sprungk, C. (2004), Why do states not obey the law? Non-compliance in the European Union, Paper presented at the workshop 'Transposition and Compliance in the European Union', June11–13, Leiden, the Netherlands. Oud-Poelgeest.

- Briatte, F. (2010), La comparaison « pair à pair » dans l'univers des cadres interprétatifs de l'analyse politique comparée. Écrire la comparaison, Jun 2010, Lyon, France.

- Checkel, J.T. (1999). Why Comply? Constructivism, Social Norms and the Study of International Institutions, ARENA Working Papers, n° 24, Oslo: Advanced Research on the Europeanisation of the Nation-State

- Choucri, N.; Gihan Daw, E. and Stuart, M. (2012), 'What is Cybersecurity? Explorations in Automated Knowledge Generation', MIT Political Science Department, Research Paper No. 2012-30.

- Church, Clive H. (1996), European Integration Theory in the 1990s, European Dossier Series, no 33, University of North London.

- Demmke, C. (2001). Towards effective environmental regulation: innovative approaches in implementing and enforcing European environmental law and policy, Harvard Jean Monnet Working Paper 5/01, Cambridge, MA: Harvard Law School.

- Dehousse, R. (2015). The New Supranationalism, Paper prepared for the ECPR General Conference, Montreal, 26-29 August, https://ecpr.eu/Filestore/PaperProposal/281383a5-0285-4417-a613-eed8cd5d36bd.pdf.

- Dimitrova, A.L., and M. Rhinard. 2005. The power of norms in the transposition of EU directives. European Integration Online Papers 9, no. 16.

- Falkner, G. and Treib, O. (2007), Three Worlds of Compliance or Four? The EU15, Compared to New Member States, Political Science Series, 112, Institute for Advanced Studies, Vienna

- George, S. (2001), The Europeanization of UK Politics and Policy-Making: the effect of European Integration in the UK, Queen's Papers on Europeanisation, Queen's University Belfast

- Guiliani, M. (2004), 'EU Compliance Macro, Meso, or No Institution at All', URGE Working Paper 6

- International Association of Insurance Supervisors (2016). Issues Paper on Cyber Risk To The Insurance Sector

- Kaufmann, D., Kraay, A., and Mastruzzi, M. (2006). Governance Matters VI: Governance Indicators for 1996–2006. World Bank Policy Research Working Paper No. 4280.

- Kelemen, D. and Mc Namara, K. (2017), How Theories of State-building Explain the EU, European Union Studies Association Bi-Annual Conference Miami, Florida

- Knill, C. and Lenschow, A. (2003), Modes of regulation in the governance of the European Union: Towards a comprehensive framework, European Integration online Papers (EioP), 7(1).

- Lamers, K. and Schäuble, W. (1994), Überlegungen zur europäischen Politik, Bonn, Christlich Demokratische Union/Christlich-Soziale Union.

- Libicki, Martin C. (2015), Sharing Information about Threats is not a Cybersecurity Panacea, Santa Monica, Calif.: RAND Corporation. CT-425.

- March, J. and Olsen, J. (2005). Elaborating the New Institutionalism. Arena Center for European Studies. University of Olso. Working Paper (11).

- Matthews, D. (1993) 'Enforcement of Health and Safety Law in the UK, Germany, France and Italy', Economic & Social Research Council Working Paper 18, London: National Institute of Economic and Social Research, p. 2

- Neyer, J. and Zürn, M. (2001) Compliance in Comparative Perspective. The EU and Other International Institutions, InIIS-Arbeitspapier, Nr. 23/01, Universität Bremen, p. 4

- Pernice, I. and Constantinesco, V. (2002), La question des compétences communau aires : vFranFrancene et de France, Walter Hallstein-Institut, Paper 6/02

- Portela, C. (2019) 'The Spread of Horizontal Sanctions', https://www.ceps.eu/the-spread-of-horizontal-sanctions

- Ramunno, G. (2014). EU Cyberdefence Strategy. European Union Military Committee, Vol. 6, May 2014

- Renard, T. (2014), Partners in Crime? The EU, its Strategic Partners, and International Organised Crime, ESPO Working Paper No. 5, European Strategic Partnership Observatory, p. 13

- Schmidt, Vivien A. (2016). The New EU Governance: New Intergovernmentalism, New Supranationalism, and New Parliamentarism, Istituto Affari Internazionali (IAI), Working Papers, 16 – 11 May.

- Skierka, I.; Morgus, R.; Hohmann, M. and Maurer T. (2015), CSIRT Basics for Policy-Makers – The History, Types & Culture of Computer Security Incident Response Teams, Transatlantic Dialogues on Security and Freedom in the Digital Age, Global Public Policy Institute

- Sverdrup, U. (2004), Compliance: a matter of ability? The role of government capacity in EU compliance, paper for the Workshop on Transposition and Compliance in the European Union, Oud-Poelgeest, Leyden.

- Tikk-Ringas, E. (2015), Comprehensive Normative Approach to Cyber Security. ICT4PEACE Norms project, Concept Paper.

- Toshkov, D. (2010), Taking stock: a review of quantitative studies of transposition and implementation of EU law, Working paper No. 01/2010, Institute for European Integration Research.

- Treib, O. (2003). EU governance, misfit, and the partisan logic of domestic adaptation: an actor-centred perspective on the transposition of EU directives, Paper presented at the EUSA 8th International Biennial Conference, Nashville Tennessee, 27 – 29 March 2003.

- Trubek, D.; Cottrell, M. and Nance, M. (2005), "Soft Law", "Hard Law", and European Integration: Toward a Theory of Hybridity, University of Wisconsin Legal Studies Research Paper No. 1002

- Warin, P. (20 0), Le non-recours : définition et typologies, Observatoire des non-recours aux droits et services, Document de Travail No. 1 (Juin).

- Young, M. (2015), Update on the cybersecurity directive – over to Luxembourg?, The National Law Review, https://www.natlawreview.com/article/update-cybersecurity-directive-over-to-luxembourg.

- Zaborowski, M. (2005), Germany and EU Enlargement: From Rapprochement to 'Reaproachment'?. In: Sjursen, H. (eds.), Enlargement in perspective, The EU's Quest for identity. Oslo : ARENA, Working Paper No. 5.

Doctoral Thesis:

- Mastenbroek, E. (2007), The politics of compliance: explaining the transposition of EC directives in the Netherlands, Doctoral Thesis, Department of Public Administration, Faculty of Social and Behavioural Sciences, Leiden University

Online Documents:

- Christakis, T. 'Schrems III"? First thoughts on the EDPB post-Schrems II recommendations on international data transfers, Part III,' [Online Article], 17 November 2020, *European Law Blog*, available at https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/ (accessed on April 4th, 2022)

- Christakis, T. 'Schrems III ? First thoughts on the EDPB post-Schrems II recommendations on international data transfers, Part II,' [Online Article], 16 November 2020, *European Law Blog*, available at https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/ (accessed on April 4th, 2022)

- Christakis, T. 'Schrems III? First thoughts on the EDPB post-Schrems II recommendations on international data transfers, Part I,' [Online Article], 13 November 2020, *European Law Blog*, available at

https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ (accessed on April 4th, 2022)

- Christakis, T. 'After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe', [Online Article], 21 July 2020, *European Law Blog*, available at https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/ (accessed on April 4th, 2022)

- Cirlig, C.-C. 'Cyber defence in the EU, Preparing for cyber warfare?', [Online Article], October 2014, *European Parliamentary Research Service*, available at https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf (accessed on November 11th, 2019)

- EEAS 3rd EU-Japan Cyber Dialogue – Joint Eléments, [Press release], 14 March 2018, available at: https://eeas.europa.eu/topics/eu-international-cyberspace-policy/41330/3rd-eu-%E2%80%93-japan-cyberdialogue-joint-elements_en, (accessed on February 24th, 2021)

- EEAS, EU-US Cyber Dialogue, [Press release], 16 December 2016, Brussels, Available at https://eeas.europa.eu/headquarters/headquarters-homepage_en/18132/EU-U.S.%20Cyber%20Dialogue, accessed on February 24th, 2021.

- European Parliament, 'The EU's Mutual Assistance Clause: The First Ever Activation of Article 42(7) TEU', [Online Article], 27 November 2015, European Parliamentary Research Ser–ice, available at - http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)572799 (accessed on November 6th, 2019)

- Homburger, Z. 'Conceptual Ambiguity of International Norms on State Behaviour in Cyberspace', [Online Article], 4 April 2019, *EU Cyber Direct*, available at https://eucyberdirect.eu/wp-content/uploads/2019/05/zine-homburger-conceptual-ambiguity-of-norms-april-2019-eucyberdirect.pdf (accessed on July 28th, 2020)

- Soesanto, S. 'Europe Has No Strategy on Cyber Sanctions', [Online Article], 20 November 2020, available at https://www.lawfareblog.com/europe-has-no-strategy-cyber-sanctions (accessed on July 28th, 2020).

- NATO, Development Of The European Security And Defence Identity (ESDI) Within NATO, Article, 1994. Available at https://www.nato.int/docu/comm/1999/9904-wsh/pres-eng/05esdi.pdf (accessed on February 26th, 2021).

- NATO, Summit Meeting of Heads of State and Government, Article, 10-11 January 1994. Available at https://www.nato.int/cps/en/natohq/events_65255.htm (accessed on February 26th, 2021)

NATO, Ministerial Meeting of the North Atlantic Council (NAC) / North Atlantic Cooperation Council (NACC) Berlin, Article, 3-4 July 1996, Available at https://www.nato.int/docu/comm/1996/9606-brl/9606-brl.htm (accessed on February 26th, 2021)

Reports / Studies:

- Batta, D. (2007), Comparative study on the transposition of EC Law in the Member States, European Parliament, Committee on Legal Affairs

- Biscop, S. (2017), Differentiated integration in defence: a plea for PESCO. Instituto Affari Internazionali.

- Cohen-Tanugi, L. (2002), L'Influence normative internationale de l'Union européenne : une ambition entravée. Les Notes de l'IFRI, 40, p. 1-54.

- Conseil d'Etat (2015), Anticiper pour mieux transposer, Rapport d'étude, November, Ed. La Documentation française

- Cooperation Group (2018), Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact, CG Publication 07/2018

- Cooperation Group (2018), Reference document on security measures for OES, CG Publication 01/2018

- Directorate general for internal policies, Committee on civil liberties, justice, and home affairs (2015), Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, PE 536.470

- ENISA (2019), Study on CSIRT landscape and IR capabilities in Europe 2025

- ENISA (2018), Guidelines on assessing DSP and OES compliance to the NIS Directive security requirements

- ENISA (2018), Good practices on interdependencies between OES and DSPs

- ENISA (2018), EU Cybersecurity Institutional Map, Stock-taking and analysis of the roles and responsibilities of EU Institutions and bodies in cybersecurity

- ENISA (2018), Reference Incident Classification Taxonomy, Task Force Status and Way Forward

- ENISA (2017), Mapping of OES Security Requirements to Specific Sectors

- ENISA (2017), Study on CSIRT Maturity – Evaluation Process

- ENISA and European Parliament's Science and Technology Options Assessment (2017), Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU, EPRS/STOA/SER/16/214N

- ENISA (2017), Incident notification for DSPs in the context of the NIS Directive, A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive

- ENISA (2016), NCSS Good Practice Guide

- ENISA (2016), Technical Guidelines for the implementation of minimum-security measures for Digital Service Providers

- ENISA (2016), Report on Gaps in N–S standardisation - Recommendations for improving NIS in EU standardisation policy

- ENISA (2016), CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs

- ENISA (2015), Leading the way ENISA's CSIRT-related capacity building activities, Impact Analysis

- ENISA (201–), CERT community - Recognition mechanisms and schemes

- ENISA (2012), Report on Cyber Incident Reporting in the EU : an overview of security articles in EU legislation

- ENISA (2012), National Cybersecurity Strategies

- ENISA (2012), The Fight against Cybercrime, Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime

- ENISA (2006), CSIRT Setting up Guide in English

- European Union Agency for Law Enforcement Cooperation, (2019), Internet Organised Crime Threat Assessment (IOCTA).

- Ojanen, H. (2006) The EU and the UN: a shared future, (2006), Finnish Institute of International Affairs Report 13

- Jaume-Palasí, L.; Gierow, H. (2014), Germany, In: Davies, S. (eds.), A Crisis of ccountability: A global analysis of the impact of the Snowden revelations

- Klimburg, A. and Heli, T.-K. (2011), Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU, Study for the European Parliament's Subcommittee on Security and Defence.

- Ladid, L.; Armin, J. and Kivekäs, H. (2019), The finish Electronic Communications –egulator TRAFICOM - A Cybersecurity Reference Model for Europe. Helsinki: SAINT Consortium/ Traficom.

- Martin, E.-A. (2019),'The European Union's sanctions policy. Multilateral Ambition vs. Power'Logic. Etudes de l'Ifri, pp. 1-46.

- Moret, E. and Pawlak, P. (2017), The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? Policy Brief, European Union Institute for Security Studies (EUISS), July 2017

- NIS Cooperation Group (Feb. 2018), Reference document on security measures for Operators of Essential Services, CG Publication 01/2018

- NIS Cooperation Group (Feb. 2018), Reference document on Incident Notification for Operators of Essential Services, Circumstances of notification, CG Publication 02/2018

- NIS Cooperation Group (July 2018), Cybersecurity Incident Taxonomy, CG Publication 04/2018

- NIS Cooperation Group (July 2018), Guidelines on notification of Operators of Essential Services incidents, Formats and procedures, CG Publication 05/2018

- NIS Cooperation Group (July 2018), Guidelines on notification of Digital Service Providers incidents, Formats and procedures, CG Publication 06/2018

- NIS Cooperation Group (July 2018), Identification of Operators of Essential Services, Reference document on modalities of the consultation process in cases with cross-border impact, CG Publication 07/2018

- Steunenberg B. and Voermans W. (2006), The transposition of EC directives: A comparative study of instruments, techniques, and processes in six Member States, Leiden University and WODC/Ministry of justice, p.121

- Van der Meulen, N. and Soesanto, S. (2015), Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses. Study, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs. https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf

Official documents:

EU:

Charters:

- Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407

Communications:

- European Commission, (2020), Joint communication to the European Parliament and the Council on the EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final, 16.12.2020, Brussels

- European Commission, (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Shaping Europe's digital future', COM(2020) 67 final, Brussels, 19.2.2020

- European Commission, (2018), Joint Communication to the European Parliament, the European Council and the Council, Increasing resilience and bolstering capabilities to address hybrid threats, JOIN(2018) 16 final

- European Commission (2017), Communication on Completing the Better Regulation Agenda: Better solutions for better results COM (2017) 651 final.

- European Commission. (2017). Joint Communication to The European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final, 13.09.2017

- European Commission, (2017), Communication 'Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union', COM(2017) 476 final/2

- European Commission, (2016), Joint Communication to the European Parliament and the Council on a "Joint Framework on countering hybrid threats - a European Union response", JOIN(2016) 18 final

- European Commission (2016), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final

- European Commission, (2016), Communication to the European Parliament, the European Council, and the Council on a Better Regulation: Delivering better results for a stronger Union, COM/2016/0615 final

- European Commission, (2015), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on A Digital Single Market Strategy for Europe, COM(2015) 192 final

- European Commission, (2015), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on The European Agenda on Security, COM(2015) 185 final

- European Commission, (2015), Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Better regulation for better results - An EU agenda, COM/2015/0215 final

- European Commission's HR/VR (2013), Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN (2013) 1 final.

- European Commission, (2012), Communication on “A coherent framework for building trust in the Digital Single Market for e-commerce and online services”, COM(2011) 942 final

- European Commission, (2011), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – “Achievements and next steps: towards global cyber-security”, COM(2011) 163 final

- European Commission, (2010), Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, 16797/10 JAI 990

- European Commission, (2010), Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions, A Digital Agenda for Europe, COM(2010)245 final

- European Commission, (2009), Communication from the Commission on Critical Information Infrastructure Protection – ‘Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience’, COM(2009) 149 final

- European Commission (2007) “Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cybercrime”, COM (2007) 267 final, 22 May.

- European Commission, (2006), Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP), COM(2006) 786 final

- European Commission, (2006), Communication from the commission on “A strategy for a Secure Information Society – “Dialogue, partnership and empowerment”, COM(2006) 251 final

- European Commission, (2005), Communication from the commission on “i2010 – A European Information Society for growth and employment”, COM(2005)229 final

- European Commission (2004), Communication from the Commission to the Council and the European Parliament on Critical Infrastructure Protection in the fight against terrorism, COM(2004)702 final

- European Commission, (2001), Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 final

Conclusions:

- European Council, (2018) 'European Council meeting (28 June 2018) – Conclusions', EUCO 9/18, Brussels.

- Council of the European Union (2018), Council conclusions on EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises, 10086/18

- Council of the European Union. (2017, June 19). Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox').

- Council of the European Union (2011), Draft Council conclusions on the Commission communication on the European Union internal security strategy in action, 6699/11 JAI 124

- European Council (2009), Conclusions on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014), 17024/09

- European Council, (2001), Göteborg Presidency conclusions on European Security and Defense Policy, Brussels

Decisions:

- Council of the European Union. (2020). Decision (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

- Council of the European Union. (2019). Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

- Council of the European Union, (2017), Council Decision (CFSP) 2017/2315 of 11 December 2017, establishing Permanent Structured Cooperation (PESCO) and Determining the List of Participating Member States, L 331/57

- Council of the European Union (2014), Council Decision 2014/415/EU on the Arrangements for the Implementation by the Union of the Solidarity Clause, O.J. (L 192) 53

- Council of the European Union (2011). Decision 2011/411/CFSP of 12 July 2011 defining the statute, seat and operational rules of the European Defence Agency and repealing Joint Action 2004/551/CFSP, 13.07.2011, L 183/16

- Council of the European Union. (2005, September 29). Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences. L253. (O. J. EU, Ed.)

- Council of the European Union (2005, September 20). Decision 2005/681/JHA establishing the European Police College (CEPOL) and repealing Decision 2000/820/JHA, OJ L 256, 1.10.2005, p. 63–70

- Council of the European Union (2005), Council Framework Decision 2005/222/JHA on attacks against information systems

- Council of the European Union (2002), Council Framework Decision on Combatting Terrorism, 2002/475/JHA

- Council of the European Union. (2000). Decision of 22 December 2000 establishing a European Police College (CEPOL), OJ L 336, 30.12.2000, p. 1–3

- European Council, (2019), 'Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States', 7299/19, 14.05.2019, Brussels.

Directives:

- Council of the European Union (2008), Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 2008/114/EC, OJ L 345, 23.12.2008, p. 75–82.

- Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ, L 95, p. 29

- Council Directive 89/665/EEC of 21 December 1989 on the coordination of the laws, regulations and administrative provisions relating to the application of review procedures to the award of public supply and public works contracts OJ L 395, p. 33

- European Commission, (2017), Directive (EU) 2017/541 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and Amending Council Decision 2005/671/JHA

- European Commission, (2016), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

- European Commission, (2016), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016, L 119/89-131.

- European Commission, (2006), Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63

- European Commission (2002), Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)

- European Parliament and Council of the European Union, Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)Text with EEA relevance, PE/52/2018/REV/1, OJ L 321, 17.12.2018, p. 36–214

- European Parliament and Council of the European Union, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA OJ L 119, 4.5.2016, p. 89–131

- European Parliament and Council, (2007). Directive 2007/66/EC of 11 December 2007 amending Council Directives 89/665/EEC and 92/13/EEC with regard to improving the effectiveness of review procedures concerning the award of public contracts (Text with EEA relevance), OJ L 335, p. 31

- European Parliament and the Council, (2002). Directive 2002/65/EC of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC, OJ L 271, 9.10.2002, p. 16–24

- European Parliament and the Council, (2002). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47

- European Parliament and the Council, (2000). Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16

- European Parliament and the Council, (1999). Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures OJ L 13, 19.1.2000, p. 12–20

- European Parliament and Council, (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 , 23.11.1995, p. 31 - 50

Divers:

- Commission of the European Communities, White paper from the Commission to the European Council, 28-29 June 1985, COM(85) 310 final

- Council of the European Union. (2020). Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack.

- Council of the European Union. (2020). Council extends cyber sanctions regime until 18 May 2021.

- Council of European Union. (2019). Permanent Structured Cooperation (PESCO) Projects: Overview.

- Council of the European Union. (2017, December 19). Annual Report on the Implementation of the Cyber Defence Policy Framework. 15870/17.

- Council of the European Union. (2017, December 08). Guidelines on the implementation and evaluation of restrictive measures (sanctions) within the framework of the EU's common foreign and security policy. 15598/17.

- Council of the European Union. (2016). Establishment of a Horizontal Working Party on Cyber Issues- Terms of Reference, 11913/2/16.

- Council of the European Union. (2014, December 19). European Union Concept for EU-led Military Operations and Missions. 17107/14.

- Council of the European Union. (2014, November 18). EU Cyber Defence Policy Framework. 15585/14

- Council of the European Union. (2014, June 27). Opinion of the legal service on NIS directive proposal legal basis, 11395/14

- Council of the European Union. (2011). CIIP "Achievements and next steps: towards global cyber-security" - Adoption of Council conclusions - 10299/11

- Council of the European Union. (2003). Sanctions Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy. 15579/03

- Council of the European Union. (2001). Common Position of 27 December 2001 on the application of specific measures to combat terrorism. L344. (O. J. EU, Ed.)

- EEAS. (2016), Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy

- Estonian Presidency of the Council of the EU. (2017). EU Sanctions Map Site.

- European Commission (2017), EU Law: Better results through better application, COM 2017/C 18/02, 19, January, p.15-16

- European Commission (2017), State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks, Press release

- European Commission (2016), Monitoring the application of European Union law, 2015 Annual Report, COM (2016) 463 final, p. 30

- European Commission. (2014). The Juncker Commission: A Strong and Experienced Team Standing for Change. Press Release: IP/14/984, September 10

- European Commission, (2013), Impact assessment accompanying proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union, SWD(2013) 32 final

- European Commission, (2012), Commission staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD(2012) 190 final

- European Commission, (2005). Lisbon Action Plan Incorporating EU Lisbon Programme And Recommendations For Actions To Member States For Inclusion In Their National Lisbon Programmes, COM (2005) 24/ SEC (2005) 192.

- European Commission (2005), Green Paper of 17 November 2005 on a European programme for critical infrastructure protection, COM(2005)576 final

- European Council. (2001, December 14-15). Laeken Declaration on the Future of the European Union. 12. (B. o. EU, Ed.)

- European Data Protection Supervisor. (2020). EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II"), 17.07.2020, Brussels.

- European Defence Agency. 21 November 2005. Code of Conduct on Defence Procurement, 21 November, Brussels: EDA.

Implementing Decision/Regulation:

- European Commission (2017), Implementing decision (EU) 2017/179 laying down procedural arrangements necessary for the functioning of the Cooperation Group

- European Commission, (2018), Implementing Regulation (EU) 2018/151 laying down rules for application of Directive (EU) 2016/1148

Proposals:

- European Commission. (2020) 'Proposal for a Directive of The European Parliament and Of The Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148', COM(2020) 823 final, Brussels, 16.12.2020.

- European Commission (2018), Proposal for a regulation of the European parliament and of the Council, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, COM(2018) 630 final

- European Commission (2017), Proposal for a Regulation on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM(2017)477 final

- European Commission, (2013), Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM/2013/048 final - 2013/0027 (COD)

- European Commission (2012), Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.

- European Commission (2001), Network and Information Security: Proposal for A European Policy Approach, COM(2001)298 final

Recommendation:

- European Commission (2017), Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises, C/2017/6100

Regulations:

- Council of the European Union, Council Implementing Regulation (EU) 2020/1744 of 20 November 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 393, 23.11.2020, p. 1–2.

- Council of the European Union, Council Implementing Regulation (EU) 2020/1536 of 22 October 2020 of implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, OJ L 351I , 22.10.2020, p. 1–4.

- Council of the European Union, Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, ST/9568/2020/INIT, OJ L 246, 30.7.2020, p. 4–9;

- Council of the European Union, Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive meas-ures against cyber-attacks threatening the Union or its Member States', L129 I/1.

- Council of the European Union, Regulation (EC) No 2580/2001 of 27 December 2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism, L344.

- European Parliament and Council of the European Union, Regulation (EU) 2021/887 of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, PE/28/2021/INIT, OJ L 202, 8.6.2021, p. 1–31

- European Parliament and Council of the European Union, Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

- European Parliament and Council of the European Union, Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, PE/37/2018/REV/1, OJ L 295, 21.11.2018, p. 138–183

- European Parliament and Council of the European Union, (2016) Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88

- European Parliament and Council of the European Union, (2014). Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114

- European Parliament and of the Council (2018). Regulation (EU) 2018/1807 of the of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, PE/53/2018/REV/1, OJ L 303, 28.11.2018, p. 59–68

- European Parliament and Council, (2004). Regulation (EC) No 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency.

Resolutions:

- Council of the European Union (2007), Council Resolution on a Strategy for a Secure Information Society in Europe, 2007/C 68/01

Reports:

- European Commission (2019), Report from the commission to the European Parliament and The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, COM(2019) 546 final

- European Commission (2017), Final report on the Evaluation of the European Union Agency for Network and Information Security (ENISA)

- European Commission, (2008), Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, COM(2008) 448 final

International:

- United Nations 'Russian Federation Revised Draft Resolution on Developments in the field of information and telecommunications in the context of international security', 2 November 1998, Doc. A/C.1/53/L.17/Rev.1

- United Nations 'Developments in the field of information and telecommunications in the context of international security', 4 January 1999, Doc. A/RES/53/70

- United Nations' Security Council 'Threats to international peace and security caused by terrorist acts', 28 September 2001, S/RES/1373

Jurisprudence:

Court of Justice of the European Union:

Single Cases

- Case **C-645/19**, Opinion of Advocate General Bobek delivered on 13 January 2021. Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit. Request for a preliminary ruling from the Hof van beroep te Brussel. Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Charter of Fundamental Rights of the European Union – Articles 7, 8 and 47 – Regulation (EU) 2016/679 – Cross-border processing of personal data – 'One-stop shop' mechanism – Sincere and effective cooperation between supervisory authorities – Competences and powers – Power to initiate or engage in legal proceedings. ECLI identifier: ECLI:EU:C:2021:5

- Case **C-623/17**, Judgment of the Court (Grand Chamber) of 6 October 2020 (request for a preliminary ruling from the Investigatory Powers Tribunal — London — United Kingdom) — Privacy International v Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service (Reference for a preliminary ruling — Processing of personal data in the electronic communications sector — Providers of electronic communications services — General and indiscriminate transmission of traffic data and location data — Safeguarding of national security — Directive 2002/58/EC — Scope — Article 1(3) and Article 3 — Confidentiality of electronic communications — Protection — Article 5 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 11 and Article 52(1) — Article 4(2) TEU), OJ C 433, 14.12.2020, p. 2–3

- Case **C-507/17**, Judgment of the Court (Grand Chamber) of 24 September 2019, Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), Request for a preliminary ruling from the Conseil d'État, Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Regulation (EU) 2016/679 — Internet search engines — Processing of data on web pages — Territorial scope of the right to de-referencing, ECLI:EU:C:2019:772.

- Case **C-712/17**, Judgment of the Court (First Chamber) of 8 May 2019. EN.SA. Srl v Agenzia delle Entrate – Direzione Regionale Lombardia Ufficio Contenzioso. Request for a preliminary ruling from the Commissione Tributaria Regionale per la Lombardia. Reference for a preliminary ruling — Value added tax (VAT) — Fictitious transactions — Impossibility of deducting the tax — Obligation on the issuer of an invoice to pay the VAT indicated thereon — Fine in an amount equal to the amount of the improperly deducted VAT — Whether compatible with the principles of VAT neutrality and proportionality. Digital reports (Court Reports - general), ECLI identifier: ECLI:EU:C:2019:374

- Case **C-266/16**, Judgment of the Court (Grand Chamber) of 27 February 2018. Western Sahara Campaign UK v Commissioners for Her Majesty's Revenue and Customs and Secretary of State for Environment, Food and Rural Affairs. Request for a preliminary ruling from the High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court). Reference for a preliminary ruling — Fisheries Partnership Agreement between the European Community and the Kingdom of Morocco — Protocol setting out the fishing opportunities provided for by the agreement — Acts approving the conclusion of the agreement and of the protocol — Regulations allocating among the Member States the fishing opportunities set out by the protocol — Jurisdiction — Interpretation — Validity having regard to Article 3(5) TEU and international law — Applicability of that agreement and that protocol to the territory of Western Sahara and the waters adjacent thereto. Digital reports (Court Reports - general - 'Information on unpublished decisions' section). ECLI identifier: ECLI:EU:C:2018:118

- Case **C-687/15**, Judgment of the Court (Grand Chamber) of 25 October 2017. European Commission v Council of the European Union. Action for annulment — Conclusions of the Council of the European Union concerning the World Radiocommunication Conference 2015 of the International Telecommunication Union — Article 218(9) TFEU — Derogation from the prescribed legal form — No indication of the legal basis. Digital reports (Court Reports - general - 'Information on unpublished decisions' section). ECLI identifier: ECLI:EU:C:2017:803

- Case **C-54/16**, Judgment of the Court (Fifth Chamber) of 8 June 2017, Vinyls Italia SpA v Mediterranea di Navigazione SpA, Request for a preliminary ruling from the Tribunale Ordinario di Venezia, Reference for a preliminary ruling — Area of freedom, security and justice — Insolvency proceedings — Regulation (EC) No 1346/2000 — Articles 4 and 13 — Acts detrimental to all the creditors — Conditions in which the act in question may be challenged — Act subject to the law of a Member State other than the State of the opening of proceedings — Act which is not open to challenge on the basis of that law — Regulation (EC) No 593/2008 — Article 3(3) — Law chosen by the parties — Location of all the elements of the situation concerned in the State of the opening of proceedings — Effect. OJ C 249, 31.7.2017, p. 8–9.

- Case **C-362/14**, Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner; Request for a preliminary ruling from the High Court (Ireland), Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities, ECLI:EU:C:2015:650

- Case **C-62/14**, Judgment of the Court (Grand Chamber) of 16 June 2015. Peter Gauweiler and Others v Deutscher Bundestag. Request for a preliminary ruling from the Bundesverfassungsgericht. Reference for a

preliminary ruling — Economic and monetary policy — Decisions of the Governing Council of the European Central Bank (ECB) on a number of technical features regarding the Eurosystem's outright monetary transactions in secondary sovereign bond markets — Articles 119 TFEU and 127 TFEU — Powers conferred on the ECB and the European System of Central Banks — Monetary policy transmission mechanism — Maintenance of price stability — Proportionality — Article 123 TFEU — Prohibition of monetary financing of Member States in the euro area. Digital reports (Court Reports - general). ECLI identifier: ECLI:EU:C:2015:400

- Case **C-131/12**, Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Request for a preliminary ruling from the Audiencia Nacional, Personal data — Protection of individuals with regard to the processing of such data — Directive 95/46/EC — Articles 2, 4, 12 and 14 — Material and territorial scope — Internet search engines — Processing of data contained on websites — Searching for, indexing and storage of such data — Responsibility of the operator of the search engine — Establishment on the territory of a Member State — Extent of that operator's obligations and of the data subject's rights — Charter of Fundamental Rights of the European Union — Articles 7 and 8. ECLI:EU:C:2014:317

- Case **C-285/12**, Judgment of the Court (Fourth Chamber), 30 January 2014. Aboubacar Diakité v Commissaire général aux réfugiés et aux apatrides. Request for a preliminary ruling from the Conseil d'État (Belgium). Directive 2004/83/EC — Minimum standards for granting refugee status or subsidiary protection status — Person eligible for subsidiary protection — Article 15(c) — Serious and individual threat to a civilian's life or person by reason of indiscriminate violence in situations of armed conflict — 'Internal armed conflict' — Interpretation independent of international humanitarian law — Criteria for assessment. Digital reports (Court Reports - general). ECLI identifier: ECLI:EU:C:2014:39

- Case **C-270/12**, Judgment of the Court (Grand Chamber), 22 January 2014. United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union. Regulation (EU) No 236/2012 — Short selling and certain aspects of credit default swaps — Article 28 — Validity — Legal basis — Powers of intervention conferred on the European Securities and Markets Authority in exceptional circumstances. Digital reports (Court Reports - general). ECLI identifier: ECLI:EU:C:2014:18

- Case **C-425/12**, Judgment of the Court (Fifth Chamber), 12 December 2013, Portgás — Sociedade de Produção e Distribuição de Gás SA v Ministério da Agricultura, do Mar, do Ambiente e do Ordenamento do Território. Request for a preliminary ruling from the Tribunal Administrativo e Fiscal do Porto, Procedures for awarding public contracts in the water, energy, transport, and telecommunications sectors — Directive 93/38/EEC — Directive not transposed into national law — Whether the State may rely on that directive against a body holding a public service concession in the case where that directive has not been transposed into national law, Digital reports (Court Reports – general), ECLI:EU:C:2013:829

- Case **C-172/11**, Judgment of the Court (Second Chamber), 28 June 2012, Georges Erny v Daimler AG - Werk Wörth, Reference for a preliminary ruling from the Arbeitsgericht Ludwigshafen am Rhein, Freedom of

movement for workers — Article 45 TFEU — Regulation (EEC) No 1612/68 — Article 7(4) — Principle of non-discrimination — Top-up amount on wages paid to workers placed on a scheme of part-time work prior to retirement — Cross-border workers subject to income tax in the Member State of residence — Notional taking into account of the tax on wages of the Member State of employment, Digital reports (Court Reports – general), ECLI:EU:C:2012:399.

- Case **C-210/10**, Judgment of the Court (First Chamber), 9 February 2012. Márton Urbán v Vám- és Pénzügyőrség Észak-alföldi Regionális Parancsnoksága. Reference for a preliminary ruling from the Hajdú-Bihar Megyei Bíróság. Road transport — Breach of the rules on the use of the tachograph — Obligation on Member States to establish proportionate penalties — Flat-rate fine — Proportionality of the penalty. Digital reports (Court Reports - general), ECLI identifier: ECLI:EU:C:2012:64.

- Case **C-352/09 P**, Judgment of the Court (Grand Chamber) of 29 March 2011. ThyssenKrupp Nirosta GmbH v European Commission. Appeals - Competition - Agreements, decisions and concerted practices - Community market in stainless steel flat products - Decision finding an infringement of Article 65 CS after the expiry of the ECSC Treaty on the basis of Regulation (EC) No 1/2003 - Powers of the Commission - Principles of nulla poena sine lege and res judicata - Rights of the defence - Attributability of the unlawful conduct - Transfer of liability by means of a statement - Limitation period - Cooperation during the administrative procedure. European Court Reports 2011 I-02359. ECLI identifier: ECLI:EU:C:2011:191

- Case **C-366/10**, Judgment of the Court (Grand Chamber) of 21 December 2011. Air Transport Association of America and Others v Secretary of State for Energy and Climate Change. Reference for a preliminary ruling: High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) - United Kingdom.

Reference for a preliminary ruling - Directive 2003/87/EC - Scheme for greenhouse gas emission allowance trading - Directive 2008/101/EC - Inclusion of aviation activities in that scheme - Validity - Chicago Convention - Kyoto Protocol - EU-United States Air Transport Agreement - Principles of customary international law - Legal effects thereof - Whether they may be relied upon - Extraterritoriality of European Union law - Meaning of 'charges', 'fees' and 'taxes'. European Court Reports 2011 -00000. ECLI identifier: ECLI:EU:C:2011:864

- Case **C-582/08**, Judgment of the Court (Third Chamber) of 15 July 2010 — European Commission v United Kingdom of Great Britain and Northern Ireland (Failure of a Member State to fulfil obligations — Value-added tax — Directive 2006/112/EC — Articles 169 to 171 — Thirteenth Directive 86/560/EEC — Article 2 — Refund — Taxable person not established in the European Union — Insurance transactions — Financial transactions). OJ C 246, 11.9.2010, p. 4–4

- Case **C-28/08**, Judgment of the Court (Grand Chamber) of 29 June 2010. European Commission v The Bavarian Lager Co. Ltd. Appeal - Access to the documents of the institutions - Document concerning a meeting held in the context of a procedure for failure to fulfil obligations -Protection of personal data - Regulation (EC) No 45/2001 - Regulation (EC) No 1049/2001. European Court Reports 2010 I-06055. ECLI:EU:C:2010:378

- Case **C-58/08**, Judgment of the Court (Grand Chamber) of 8 June 2010. The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise, and Regulatory Reform. Reference for a preliminary ruling: High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) - United Kingdom. Regulation (EC) No 717/2007 - Roaming on public mobile telephone networks within the Community - Validity - Legal basis - Article 95 EC - Principles of proportionality and subsidiarity. European Court Reports 2010 I-04999. ECLI identifier: ECLI:EU:C:2010:321

- Case **C-101/08**, Judgment of the Court (Fourth Chamber) of 15 October 2009, Audiolux SA e.a v Groupe Bruxelles Lambert SA (GBL) and Others and Bertelsmann AG and Others, Reference for a preliminary ruling: Cour de cassation – Luxembourg, Directives 77/91/EEC, 79/279/EEC and 2004/25/EC - General principle of Community law on the protection of minority shareholders - None - Company law - Acquisition of control - Mandatory bid - Recommendation 77/534/EEC - Code of Conduct, European Court Reports 2009 I-09823, ECLI:EU:C:2009:626.

- Case **C-275/06**, Judgment of the Court (Grand Chamber) of 29 January 2008. Productores de Música de España (Promusicae) v Telefónica de España SAU. Reference for a preliminary ruling: Juzgado de lo Mercantil nº 5 de Madrid - Spain. Information society - Obligations of providers of services - Retention and disclosure of certain traffic data - Obligation of disclosure - Limits - Protection of the confidentiality of electronic communications - Compatibility with the protection of copyright and related rights - Right to effective protection of intellectual property. ECLI:EU:C:2008:54

- Case **C-377/98**, Judgment of the Court of 9 October 2001. Kingdom of the Netherlands v European Parliament and Council of the European Union. Annulment - Directive 98/44/EC - Legal protection of biotechnological inventions - Legal basis - Article 100a of the EC Treaty (now, after amendment, Article 95 EC), Article 235 of the EC Treaty (now Article 308 EC) or Articles 130 and 130f of the EC Treaty (now Articles 157 EC and 163 EC) - Subsidiarity - Legal certainty - Obligations of Member States under international law - Fundamental rights - Human dignity - Principle of collegiality for draft legislation of the Commission. European Court Reports 2001 I-07079. ECLI:EU:C:2001:523

Joined Cases

- Joined Cases **C-203/15 and C-698/15**, Judgment of the Court (Grand Chamber) of 21 December 2016, Reference for a preliminary ruling — Electronic communications — Processing of personal data — Confidentiality of electronic communications — Protection — Directive 2002/58/EC — Articles 5, 6 and 9 and Article 15(1) — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 11 and Article 52(1) — National legislation — Providers of electronic communications services — Obligation relating to the general

and indiscriminate retention of traffic and location data — National authorities — Access to data — No prior review by a court or independent administrative authority — Compatibility with EU law, ECLI:EU:C:2016:970

- Joined Cases **C-293/12 and C-594/12**, Judgment of the Court (Grand Chamber), 8 April 2014. Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof. Electronic communications — Directive 2006/24/EC — Publicly available electronic communications services or public communications networks services — Retention of data generated or processed in connection with the provision of such services — Validity — Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union. Joined Cases C-293/12 and C-594/12. Digital reports (Court Reports - general). ECLI identifier: ECLI:EU:C:2014:238

- Joined Cases **C-29/13 and C-30/13**, Judgment of the Court (First Chamber) of 13 March 2014 (requests for a preliminary ruling from the Administrativen sad Sofia-grad — Bulgaria) — Global Trans Lodzhistik OOD v Nachalnik na Mitnitsa Stolichna (Reference for a preliminary ruling — Community Customs Code — Articles 243 and 245 — Regulation (EEC) No 2454/93 — Article 181a — Decision amenable to review — Admissibility of legal proceedings where a prior administrative complaint has not been made — Principle of respect for the rights of defence). OJ C 135, 5.5.2014, p. 11–12

- Joined Cases **C-428/06 to C-434/06**, Judgment of the Court (Third Chamber) of 11 September 2008. Unión General de Trabajadores de La Rioja (UGT-Rioja) and Others v Juntas Generales del Territorio Histórico de Vizcaya and Others. Reference for a preliminary ruling: Tribunal Superior de Justicia de la Comunidad Autónoma del País Vasco - Spain. State aid - Tax measures adopted by a regional or local authority - Selective nature. Joined cases C-428/06 to C-434/06. European Court Reports 2008 I-06747. ECLI identifier: ECLI:EU:C:2008:488

- Joined Cases **C-402/05 P and C-415/05 P**, Judgment of the Court (Grand Chamber) of 3 September 2008. Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities. Common foreign and security policy (CFSP) - Restrictive measures taken against persons and entities associated with Usama bin Laden, the Al-Qaeda network and the Taliban - United Nations - Security Council - Resolutions adopted under Chapter VII of the Charter of the United Nations - Implementation in the Community - Common Position 2002/402/CFSP - Regulation (EC) No 881/2002 Measures against persons and entities included in a list drawn up by a body of the United Nations - Freezing of funds and economic resources - Committee of the Security Council created by paragraph 6 of Resolution 1267 (1999) of the Security Council (Sanctions Committee) - Inclusion of those persons and entities in Annex I to Regulation (EC) No 881/2002 - Actions for annulment - Competence of the Community - Joint legal basis of Articles 60 EC, 301 EC and 308 EC - Fundamental rights - Right to respect for property, right to be heard and right to effective judicial review. European Court Reports 2008 I-06351. ECLI identifier: ECLI:EU:C:2008:461

Cour of Justice of the European Communities:

Single Cases

- Case **C-94/07**, Judgment of the Court (Fifth Chamber) of 17 July 2008, Andrea Raccanelli v Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV, Reference for a preliminary ruling: Arbeitsgericht Bonn – Germany, Article 39 EC - Concept of 'worker' - Non-governmental organisation operating in the public interest - Doctoral grant - Employment contract – Conditions, European Court Reports 2008 I-05939, ECLI:EU:C:2008:425.

- Case **C-341/05**, Judgment of the Court (Grand Chamber) of 18 December 2007, Laval un Partneri Ltd v Svenska Byggnadsarbetareförbundet, Svenska Byggnadsarbetareförbundets avdelning 1, Byggettan and Svenska Elektrikerförbundet, Reference for a preliminary ruling: Arbetsdomstolen – Sweden, Freedom to provide services - Directive 96/71/EC - Posting of workers in the construction industry - National legislation laying down terms and conditions of employment covering the matters referred to in Article 3(1), first subparagraph, (a) to (g), save for minimum rates of pay - Collective agreement for the building sector the terms of which lay down more favourable conditions or relate to other matters - Possibility for trade unions to attempt, by way of collective action, to force undertakings established in other Member States to negotiate on a case-by-case basis in order to determine the rates of pay for workers and to sign the collective agreement for the building sector, European Court Reports 2007 I-11767, ECLI:EU:C:2007:809.

- Case **C-438/05**, Judgment of the Court (Grand Chamber) of 11 December 2007, International Transport Workers' Federation and Finnish Seamen's Union v Viking Line ABP and OÜ Viking Line Eesti, Reference for a preliminary ruling: Court of Appeal (England & Wales), Civil Division - United Kingdom, Maritime transport - Right of establishment - Fundamental rights - Objectives of Community social policy - Collective action taken by a trade union organisation against a private undertaking - Collective agreement liable to deter an undertaking from registering a vessel under the flag of another Member State, European Court Reports 2007 I-10779, ECLI:EU:C:2007:772

- Case **C-254/05**, Judgment of the Court (Fourth Chamber) of 7 June 2007. Commission of the European Communities v Kingdom of Belgium. Failure of a Member State to fulfil obligations - Articles 28 EC and 30 EC - Quantitative restrictions on imports - Measures having equivalent effect - Automatic fire detection systems with point detectors - Requirement of conformity to a national standard - National approval procedure. European Court Reports 2007 I-04269. ECLI identifier: ECLI:EU:C:2007:319

- Case **C-252/05**, Judgment of the Court (Second Chamber) of 10 May 2007. The Queen on the application of Thames Water Utilities Ltd v South East London Division, Bromley Magistrates' Court (District Judge Carr). Reference for a preliminary ruling: High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) - United Kingdom. Waste - Directives 75/442/EEC, 91/156/EEC, and 91/271/EEC - Waste water which escapes from a sewerage network - Classification - Scope of Directives 75/442/EEC and 91/271/EEC. European Court Reports 2007 I-03883. ECLI identifier: ECLI:EU:C:2007:276

- Case **C-380/03**, Judgment of the Court (Grand Chamber) of 12 December 2006. Federal Republic of Germany v European Parliament and Council of the European Union. Action for annulment - Approximation of laws - Directive 2003/33/EC - Advertising and sponsorship in respect of tobacco products - Annulment of Articles 3 and 4 - Choice of legal basis - Articles 95 EC and 152 EC - Principle of proportionality. European Court Reports 2006 I-11573. ECLI identifier: ECLI:EU:C:2006:772

- Case **C-53/04**, Judgment of the Court (Second Chamber) of 7 September 2006, Cristiano Marrosu and Gianluca Sardino v Azienda Ospedaliera Ospedale San Martino di Genova e Cliniche Universitarie Convenzionate, Reference for a preliminary ruling: Tribunale di Genova – Italy, Directive 1999/70/EC - Clauses 1(b) and 5 of the framework agreement on fixed-term work - Establishment of employment relationships of indefinite duration resulting from infringement of the rules governing successive fixed-term contracts - Possible derogation in respect of employment contracts in the public sector, European Court Reports 2006 I-07213, ECLI:EU:C:2006:517

- Case **C-212/04**, Judgment of the Court (Grand Chamber) of 4 July 2006, Konstantinos Adeneler and Others v Ellinikos Organismos Galaktos (ELOG), Reference for a preliminary ruling: Monomeles Protodikeio Thessalonikis – Greece, Directive 1999/70/EC - Clauses 1(b) and 5 of the framework agreement on fixed-term work -- Successive fixed-term employment contracts in the public sector - Concepts of 'successive contracts' and 'objective reasons' justifying the renewal of such contracts - Measures intended to prevent abuse - Sanctions - Scope of the obligation to interpret national law in conformity with Community law, European Court Reports 2006 I-06057, ECLI:EU:C:2006:443

- Case **C-217/04**, Judgment of the Court (Grand Chamber) of 2 May 2006. United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union. Regulation (EC) No 460/2004 - European Network and Information Security Agency - Choice of legal basis. European Court Reports 2006 I-03771. ECLI identifier: ECLI:EU:C:2006:279

- Case **C-66/04**, Judgment of the Court (Grand Chamber) of 6 December 2005. United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union. Foods - Regulation (EC) No 2065/2003 - Smoke flavourings - Choice of legal basis. European Court Reports 2005 I-10553. ECLI identifier: ECLI:EU:C:2005:743

- Case **C-444/03**, Judgment of the Court (Second Chamber) of 12 May 2005. Meta Fackler KG v Bundesrepublik Deutschland. Reference for a preliminary ruling: Verwaltungsgericht Berlin - Germany. Medicinal products for human use - Homeopathic medicinal products - National provision excluding from the special, simplified registration procedure a medicinal product composed of known homeopathic substances if its use as a homeopathic medicinal product is not generally known. European Court Reports 2005 I-03913. ECLI identifier: ECLI:EU:C:2005:288

- Case **C-27/02**, Judgment of the Court (Second Chamber) of 20 January 2005. Petra Engler v Janus Versand GmbH. Reference for a preliminary ruling: Oberlandesgericht Innsbruck - Austria. Brussels Convention - Request for the interpretation of Article 5(1) and (3) and Article 13, first paragraph, point 3 - Entitlement of a consumer to whom misleading advertising has been sent to seek payment, in judicial proceedings, of the prize which he has ostensibly won - Classification - Action of a contractual nature covered by Article 13, first paragraph, point 3, or by Article 5(1) or in matters of tort, delict or quasi-delict by Article 5(3) - Conditions. European Court Reports 2005 I-00481. ECLI identifier: ECLI:EU:C:2005:33

- Case **C-36/02**, Judgment of the Court (First Chamber) of 14 October 2004, Omega Spielhallen- und Automatenaufstellungs-GmbH v Oberbürgermeisterin der Bundesstadt Bonn, Reference for a preliminary ruling: Bundesverwaltungsgericht – Germany, Freedom to provide services - Free movement of goods - Restrictions - Public policy - Human dignity - Protection of fundamental values laid down in the national constitution – 'Playing at killing', European Court Reports 2004 I-09609, ECLI:EU:C:2004:614

- Case **C-338/01**, Judgment of the Court (Sixth Chamber) of 29 April 2004. Commission of the European Communities v Council of the European Union. Directive 2001/44/EC - Choice of legal basis. European Court Reports 2004 I-04829. ECLI identifier: ECLI:EU:C:2004:253

- Case **C-453/00**, Judgment of the Court of 13 January 2004, Kühne & Heitz NV v Produktschap voor Pluimvee en Eieren, Reference for a preliminary ruling: College van Beroep voor het bedrijfsleven – Netherlands, Poultrymeat - Export refunds - Failure to refer a question for a preliminary ruling - Final administrative decision - Effect of a preliminary ruling given by the Court after that decision - Legal certainty - Primacy of Community law - Principle of cooperation - Article 10 EC, European Court Reports 2004 I-00837. ECLI:EU:C:2004:17

- Case **C-444/00**, Judgment of the Court (Fifth Chamber) of 19 June 2003. The Queen, on the application of Mayer Parry Recycling Ltd, v Environment Agency and Secretary of State for the Environment, Transport and the Regions, and Corus (UK) Ltd and Allied Steel and Wire Ltd (ASW). Reference for a preliminary ruling: High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) - United Kingdom. Directive 75/442/EEC, as amended by Directive 91/156/EEC and Decision 96/350/EC - Directive 94/62/EC - Concept of waste - Concept of recycling - Processing of metal packaging waste. European Court Reports 2003 I-06163. ECLI identifier: ECLI:EU:C:2003:356

- Case C-139/01, Judgment of the Court of 20 May 2003. References for a preliminary ruling: Verfassungsgerichtshof (C-465/00) and Oberster Gerichtshof (C-138/01 and C-139/01) - Austria. Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Protection of private life - Disclosure of data on the income of employees of bodies subject to control by the Rechnungshof. Joined cases C-465/00, C-138/01 and C-139/01. ECLI identifier: ECLI:EU:C:2003:294

- Case **C-439/01**, Judgment of the Court (Fifth Chamber) of 16 January 2003. Libor Cipra and Vlastimil Kvasnicka v Bezirkshauptmannschaft Mistelbach. Reference for a preliminary ruling: Unabhängiger Verwaltungssenat im Land Niederösterreich - Austria. Road transport - Social legislation - Regulation (EEC) No 3820/85 - Breaks and rest periods - Crew consisting of more than one driver - Jurisdiction of the Court to interpret the AETR Agreement - Principle of legal certainty. European Court Reports 2003 I-00745. ECLI identifier: ECLI:EU:C:2003:31

- Case **C-491/01**, Judgment of the Court of 10 December 2002. The Queen v Secretary of State for Health, ex parte British American Tobacco (Investments) Ltd and Imperial Tobacco Ltd. Reference for a preliminary ruling: High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) - United Kingdom. Directive 2001/37/EC - Manufacture, presentation, and sale of tobacco products - Validity - Legal basis - Articles 95 EC and 133 EC - Interpretation - Applicability to tobacco products manufactured in the Community and intended for export to non-member countries. European Court Reports 2002 I-11453. ECLI identifier: ECLI:EU:C:2002:741

- Case **C-52/00**, Judgment of the Court (Fifth Chamber) of 25 April 2002. Commission of the European Communities v French Republic. Failure by a Member State to fulfil its obligations - Directive 85/374/EEC - Product liability - Incorrect transposition. European Court Reports 2002 I-03827. ECLI identifier: ECLI:EU:C:2002:252

- Case **C-183/00**, Judgment of the Court (Fifth Chamber) of 25 April 2002. María Victoria González Sánchez v Medicina Asturiana SA. Reference for a preliminary ruling: Juzgado de Primera Instancia e Instrucción nº 5 de Oviedo - Spain. Approximation of laws - Directive 85/374/EEC - Product liability - Relationship with other systems of liability. European Court Reports 2002 I-03901. ECLI identifier: ECLI:EU:C:2002:255

- Case **C-13/00**, Judgment of the Court of 19 March 2002. Commission of the European Communities v Ireland. Failure by a Member State to fulfil its obligations - Failure to adhere within the prescribed period to the Berne Convention for the Protection of Literary and Artistic Works (Paris Act of 24 July 1971) - Failure to fulfil obligations under Article 228(7) of the EC Treaty (now, after amendment, Article 300(7) EC) in conjunction with Article 5 of Protocol 28 to the EEA Agreement. European Court Reports 2002 I-02943. ECLI identifier: ECLI:EU:C:2002:184

- Case **C-411/98**, Judgment of the Court of 3 October 2000, Angelo Ferlini v Centre hospitalier de Luxembourg, Reference for a preliminary ruling: Tribunal d'arrondissement de Luxembourg - Grand Duchy of Luxemburg,

Workers - Regulation (EEC) No 1612/68 - Equal treatment - Persons not affiliated to the national social security scheme - Officials of the European Communities - Application of scales of fees for medical and hospital expenses connected with childbirth, European Court Reports 2000 I-08081, ECLI:EU:C:2000:530

- Case **C-456/98**, Judgment of the Court (First Chamber) of 13 July 2000, Centrosteel Srl v Adipol GmbH, Reference for a preliminary ruling: Pretore di Brescia – Italy, Directive 86/653/EEC - Self-employed commercial agents - National legislation providing that commercial agency contracts concluded by persons not entered in the register of agents are void, European Court Reports 2000 I-06007, ECLI:EU:C:2000:402

- Case **C-424/97**. Judgment of the Court of 4 July 2000. Salomone Haim v Kassenzahnärztliche Vereinigung Nordrhein. Reference for a preliminary ruling: Landgericht Düsseldorf - Germany. Member State liability in the event of a breach of Community law - Breaches attributable to a public-law body of a Member State - Conditions for the liability of the Member State and of a public-law body of that State - Compatibility of a language requirement with freedom of establishment. European Court Reports 2000 I-05123. ECLI identifier: ECLI:EU:C:2000:357

- Case **C-281/98**, Judgment of the Court of 6 June 2000, Roman Angonese v Cassa di Risparmio di Bolzano SpA, Reference for a preliminary ruling: Pretore di Bolzano – Italy, Freedom of movement for persons - Access to employment - Certificate of bilingualism issued by a local authority - Article 48 of the EC Treaty (now, after amendment, Article 39 EC) - Council Regulation (EEC) No 1612/68, European Court Reports 2000 I-04139, ECLI:EU:C:2000:296.

- Case **C-78/98**, Judgment of the Court of 16 May 2000. Shirley Preston and Othes v Wolverhampton Healthcare NHS Trust and Others and Dorothy Fletcher and Others v Midland Bank plc. Reference for a preliminary ruling: House of Lords - United Kingdom. Social policy - Men and women - Equal pay - Membership of an occupational pension scheme - Part-time workers - Exclusion - National procedural rules - Principle of effectiveness - Principle of equivalence. European Court Reports 2000 I-03201. ECLI identifier: ECLI:EU:C:2000:247

- Case **C-378/97**, Judgment of the Court of 21 September 1999. Criminal proceedings against Florus Ariël Wijsenbeek. Reference for a preliminary ruling: Arrondissementsrechtbank Rotterdam - Netherlands. Freedom of movement for persons - Right of citizens of the European Union to move and reside freely - Border controls - National legislation requiring persons coming from another Member State to present a passport. European Court Reports 1999 I-06207, ECLI identifier: ECLI:EU:C:1999:439.

- Case **C-326/96**, Judgment of the Court of 1 December 1998. B.S. Levez v T.H. Jennings (Harlow Pools) Ltd. Reference for a preliminary ruling: Employment Appeal Tribunal, London - United Kingdom. Social policy - Men and women - Equal pay - Article 119 of the EC Treaty - Directive 75/117/EEC - Remedies for breach of the prohibition on discrimination - Pay arrears - Domestic legislation placing a two-year limit on awards for the

period prior to the institution of proceedings - Similar domestic actions. European Court Reports 1998 I-07835. ECLI identifier: ECLI:EU:C:1998:577

- Case **C-162/97**, Judgment of the Court (Fifth Chamber) of 19 November 1998. Criminal proceedings against Gunnar Nilsson, Per Olov Hagelgren and Solweig Arrborn. Reference for a preliminary ruling: Helsingborgs tingsrätt - Sweden. Free movement of goods - Prohibition of quantitative restrictions and measures having equivalent effect between Member States - Derogations - Protection of the life and health of animals - Improvement of livestock - Breeding of purebred breeding animals of the bovine species - Artificial insemination. European Court Reports 1998 I-07477. ECLI identifier: ECLI:EU:C:1998:554

- Case **C-231/96**, Judgment of the Court of 15 September 1998. Edilizia Industriale Siderurgica Srl (Edis) v Ministero delle Finanze. Reference for a preliminary ruling: Tribunale di Genova - Italy. Recovery of sums paid but not due - Procedural time-limits under national law. European Court Reports 1998 I-04951. ECLI identifier: ECLI:EU:C:1998:401

- Case **C-261/95**, Judgment of the Court (Fifth Chamber) of 10 July 1997. Rosalba Palmisani v Istituto nazionale della previdenza sociale (INPS). Reference for a preliminary ruling: Pretura circondariale di Frosinone - Italy. Social policy - Protection of employees in the event of the insolvency of their employer - Directive 80/987/EEC - Liability of a Member State arising from belated transposition of a directive - Adequate reparation - Limitation period. European Court Reports 1997 I-04025. ECLI identifier: ECLI:EU:C:1997:351

- Case **C-66/95**, Judgment of the Court of 22 April 1997. The Queen v Secretary of State for Social Security, ex parte Eunice Sutton. Reference for a preliminary ruling: High Court of Justice, Queen's Bench Division - United Kingdom. Directive 79/7/EEC - Equal treatment for men and women in matters of social security - Responsibility of a Member State for an infringement of Community law - Right to receive interest on arrears of social security benefits. European Court Reports 1997 I-02163. ECLI identifier: ECLI:EU:C:1997:207

- Case **C-84/94**, Judgment of the Court of 12 November 1996. United Kingdom of Great Britain and Northern Ireland v Council of the European Union. Council Directive 93/104/EC concerning certain aspects of the organization of working time - Action for annulment. European Court Reports 1996 I-05755. ECLI identifier: ECLI:EU:C:1996:431

- Case **C-61/94**, Judgment of the Court of 10 September 1996. Commission of the European Communities v Federal Republic of Germany. Failure of a Member State to fulfil its obligations - International Dairy Arrangement. European Court Reports 1996 I-03989. ECLI identifier: ECLI:EU:C:1996:313

- Case **C-473/93**, Judgment of the Court of 2 July 1996, Commission of the European Communities v Grand Duchy of Luxemburg, Failure of a Member State to fulfil its obligations - Freedom of movement for persons - Employment in the public service, European Court Reports 1996 I-03207, ECLI:EU:C:1996:263.

- Case **C-194/94**, Judgment of the Court of 30 April 1996, CIA Security International SA v Signalson SA and Securitel SPRL, Reference for a preliminary ruling: Tribunal de commerce de Liège – Belgium, Interpretation of Article 30 of the EC Treaty and of Directive 83/189/EEC laying down a procedure for the provision of information in the field of technical standards and regulations - National legislation on the marketing of alarm systems and networks - Prior administrative approval, European Court Reports 1996 I-02201, ECLI:EU:C:1996:172

- Case C-312/93, Judgment of the Court of 14 December 1995. Peterbroeck, Van Campenhout & Cie SCS v Belgian State. Reference for a preliminary ruling: Cour d'appel de Bruxelles - Belgium. Power of a national court to consider of its own motion: the question whether national law is compatible with Community law. European Court Reports 1995 I-04599. ECLI identifier: ECLI:EU:C:1995:437

- Case **C-275/92**, Judgment of the Court of 24 March 1994. Her Majesty's Customs and Excise v Gerhart Schindler and Jörg Schindler. Reference for a preliminary ruling: High Court of Justice, Queen's Bench Division - United Kingdom. Lotteries. European Court Reports 1994 I-01039. ECLI identifier: ECLI:EU:C:1994:119

- Case **C-271/91**, Judgment of the Court of 2 August 1993. M. Helen Marshall v Southampton and South-West Hampshire Area Health Authority. Reference for a preliminary ruling: House of Lords - United Kingdom. Directive 76/207/EEC - Equal treatment for men and women - Right to compensation in the event of discrimination. European Court Reports 1993 I-04367. ECLI identifier: ECLI:EU:C:1993:335

- Case **C-300/89**, Judgment of the Court of 11 June 1991. Commission of the European Communities v Council of the European Communities. Directive on waste from the titanium dioxide industry - Legal basis. European Court Reports 1991 I-02867. ECLI identifier: ECLI:EU:C:1991:244

- Case **C-106/89**, Judgment of the Court (Sixth Chamber) of 13 November 1990, Marleasing SA v La Comercial Internacional de Alimentacion SA, Reference for a preliminary ruling: Juzgado de Primera Instancia e Instruccion no 1 de Oviedo – Spain, Directive 68/151/CEE - Article 11 - Consistent interpretation of national law, European Court Reports 1990 I-04135, ECLI:EU:C:1990:395

- Case **C-213/89**, Judgment of the Court of 19 June 1990, The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others, Reference for a preliminary ruling: House of Lords - United Kingdom, Rights derived from provisions of Community law - Protection by national courts - Power of national courts to grant interim relief when a reference is made for a preliminary ruling, European Court Reports 1990 I-02433, ECLI:EU:C:1990:257

- Case **103/88**, 22 June 1989. Fratelli Costanzo SpA v Comune di Milano. Reference for a preliminary ruling: Tribunale amministrativo regionale della Lombardia - Italy. Public works contracts - Abnormally low tenders - Direct effect of directives in relation to administrative authorities, European Court Reports 1989 -01839, ECLI identifier: ECLI:EU:C:1989:256

- Case **68/88**, Judgment of the Court of 21 September 1989, Commission of the European Communities v Hellenic Republic. Failure of a Member State to fulfil its obligations - Failure to establish and make available the Community's own resources. European Court Reports 1989 -02965, ECLI identifier: ECLI:EU:C:1989:339

- Case **222/86**, Judgment of the Court of 15 October 1987. Union nationale des entraîneurs et cadres techniques professionnels du football (Unectef) v Georges Heylens and others. Reference for a preliminary ruling: Tribunal de grande instance de Lille - France. Free movement of workers - Equivalence of diplomas - Sports trainer. European Court Reports 1987 -04097. ECLI identifier: ECLI:EU:C:1987:442

- Case **222/84**, Judgment of the Court of 15 May 1986. Marguerite Johnston v Chief Constable of the Royal Ulster Constabulary. Reference for a preliminary ruling: Industrial Tribunal, Belfast (Northern Ireland) - United Kingdom. Equal treatment for men and women - Armed member of a police reserve force. European Court Reports 1986 -01651. ECLI identifier: ECLI:EU:C:1986:206

- Case **14/83**, Judgment of the Court of 10 April 1984. Sabine von Colson and Elisabeth Kamann v Land Nordrhein-Westfalen. Reference for a preliminary ruling: Arbeitsgericht Hamm - Germany. Equal treatment for men and women - Access to employment. European Court Reports 1984 -01891. ECLI identifier: ECLI:EU:C:1984:153

- Case **66/82**, Judgment of the Court (First Chamber) of 23 February 1983. Fromançais SA v Fonds d'orientation et de régularisation des marchés agricoles (FORMA). Reference for a preliminary ruling: Tribunal administratif de Paris - France. Forfeiture of security. European Court Reports 1983 -00395, ECLI identifier: ECLI:EU:C:1983:42.

- Case **15/81**, Judgment of the Court of 5 May 1982. Gaston Schul Douane Expediteur BV v Inspecteur der Invoerrechten en Accijnzen, Roosendaal. Reference for a preliminary ruling: Gerechtshof 's-Hertogenbosch - Netherlands. Turnover tax on the importation of goods supplied by private persons. European Court Reports 1982 -01409. ECLI identifier: ECLI:EU:C:1982:135

- Case **169/80**, Judgment of the Court (Third Chamber) of 9 July 1981. Administration des douanes v Société anonyme Gondrand Frères and Société anonyme Garancini. Reference for a preliminary ruling: Cour de cassation - France. Monetary compensatory amounts and the Common Customs Tariff 'Emmentaler Cheese'. European Court Reports 1981 -01931. ECLI identifier: ECLI:EU:C:1981:171

- Case **98/80**, Judgment of the Court (First Chamber) of 14 May 1981. Giuseppe Romano v Institut national d'assurance maladie-invalidité. Reference for a preliminary ruling: Tribunal du travail de Bruxelles - Belgium. Social security - Applicable exchange rate. European Court Reports 1981 -01241. ECLI identifier: ECLI:EU:C:1981:104

- Case **120/78**, Judgment of the Court of 20 February 1979. Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein. Reference for a preliminary ruling: Hessisches Finanzgericht - Germany. Measures heaving an

effect equivalent to quantitative restrictions. European Court Reports 1979 -00649. ECLI identifier: ECLI:EU:C:1979:42

- Case **106/77**, Judgment of the Court of 9 March 1978, Amministrazione delle Finanze dello Stato v Simmenthal SpA, Reference for a preliminary ruling: Pretura di Susa – Italy, Discarding by the national court of a law contrary to Community law, European Court Reports 1978 -00629, ECLI:EU:C:1978:49

- Case **45-76**, Judgment of the Court of 16 December 1976. Comet BV v Produktschap voor Siergewassen. Reference for a preliminary ruling: College van Beroep voor het Bedrijfsleven - Netherlands. European Court Reports 1976 -02043. ECLI identifier: ECLI:EU:C:1976:191

- Case **36-74**, Judgment of the Court of 12 December 1974, B.N.O. Walrave and L.J.N. Koch v Association Union cycliste internationale, Koninklijke Nederlandsche Wielren Unie and Federación Española Ciclismo, Reference for a preliminary ruling: Arrondissementsrechtbank Utrecht – Netherlands, European Court Reports 1974 -01405, ECLI:EU:C:1974:140

- Case **181-73**, Judgment of the Court of 30 April 1974. R. & V. Haegeman v Belgian State. Reference for a preliminary ruling: Tribunal de première instance de Bruxelles - Belgium. European Court Reports 1974 -00449. ECLI identifier: ECLI:EU:C:1974:41

- Case **34-73**, Judgment of the Court of 10 October 1973, Fratelli Variola S.p.A. v Amministrazione italiana delle Finanze, Reference for a preliminary ruling: Tribunale civile e penale di Trieste – Italy, Unloading charge, European Court Reports 1973 -00981, ECLI:EU:C:1973:101

- Case **48-71**, Judgment of the Court of 13 July 1972. Commission of the European Communities v Italian Republic. ECLI identifier: ECLI:EU:C:1972:65

- Case **11-70**, Judgment of the Court of 17 December 1970, Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel, Reference for a preliminary ruling: Verwaltungsgericht Frankfurt am Main – Germany, ECLI:EU:C:1970:114

- Case **14-68**, Judgment of the Court of 13 February 1969, Walt Wilhelm, and others v Bundeskartellamt, Reference for a preliminary ruling: Kammergericht Berlin – Germany, ECLI:EU:C:1969:4

- Case **26-62**, 5 February 1963. NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration. Reference for a preliminary ruling: Tariefcommissie – Netherlands, ECLI:EU:C:1963:1

Joined Cases

- Joined cases **C-397/01 to C-403/01**, Judgment of the Court (Grand Chamber) of 5 October 2004, Bernhard Pfeiffer (C-397/01), Wilhelm Roith (C-398/01), Albert Süß (C-399/01), Michael Winter (C-400/01), Klaus Nestvogel (C-401/01), Roswitha Zeller (C-402/01) and Matthias Döbele (C-403/01) v Deutsches Rotes Kreuz, Kreisverband Waldshut eV, Reference for a preliminary ruling: Arbeitsgericht Lörrach – Germany, Social policy - Protection of the health and safety of workers - Directive 93/104/EC - Scope - Emergency workers in attendance in ambulances in the framework of an emergency service run by the German Red Cross - Definition of 'road transport' - Maximum weekly working time - Principle - Direct effect - Derogation – Conditions, European Court Reports 2004 I-08835, ECLI:EU:C:2004:584

- Joined cases **C-482/01 and C-493/01**, Judgment of the Court (Fifth Chamber) of 29 April 2004. Georgios Orfanopoulos and Others (C-482/01) and Raffaele Oliveri (C-493/01) v Land Baden-Württemberg. References for a preliminary ruling: Verwaltungsgericht Stuttgart - Germany. Freedom of movement of persons - Public policy - Directive 64/221/EEC - Decision to expel on ground of criminal offences - Taking into account of the length of residence and personal circumstances - Fundamental rights - Protection of family life - Taking into account circumstances occurring between the final decision of the administrative authorities and the review by an administrative court of the lawfulness of that decision - The person concerned's right to make submissions as to the expediency of the measure before an authority called upon to give an opinion. European Court Reports 2004 I-05257. ECLI identifier: ECLI:EU:C:2004:262

- Joined cases **C-10/97 to C-22/97**, Judgment of the Court of 22 October 1998, Ministero delle Finanze v IN.CO.GE.'90 Srl, Idelgard Srl, Iris'90 Srl, Camed Srl, Pomezia Progetti Appalti Srl (PPA), Edilcam Srl, A. Cecchini & C. Srl, EMO Srl, Emoda Srl, Sappesi Srl, Ing. Luigi Martini Srl, Giacomo Srl and Mafar Srl, Reference for a preliminary ruling: Pretura circondariale di Roma – Italy, Recovery of sums paid but not due - Treatment of a national charge incompatible with Community law, European Court Reports 1998 I-06307, ECLI:EU:C:1998:498

- Joined cases **C-430/93 and C-431/93**, Judgment of the Court of 14 December 1995, Jeroen van Schijndel and Johannes Nicolaas Cornelis van Veen v Stichting Pensioenfonds voor Fysiotherapeuten. References for a preliminary ruling: Hoge Raad – Netherlands, Treatment of an occupational pension fund as an undertaking - Compulsory membership of an occupational pension scheme - Compatibility with the rules of competition - Whether a point of Community law may be raised for the first time in cassation, thereby altering the subject-matter of the proceedings and entailing an examination of facts, European Court Reports 1995 I-04705, ECLI:EU:C:1995:441

- Joined cases **51 to 54-71**, Judgment of the Court of 15 December 1971. International Fruit Company NV and others v Produktschap voor groenten en fruit. References for a preliminary ruling: College van Beroep voor het Bedrijfsleven - Netherlands. Quantitative restrictions and measures having equivalent effect. ECLI identifier: ECLI:EU:C:1971:128

Court of Justice of the European Coal and Steel Community:

- Case **9-56**, Judgment of the Court of 13 June 1958. Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community. English special edition 1957-1958 00133. ECLI identifier: ECLI:EU:C:1958:7

Court of First Instance:

- Case **T-362/04**, Judgment of the Court of First Instance (Second Chamber) of 31 January 2007. Leonid Minin v Commission of the European Communities. Common foreign and security policy - Restrictive measures in respect of Liberia - Freezing of funds of persons associated with Charles Taylor - Competence of the Community - Fundamental rights - Action for annulment. European Court Reports 2007 II-002003. ECLI identifier: ECLI:EU:T:2007:25

- Case **T-253/02**, Judgment of the Court of First Instance (Second Chamber) of 12 July 2006. Chafiq Ayadi v Council of the European Union. Common foreign and security policy - Restrictive measures taken against persons and entities associated with Usama bin Laden, the Al-Qaeda network, and the Taliban - Competence of the Community - Freezing of funds - Fundamental rights - Jus cogens - Review by the Court - Action for annulment. European Court Reports 2006 II-02139. ECLI identifier: ECLI:EU:T:2006:200

- Case **T-306/01**, Judgment of the Court of First Instance (Second Chamber, extended composition) of 21 September 2005. Ahmed Ali Yusuf and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities. Common foreign and security policy - Restrictive measures taken against persons and entities associated with Usama bin Laden, the Al-Qaeda network, and the Taliban - Competence of the Community - Freezing of funds -Fundamental rights - Jus cogens - Review by the Court - Action for annulment. European Court Reports 2005 II-03533. ECLI identifier: ECLI:EU:T:2005:331

- Case **T-315/01**, Judgment of the Court of First Instance (Second Chamber, extended composition) of 21 September 2005. Yassin Abdullah Kadi v Council of the European Union and Commission of the European Communities. Common foreign and security policy - Restrictive measures taken against persons and entities associated with Usama bin Laden, the Al-Qaeda network, and the Taliban - Competence of the Community - Freezing of funds -Fundamental rights - Jus cogens - Review by the Court - Action for annulment. European Court Reports 2005 II-03649. ECLI identifier: ECLI:EU:T:2005:332

International Court of Justice:

- Advisory Opinion, 'Legality of the Threat or Use of Nuclear Weapons', 8 July 1996

- Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicar v. U.S.), ICJ, Merits, Rep. 1986

Treaties and Conventions:

- Additional Protocol (II) to the Geneva Conventions, 1977; Resolutions of the Diplomatic Geneva Conference, 1974-1977

- Additional Protocol (III) to the Geneva Conventions, 2005

- Geneva Convention (I) on Wounded and Sick in Armed Forces in the Field,1949; Geneva Convention (II) on Wounded, Sick and Shipwrecked of Armed Forces at Sea, 1949; Geneva Convention (III) on Prisoners of War, 1949; Geneva Convention (IV) on Civilians, 1949

- Protocol Additional to the Geneva Conventions of August 12th, 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, Article 49.

- Hague Convention (II) on the Laws and Customs of War on Land, 1899; Hague Declaration (IV,2) concerning Asphyxiating Gases, 1899; Hague Declaration (IV,3) concerning Expanding Bullets, 1899

- Hague Convention (IV) on War on Land and its Annexed Regulations, 1907; Hague Convention (IX) on Bombardment by Naval Forces, 1907; Hague Declaration (XIV) on Explosives from Balloons, 1907

- Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, 18 October 1907, 205 CTS 299.

- Hague Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War, 18 October 1907, 205 CTS 395.

Finland

Experts Opinion (Parliament of Finland):

- Elisa Oyj:n lausunto verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta, 28 February 2018

- Liikenne- ja viestintävaliokunta torstai, 01 March 2018

- FiComin lausunto verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta, 01 March 2018

- Lakiasianjohtaja Marko Vuorinen, Finnet-liitto ry Asiantuntijalausunto, 02 March 2018

- Apulaisjohtaja Kirsti Tarnanen-Sariola, Suomen Satamaliitto Asiantuntijalausunto, 02 March 2018

- ITC-johtaja Heikki Linnanen, Caruna Oy Asiantuntijalausunto, , 09 March 2018

- Älykkään liikenteen verkosto - ITS Finland ry Asiantuntijalausunto, 09 March 2018

- Air Navigation Services Finland Oy (ANS Finland) Asiantuntijalausunto, 09 March 2018

- Energiavirasto Asiantuntijalausunto, 09 March 2018

- Finanssivalvonta Asiantuntijalausunto, 09 March 2018

- UpCloud Oy Asiantuntijalausunto, 09 March 2018

- Liikennevirasto Asiantuntijalausunto, 09 March 2018

- Helsingin seudun ympäristöpalvelut -kuntayhtymä Asiantuntijalausunto, 14 March 2018

- Google Finland Oy Asiantuntijalausunto, 14 March 2018

- Ylitarkastaja Maija Rönkä, liikenne- ja viestintäministeriö Asiantuntijalausunto, 16 March 2018

Legislation (Finlex Data Bank):

- Alusliikennepalvelulaki (623/2005) 05/08/2005, viimeksi muutettuna (284/2018) 04/05/2018

- Henkilötietolaki (523/1999) 22/04/1999

- Ilmailulaki (864/2014) 07/11/2014, viimeksi muutettuna (282/2018) 04/05/2018

- Kuluttajansuojalaki 20.1.1978/38

- Laki huoltovarmuuden turvaamisesta (1390/1992) 18/12/1992

- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 7.8.2009/617

- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) 09/02/2007

- Laki tietoyhteiskunnan palvelujen tarjoamisesta annetun lain 15 §:n muuttamisesta 512/2011

- Laki tietoyhteiskuntakaaren muuttamisesta (281/2018) 04/05/2018

- Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 1226/2013

- Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015

- Laki sähköisen viestinnän palveluista (917/2014) 07/11/2014, viimeksi muutettuna (281/2018) 04/05/2018

- Laki eräiden alusten ja niitä palvelevien satamien turvatoimista ja turvatoimien valvonnasta (485/2004) 11/06/04, viimeksi muutettuna (285/2018) 04/05/2018

- Laki liikenteen palveluista (320/2017) 24/05/2017, Lag om ändring av lagen om transportservice (286/2018) 04/05/2018

- Laki kaupankäynnistä rahoitusvälineillä (1070/2017) 28/12/2017

- Laki luottolaitostoiminnasta (610/2014) 08/08/2014, viimeksi muutettuna (1073/2017) 28/12/2017

- Laki Sosiaali- ja terveysalan lupa- ja valvontavirastosta annetun lain 6 §:n muuttamisesta (669/2008)- 28/12/2017

- Laki sähkö- ja maakaasumarkkinoiden valvonnasta (590/2013) 09/08/2013, viimeksi muutettuna (289/2018) 04/05/2018

- Laki viranomaisten toiminnan julkisuudesta (621/1999) 21/05/1999

- Luottolaitostoiminnasta annetun lain (610/2014)

- Määräykset ja ohjeet, Operatiivisen riskin hallinta rahoitussektorin valvottavissa on päivitetty, 8/2014

- Määräykset ja ohjeet, Ulkoistaminen rahoitussektoriin kuuluvissa valvottavissa, 1/2012

-Maakaasumarkkinalaki (587/2017) 25/08/2017, viimeksi muutettuna (288/2018) 04/05/2018

- Rautatielaki (304/2011) 08/04/2011, viimeksi muutettuna (283/2018)-04/05/2018

- Sähkömarkkinalaki (588/2013) 09/08/2013, viimeksi muutettuna (287/2018) 04/05/2018

- Suomessa terveydenhuoltolakia (1326/2010)

- Terveydenhuoltolaki (1326/2010) 30/12/2010

- Terveydenhuollon laitteista ja tarvikkeista annetun lain (629/2010) 24/06/2010

- Tietoyhteiskuntakaari (917/2014) 07/11/2014

- Vesihuoltolaki (119/2001) 09/02/2001, viimeksi muutettuna (290/2018) 04/05/2018

Official Documents (Valto-Institutional Repository for the Government):

- Liikenne- ja viestintäministeriön, 'Verkko- ja tietoturvadirektiivi Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti', 9/2017 (report)

- Liikenne- ja viestintäministeriö, 'Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta', HE 192/2017

- Valtioneuvosto, Tasavallan presidentin esittely 4.5.2018 TP 30/2018

- Valtioneuvoston päätös huoltovarmuuden tavoitteista (857/2013) 05/12/2013

- Valtioneuvoston päätös huoltovarmuuden tavoitteista 1048/2018

- Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015

- Valtioneuvoston päätös huoltovarmuuden tavoitteista 21.8.2008/539

- Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 132/2014

- Valtioneuvoston asetus yhteiskunnan toiminnan kannalta merkittävistä lentoasemista ja satamista, 02/05/2018

- The Finnish Security and Defence Committee, 'The Strategy for Securing the Functions Vital to Society', Government Resolution, 23 November 2006

- The Finnish Security and Defence Committee, 'Security Strategy for Society', Government Resolution, 16 December 2010

- The Finnish Security and Defence Committee, 'Finland´s Cyber security Strategy', Government Resolution, 24 January 2013

- The Finnish Security and Defence Committee, 'Implementation Programme for Finland's Cyber Security Strategy for 2017–2020', Government Resolution, 24 January 2013

- The Finnish Ministry of Transports and Communications, 'Information Security Strategy for Finland

The World's Most Trusted Digital Business Environment', September 2016

- The Finnish Security and Defence Committee, ‘Finland´s Cyber security Strategy 2019’, Government Resolution, 3 October 2019

Parliament of Finland:

- Eduskunta, Pöytäkirjan asiakohta PTK 2/2018 vp, Täysistunto, ‘7. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta’, Keskiviikko 7.2.2018 klo 14.05—15.55 (Parlement minutes)

- Eduskunta, Pöytäkirjan asiakohta PTK 28/2018 vp, Täysistunto, ‘15. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta’, Tiistai 3.4.2018 klo 14.00—16.34

- Eduskunta, Pöytäkirjan asiakohta PTK 29/2018 vp, Täysistunto, ‘11. Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta’, Keskiviikko 4.4.2018 klo 14.00—18.19

- Eduskunta, Eduskunnan vastaus EV 25/2018 vp, ‘Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta’, 29 January 2021, HE 192/2017 vp

- Eduskunta, Betänkande KoUB 6/2018 rd, RP 192/2017 rd, ‘Regeringens proposition till riksdagen med förslag till lagar om ändring av lagar som har samband med genomförandet Europeiska unionens av direktiv om nät- och informationssäkerhet’, Kommunikationsutskottet, 8 May 2021

- Eduskunta, Asian käsittelytiedot HE 192/2017 vp, ‘Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta’, 29 January 2021

France

Case Law:

- Conseil Constitutionnel, Décision n° 2004-496 DC du 10 juin 2004 - Saisine par 60 députés

Legislation (Légifrance):

Code:

- Code de la Défense

- Code des postes et des communications électroniques

Law:

- Loi n° 2005-1550 du 12 décembre 2005 modifiant diverses dispositions relatives à la défense (1), JORF n°289

- Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, JORF n°0020

- Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, JORF n°0294

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978

- Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, JORF n°0048

- Loi constitutionnelle du 23 juillet 2008 de modernisation des institutions de la Vème République

Decree:

- Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, JORF n°0118

- Décret n°2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale, JORF n°47

- Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense, JORF n°0075

- Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information, JORF n°0075

- Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », JORF n°0156

- Décret n° 2018-1136 du 13 décembre 2018 pris pour l'application de l'article L. 2321-2-1 du code de la défense et des articles L. 33-14 et L. 36-14 du code des postes et des communications électroniques, JORF n°0289

Ordinance:

- Arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, JORF n°129

- Arrêté du 3 juillet 2008 portant modification de l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs, JORF n°156

Official Documents:

- ANSSI, Défense et sécurité des systèmes d'information: Stratégie de la France, February 2011

- E. Macron, 'Déclaration de M. Emmanuel Macron, président de la République, sur les cyberattaques dans les hôpitaux et la stratégie nationale pour la cybersécurité, à Paris le 18 février 2021', [discours] Vie Publique, February 2018

- Gouvernement, Etude d'Impact relative au 'Projet de Loi portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', 17 Novembre 2017, INTX1728622L/Bleue-1

- Ministère des Affaires Etrangères, 'Stratégie internationale de la France pour le numérique', December 2017

- SGDSN, 'Stratégie Nationale pour la Sécurité du Numérique', October 2015

- SGDSN, 'Revue stratégique de cyberdéfense', February 2018

Parliament:

Sénat :

- Sénat, 'Projet de Loi (Procédure Accélérée) portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', Présenté au nom de M. Édouard PHILIPPE, Premier ministre, Par M. Gérard COLLOMB, Ministre d'État, Ministre de l'Intérieur, Texte n° 105 (2017-2018), déposé le 22 Novembre 2017

- Sénat, 'Rapport fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur le projet de loi (Procédure Accélérée) portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité', M. Philippe Bonnecarrère, Sénateur, N° 161, 13.01.2017

Assemblée Nationale :

- Assemblée Nationale, 'Rapport sur le projet de loi, adopté par le Sénat après engagement de la procédure accélérée, portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (n°530)', par M. Christophe EUZET – Député, 17.02.2018

Greece

Legislation (Official Journal of the Hellenic Republic):

Presidential Order:

- Προεδρικό Διάταγμα Υπ'Αριθμ. 39, 'Προσαρμογή της ελληνικής νομοθεσίας προς τις διατάξεις της Οδηγίας 2008/114/ΕΚ του Συμβουλίου της 8ης Δεκεμβρίου 2008'

- Προεδρικό Διάταγμα Υπ'Αριθμ. 131, 'Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. (Οδηγία για το ηλεκτρονικό εμπόριο)'

- Προεδρικό Διάταγμα Υπ'Αριθμ. 96/2020, Τροποποίηση και συμπλήρωση διατάξεων του π.δ. 1/2017 «Οργανισμός της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.)» (Α' 2), ΦΕΚ 232/Α/20.11.2020

- Προεδρικό Διάταγμα Υπ'Αριθμ. 1/2017, 'Οργανισμός της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.)', ΦΕΚ 2/Α/18.1.2017

- Προεδρικό Διάταγμα Υπ'Αριθμ. 178/2014, 'Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας', ΦΕΚ 281/Α/31.12.2014

Law:

- Νόμος 3471/2006, Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997, ΦΕΚ 133/Α/28.6.2006

- Νόμος 2472/1997, Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, ΦΕΚ Α-50/10.4.1997

- Νόμος 3959/2011, 'Προστασία του ελεύθερου ανταγωνισμού', ΦΕΚ Α-93/20.4.2011

- Νόμος 2867/2000, 'Οργάνωση και λειτουργία των τηλεπικοινωνιών και άλλες διατάξεις', ΦΕΚ 273/Α/19.12.2000

- Νόμος 3431/2006, 'Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις', ΦΕΚ 13/Α/13.2.2006

-Νόμος 4070/2012, 'Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων και άλλες διατάξεις', ΦΕΚ 82 Α/10.4.2012

- Νόμος 3674/2008, Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις, ΦΕΚ 136/Α/10.7.2008

- Νόμος 3649/2008, 'Εθνική Υπηρεσία Πληροφοριών και άλλες διατάξεις', ΦΕΚ 39/Α'/3.3.2008

- Νόμος 4261/2014, 'Πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων (ενσωμάτωση της Οδηγίας 2013/36/ΕΕ), κατάργηση του ν. 3601/2007 και άλλες διατάξεις , κωδικοποιημένος με τον 4799/2021', ΦΕΚ Α 107/05.05.2014

- Νόμος 4577/2018, 'Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις', ΦΕΚ 199/Α/3.12.2018

- Νόμος 4624/2019, 'Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων', ΦΕΚ 137/Α/29.8.2019

- Νόμος 4389/2016 Επείγουσες διατάξεις για την εφαρμογή της συμφωνίας δημοσιονομικών στόχων και διαρθρωτικών μεταρρυθμίσεων και άλλες διατάξεις', ΦΕΚ Α 94/27.05.2016

- Νόμος 3959/2011, 'Προστασία του ελεύθερου ανταγωνισμού', ΦΕΚ Α-93/20.4.2011

Decisions:

- Απόφαση Υπουργική Φ. 120/01/510313/Σ.94 (1), Κύρωση του Εθνικού Κανονισμού Ασφαλείας (ΕΚΑ), ΦΕΚ 683/Β/27.2.2018

- Απόφαση Α.Δ.Α.Ε. 205/2013 - ΦΕΚ 1742/Β/15.7.2013

- Απόφαση ΑΔΑΕ Αριθμ. 99/2017 - ΦΕΚ 4073/Β/23.11.2017

Official Documents:

Ministry of Economy & Finance :

- Υπουργείο Οικονομίας & Οικονομικών – Ειδική Γραμματεία Ψηφιακού Σχεδιασμού, 'Ψηφιακή Στρατηγική 2006-2013: Τεχνολογικά εργαλεία για την ανάπτυξη των δήμων'

Ministry of Digital Policy :

- Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης - Γενική Γραμματεία Ψηφιακής Πολιτικής, Εθνική Ψηφιακή Στρατηγική 2016-2021

Parliament of Greece:

- Βουλή των Ελλήνων, 'Επεξεργασία και εξέταση του σχεδίου νόμου του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης "Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας

συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση"', Διαρκής Επιτροπή Δημοσίας Διοίκησης, Δημόσιας Τάξης και Δικαιοσύνης Και η Διαρκής Επιτροπή Παραγωγής και Εμπορίου, Εισηγητές: Αναστασία Γκαρά και Ανδρέας Κατσανιώτης, 15.11.2018

Ireland

Legislation (electronic Irish Statute Book):

- Government decision S180/20/10/481

- S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011

- S.I. No. 360/2018 - European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018

- Statutory Instruments Act, 1947, Number 44 of 1947

Official Documents (Government of Ireland):

- Department of Communications, Energy and Natural Resources, 'Doing more with Digital – National Digital Strategy for Ireland – Phase 1 – Digital Engagement', July 2013

- Department of the Environment, Climate and Communications, 'National Cyber Security Strategy 2015 – 2017', June 2015

- Department of the Environment, Climate and Communications, 'Department of the Environment, Climate and Communications', November 2017

- Department of the Environment, Climate and Communications, 'NIS Compliance Guidelines for Operators of Essential Service (OES)', August 2019 (updated on January 2021)

- Government of Ireland, 'National Cyber Security Strategy 2019-2024'

Luxembourg

Experts Opinion:

- Avis de la Chambre des Métiers, Dépêche du Directeur Général de la Chambre des Métiers au Premier Ministre, Ministre d'Etat (29.8.2018)

- Avis de la Chambre de Commerce sur le projet de loi et les amendements gouvernementaux y relatifs, (14.11.2018)

Legislation (Journal officiel du Grand-Duché de Luxembourg):

Law:

- Loi du 30 mai 2005 sur les réseaux et les services de communications électroniques, JO A-N°73 7.6.2005

- Loi du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, JO A-N°81 27.4.2009

- Loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques, JO A-N°43 8.3.2011

- Loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant 1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, JO A-N°372 31.5.2019

- Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en œuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, JO A-N°686 16.8.2018

Ordinance:

- Arrêté grand-ducal du 28 janvier 2015 portant constitution des Ministères, JO A-N°15 30.1.2015

- Arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental », JO A-N°424 29.5.2018

- Arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé «Computer Emergency Response Team Gouvernemental», JO A-N°161 6.9.2013

Regulation :

- CSSF Règlement N° 20-04 du 15 juillet 2020 relatif à la définition des services essentiels selon la loi du 28 mai 2019 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne, JO A-N°621 16.7.2020

- Institut Luxembourgeois de Régulation - Règlement 15/200/ILR du 18 décembre 2015 portant sur les modalités de notification des mesures de sécurité à prendre par les entreprises fournissant des réseaux de communications publics et/ou des services de communications électroniques au public dans le cadre de l'article 45 (1) et (2) de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques - Secteur Communications électroniques

- Institut Luxembourgeois de Régulation - Règlement ILR/N19/1 du 5 novembre 2019 portant sur la fixation des services essentiels - Service NISS, JO A-N°768 11.11.2019

- Institut Luxembourgeois de Régulation - Règlement 14/181/ILR du 28 août 2014 portant définition de critères et de seuils en relation avec l'impact significatif sur le fonctionnement des réseaux ou des services à signaler obligatoirement à l'Institut en cas d'atteinte à la sécurité ou à la perte d'intégrité de réseaux et de services de communications électroniques - Secteur Communications électroniques.

Official Documents (Gouvernement du Grand-Duché de Luxembourg):

- Gouvernement du Grand-Duché de Luxembourg, 'L'ILR lance une nouvelle plateforme d'analyse de risques pour les opérateurs de télécommunications', [Prees Release] 31 July 2020

- Gouvernement du Grand-Duché de Luxembourg, 'Stratégie nationale en matière de cyber sécurité', November 2011

- Gouvernement du Grand-Duché de Luxembourg, Stratégie Nationale en matière de Cybersécurité II, 2015

- Gouvernement du Grand-Duché de Luxembourg, Stratégie Nationale en matière de Cybersécurité III, 2018

Parliament (Chambre Des Députés):

- Chambre Des Députés, Session ordinaire 2017-2018, Projet de Loi No 73141 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, Avis Du Conseil D'Etat (10.7.2018)

- Chambre des Députés, Session ordinaire 2017-2018, Projet de Loi N° 7314 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, Dépôt le 6.6.2018.

- Chambre Des Députés, Session ordinaire 2018-2019, Projet de Loi No 7314 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, Avis Complémentaire Du Conseil D'Etat (27.11.2018)

- Chambre Des Députés, Session ordinaire 2018-2019, Projet de Loi No 7314 portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union et modifiant 1. la loi du 23 juillet 2016 portant création d'un Haut- Commissariat à la Protection nationale et 2. la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'Etat, Deuxième Avis Complémentaire Du Conseil D'Etat (26.04.2019)

- Chambre des Députés, Séance publique n° 24, Point d'ordre du jour n° 4, Compte rendu de la Séance (15.05.2019)

Poland

Case Law (Judgments of the Supreme Administrative Court):

- Wyrok, Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 22 października 2020 r., VI SA/Wa 2666/19

- Wyrok, Wojewódzkiego Sądu Administracyjnego w Warszawie, z dnia 3 września 2020 r., VI SA/Wa 2151/19

- Wyrok, Wojewódzkiego Sądu Administracyjnego w Warszawie, z dnia 5 sierpnia 2020 r., VI SA/Wa 2667/19

Official Documents (Government of Poland):

- Ministerstwo Spraw Wewnętrznych I Administracji, 'Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej Na Lata 2011-2016', Czerwiec 2010

- Ministerstwo Cyfryzacji, 'Strategia Cyberbezpieczenstwa Rzeczypospolitej Polskiej Na Lata 2017–2022', 2017

- Ministerstwo Cyfryzacji, 'Materiały dla Operatorów Usług Kluczowych -Metodyka statycznej i dynamicznej analizy ryzyka', 30 May 2019

- Ministry of Administration and Digitisation, Internal Security Agency, 'Cyberspace Protection Policy of The Republic Of Poland', June 2013

- Ministry of Digital Affairs, 'Cybersecurity Strategy Of The Republic Of Poland For 2019–2024', 2019

Legislation (Polish Internet System of Legal Acts - ISAP):

Law:

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560

- Ustawa z dnia 9 czerwca 2011 r. Prawo geologiczne i górnicze, Dz.U. 2011 Nr 163 poz. 981

- Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, Dz. U. z 2012 r. poz. 855 - Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r. Nr 89, poz. 590

- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. z 2007 r. Nr 89, poz. 590

- Ustawa z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, Dz.U. 2005 nr 169 poz. 1414

- Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług, Dz.U. z 2004 r. Nr 54, poz. 535

- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. z 2004 r. Nr 171, poz. 1800

- Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczenstwa Wewnetrznego oraz Agencji Wywiadu, Dz.U. z 2002 r. Nr 74, poz. 676

- Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, Dz.U. 1997 Nr 54 poz.348

- Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe, Dz.U. 1997 Nr 140 poz. 939

Ordinance:

- Zarządzenie Nr 17 Ministra Gospodarki Morskiej I Żeglugi Śródlądowej z dnia 7 kwietnia 2020 r. w sprawie warunków organizacyjno-technicznych oraz zgłaszania incydentów w ramach krajowego systemu cyberbezpieczeństwa w podsektorze transportu wodnego i w sektorze zaopatrzenia w wodę pitną i jej dystrybucji, Dz.Urz.MGMiŻŚ.2020.20

Regulation:

- Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz. U. z 2010 r Nr 83, poz. 542

- Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Dz.U. 2018 poz. 1806

- Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny, Dz.U. 2018 poz. 2180

- Rozporządzenie Rady Ministrów z dnia 23 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz.U. 2019 poz. 2479

Parliament (Sejm of the Republic of Poland):

- SEJM Rzeczypospolitej Polskiej, Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa, Druk nr 2505, 30.04.2018

- SEJM Rzeczypospolitej Polskiej, 'Dodatkowe sprawozdanie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Komisji Obrony Narodowej o rządowym projekcie ustawy o krajowym systemie cyberbezpieczeństwa, Druk nr 2659-A

- SEJM Rzeczypospolitej Polskiej, 'Raport z konsultacji publicznych i opiniowania projektu ustawy o krajowym systemie cyberbezpieczeństwa', Druk nr 2505 cz. II, 30.04.2018

List of Interviews

A/A	Entity
Interview 1	European Commission, DG CONNECT
Interview 2	National Cybersecurity Agency
Interview 3	National Cybersecurity Authority
Interview 4	National Cybersecurity Agency
Interview 5	European Union Agency
Interview 6	Information Sharing & Analysis Centre
Interview 7	European Union Body
Interview 8	Information Systems Director, Hospital Center
Interview 9	Data Protection Officer, Seaport
Interview 10	Information Systems Director, Airport

Appendix

Appendix 1: Directive 2016/1148 Provisions Typology

(Table made by author)

	Types of Obligations			
	To Act		**Not to Act**	**Volontary**
Actors	***Of Result***	***Of means***		
Commission				In order to contribute to the provision of comparable information, the Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical guidelines on parameters for the information referred to in this paragraph. (Art.5§7)
	The Commission shall publish the list of designated single points of contacts. (Art.8§7)			
	The Commission shall provide the secretariat. (Art.11§2 al.3)			
	The Commission shall adopt implementing acts laying down procedural arrangements necessary for the functioning of the Cooperation Group. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2). For the purposes of the first subparagraph, the Commission shall submit the first draft implementing act to the committee referred to in Article 22(1) by 9 February 2017. (Art.11§5)			
		The Commission shall adopt implementing acts in order to specify further the elements referred to in paragraph 1 and the parameters listed in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2) by 9 August 2017. (Art.16§8)		
				The Commission may adopt implementing acts laying down the formats and procedures applicable to notification requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 22(2). (Art.16§9)
	By 9 May 2019, the Commission shall submit a report to the European Parliament and to Council, assessing the consistency of the approach taken by Member States in the identification of the operators of essential services. (Art.23§1)			

	The Commission shall periodically review the functioning of this Directive and report to the European Parliament and to the Council. For this purpose and with a view to further advancing the strategic and operational cooperation, the Commission shall take into account the reports of the Cooperation Group and the CSIRTs network on the experience gained at a strategic and operational level. In its review, the Commission shall also assess the lists contained in Annexes II and III, and the consistency in the identification of operators of essential services and services in the sectors referred to in Annex II. The first report shall be submitted by 9 May 2021. (Art.23§2)			
Union		The Union may conclude international agreements, in accordance with Article 218 TFEU, with third countries or international organisations, allowing and organising their participation in some activities of the Cooperation Group. Such agreements shall take into account the need to ensure adequate protection of data. (Art.13§1)		
Member States	When determining the significance of a disruptive effect as referred to in point (c) of Article 5(2), Member States shall take into account at least the following cross-sectoral factors: (a) the number of users relying on the service provided by the entity concerned; (b) the dependency of other sectors referred to in Annex II on the service provided by that entity; (c) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; (d) the market share of that entity; (e) the geographic spread with regard to the area that could be affected by an incident; (f) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service. (Art.6§1)			
	In order to determine whether an incident would have a significant disruptive effect, Member States shall also, where appropriate, take into account sector-specific factors. (Art.6§2)			

	Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. (Art.7)			
	Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption. *In so doing, Member States may exclude elements of the strategy which relate to national security.* (Art.7§3)			
	Each Member State shall designate one or more national competent authorities on the security of network and information systems ('competent authority'), covering at least the sectors referred to in Annex II and the services referred to in Annex III. Member States may assign this role to an existing authority or authorities. (Art.8§1)			
	Each Member State shall designate a national single point of contact on the security of network and information systems ('single point of contact'). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact. (Art.8§3)			
		Member States shall ensure that the competent authorities and the single points of contact have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Directive. Member States shall ensure effective, efficient, and secure cooperation of the designated representatives in the Cooperation Group. (Art.8§5)		
	Each Member State shall notify to the Commission without delay the designation of the competent authority and single point of contact, their tasks, and any subsequent change thereto. Each Member State shall make public its designation of the competent authority and single point of contact. The Commission shall publish the list of designated single points of contacts. (Art.8§7)			

	Each Member State shall designate one or more CSIRTs which shall comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, responsible for risk and incident handling in accordance with a well-defined process. A CSIRT may be established within a competent authority. (Art. 9§1)			
		Member States shall ensure that the CSIRTs have adequate resources to effectively carry out their tasks as set out in point (2) of Annex I. Member States shall ensure the effective, efficient, and secure cooperation of their CSIRTs in the CSIRTs network referred to in Article 12. (Art.9§2)		
		Member States shall ensure that their CSIRTs have access to an appropriate, secure, and resilient communication and information infrastructure at national level. (Art.9§3)		
		Member States shall inform the Commission about the remit, as well as the main elements of the incident- handling process, of their CSIRTs. (Art.9§4)		
				Member States may request the assistance of ENISA in developing national CSIRTs. (Art.9§5)
		Where they are separate, the competent authority, the single point of contact and the CSIRT of the same Member State shall cooperate with regard to the fulfilment of the obligations laid down in this Directive. (Art.10§1)		
		Member States shall ensure that either the competent authorities or the CSIRTs receive incident notifications submitted pursuant to this Directive. Where a Member State decides that CSIRTs shall not receive notifications, the CSIRTs shall, to the extent necessary to fulfil their tasks, be granted access to data on incidents notified by operators of essential services, pursuant to Article 14(3) and (5), or by digital service providers, pursuant to Article 16(3) and (6). (Art.10§2)		
		Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive. (Art.10§3 al.1)		
	Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed. (Art.14§1)			

	Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services. (Art.14§2)			
	Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability. (Art.14§3)			
		Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of network and information systems. (Art.15§1)		
		Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide: (a) the information necessary to assess the security of their network and information systems, including documented security policies; (b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority. When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required. (Art.15§2)		
		Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards. (Art.16§1)		

		Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services. (Art.16§2)		
		Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability. (Art.16§3)		
			Without prejudice to Article 1(6), Member States shall not impose any further security or notification requirements on digital service providers. (Art.16§10)	
			Chapter V shall not apply to micro- and small enterprises as defined in Commission Recommendation 2003/361/EC (1). (Art.16§11)	
		Member States shall ensure that the competent authorities take action, if necessary, through ex post supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State where the service is provided. (Art.17§1)		
			For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in that Member State. (Art.18§1)	
			In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems. (Art.19§1)	

	When processing (voluntary) notifications, Member States shall act in accordance with the procedure set out in Article 14. Member States may prioritise the processing of mandatory notifications over voluntary notifications. Voluntary notifications shall only be processed where such processing does not constitute a disproportionate or undue burden on Member States concerned. Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification. (Art.20§2)			
	Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate, and dissuasive. Member States shall, by 9 May 2018, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them. (Art.21)			
	By 9 February 2017 and for the purposes of this Article, Member States shall ensure appropriate representation in the Cooperation Group and the CSIRTs network. (Art.24§3)			
	Member States shall adopt and publish, by 9 May 2018, the laws, regulations, and administrative provisions necessary to comply with this Directive. They shall immediately inform the Commission thereof. They shall apply those measures from 10 May 2018. When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such a reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States. (Art.25§1)			
	Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive. (Art.25§2)			

National competent authorities and single point of contact		The competent authorities shall monitor the application of this Directive at national level. (Art.8§2)		
		The single point of contact shall exercise a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group referred to in Article 11 and the CSIRTs network referred to in Article 12. (Art.8§4)		
		The competent authorities and single point of contact shall, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities. (Art.8§6)		
		By 9 August 2018, and every year thereafter, the single point of contact shall submit a summary report to the Cooperation Group on the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken in accordance with Article 14(3) and (5) and Article 16(3) and (6). (Art.10§3 al.2)		
	On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification. (Art.14§5 al.1)			
	Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling. (Art.14§5 al.2)			
	At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States. (Art. 14§5 al.3)			

				After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident. (Art.14§6)
				Competent authorities acting together within the Cooperation Group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident as referred to in paragraph 4. (Art.14§7)
				Following the assessment of information or results of security audits referred to in paragraph 2, the competent authority may issue binding instructions to the operators of essential services to remedy the deficiencies identified. (Art.15§3)
		The competent authority shall work in close cooperation with data protection authorities when addressing incidents resulting in personal data breaches. (Art.15§4)		
	Member States shall ensure that the competent authorities or the CSIRTs inform the single points of contact about incident notifications submitted pursuant to this Directive. (Art.10§3 al.1)			
	Member States shall ensure that the competent authorities have the necessary powers and means to assess the compliance of operators of essential services with their obligations under Article 14 and the effects thereof on the security of network and information systems. (Art.15§1)			
	Member States shall ensure that the competent authorities have the powers and means to require operators of essential services to provide: (a) the information necessary to assess the security of their network and information systems, including documented security policies; (b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority. When requesting such information or evidence, the competent authority shall state the purpose of the request and specify what information is required. (Art.15§2)			

	Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided. (Art.16§6)			
	After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest. (Art.16§7)			
	Member States shall ensure that the competent authorities take action, if necessary, through ex post supervisory measures, when provided with evidence that a digital service provider does not meet the requirements laid down in Article 16. Such evidence may be submitted by a competent authority of another Member State where the service is provided. (Art.17§1)			
	For the purposes of paragraph 1, the competent authorities shall have the necessary powers and means to require digital service providers to: (a) provide the information necessary to assess the security of their network and information systems, including documented security policies; (b) remedy any failure to meet the requirements laid down in Article 16. (Art.17§2)			
		If a digital service provider has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and the competent authorities of those other Member States shall cooperate and assist each other as necessary. Such assistance and cooperation may cover information exchanges between the competent authorities concerned and requests to take the supervisory measures referred to in paragraph 2. (Art.17§3)		

Computer security incident response teams (CSIRTs)	On the basis of the information provided in the notification by the operator of essential services, the competent authority or the CSIRT shall inform the other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. In so doing, the competent authority or the CSIRT shall, in accordance with Union law or national legislation that complies with Union law, preserve the security and commercial interests of the operator of essential services, as well as the confidentiality of the information provided in its notification. (Art.14§5 al.1)			
	Where the circumstances allow, the competent authority or the CSIRT shall provide the notifying operator of essential services with relevant information regarding the follow-up of its notification, such as information that could support the effective incident handling. (Art.14§5 al.2)			
	At the request of the competent authority or the CSIRT, the single point of contact shall forward notifications as referred to in the first subparagraph to single points of contact of other affected Member States. (Art. 14§5 al.3)			
				After consulting the notifying operator of essential services, the competent authority or the CSIRT may inform the public about individual incidents, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident. (Art.14§6)
	Where appropriate, and in particular if the incident referred to in paragraph 3 concerns two or more Member States, the competent authority or the CSIRT shall inform the other affected Member States. In so doing, the competent authorities, CSIRTs and single points of contact shall, in accordance with Union law, or national legislation that complies with Union law, preserve the digital service provider's security and commercial interests as well as the confidentiality of the information provided. (Art.16§6)			

	After consulting the digital service provider concerned, the competent authority or the CSIRT and, where appropriate, the authorities or the CSIRTs of other Member States concerned may inform the public about individual incidents or require the digital service provider to do so, where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or where disclosure of the incident is otherwise in the public interest. (Art.16§7)			
	Without prejudice to Article 25 and with a view to providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs network shall begin to perform the tasks set out in Articles 11(3) and 12(3) respectively by 9 February 2017. (Art.24§1)			
	CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners. (b) CSIRTs' premises and the supporting information systems shall be located in secure sites. (c) Business continuity: (i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers. (ii) CSIRTs shall be adequately staffed to ensure availability at all times. (iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available. (d) CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks. (2) CSIRTs' tasks: (a) CSIRTs' tasks shall include at least the following: (i) monitoring incidents at a national level; (ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents; (iii) responding to incidents; (iv) providing dynamic risk and incident analysis and situational awareness; (v) participating in the CSIRTs network. (b) CSIRTs shall establish cooperation relationships with the			

	private sector. (c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for: (i) incident and risk-handling procedures; (ii) incident, risk and information classification schemes. (ANNEXE I)			
Cooperation Group		The Cooperation Group shall carry out its tasks on the basis of biennial work programmes as referred to in the second subparagraph of paragraph 3. (Art.11§1 al.2)		
	The Cooperation Group shall be composed of representatives of the Member States, the Commission and ENISA. Where appropriate, the Cooperation Group may invite representatives of the relevant stakeholders to participate in its work. The Commission shall provide the secretariat. (Art.11§2)			

	The Cooperation Group shall have the following tasks: (a) providing strategic guidance for the activities of the CSIRTs network established under Article 12; (b) exchanging best practice on the exchange of information related to incident notification as referred to in Article 14(3) and (5) and Article 16(3) and (6); (c) exchanging best practice between Member States and, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information systems; (d) discussing capabilities and preparedness of the Member States, and, on a voluntary basis, evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice; (e) exchanging information and best practice on awareness-raising and training; (f) exchanging information and best practice on research and development relating to the security of network and information systems; (g) where relevant, exchanging experiences on matters concerning the security of network and information systems with relevant Union institutions, bodies, offices and agencies; (h) discussing the standards and specifications referred to in Article 19 with representatives from the relevant European standardisation organisations; (i) collecting best practice information on risks and incidents; (j) examining, on an annual basis, the summary reports referred to in the second subparagraph of Article 10(3); (k) discussing the work undertaken with regard to exercises relating to the security of network and information systems, education programmes and training, including the work done by ENISA; (l) with ENISA's assistance, exchanging best practice with regard to the identification of operators of essential services by the Member States, including in relation to cross-border dependencies, regarding risks and incidents; (m) discussing modalities for reporting notifications of incidents as referred to in Articles 14 and 16. (Art.11§3)			

	By 9 February 2018 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks, which shall be consistent with the objectives of this Directive. (Art.11§3)			
	For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the Cooperation Group shall prepare a report assessing the experience gained with the strategic cooperation pursued under this Article. (Art.11§4)			
	Without prejudice to Article 25 and with a view to providing Member States with additional possibilities for appropriate cooperation during the period of transposition, the Cooperation Group and the CSIRTs network shall begin to perform the tasks set out in Articles 11(3) and 12(3) respectively by 9 February 2017. (Art.24§1)			
	For the period from 9 February 2017 to 9 November 2018, and for the purposes of supporting Member States in taking a consistent approach in the process of identification of operators of essential services, the Cooperation Group shall discuss the process, substance and type of national measures allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6. The Cooperation Group shall also discuss, at the request of a Member State, specific draft national measures of that Member State, allowing for the identification of operators of essential services within a specific sector in accordance with the criteria set out in Articles 5 and 6. (Art.24§2)			
CSIRTs network	*The CSIRTs network shall be composed of representatives of the Member States' CSIRTs and CERT-EU. The Commission shall participate in the CSIRTs network as an observer. ENISA shall provide the secretariat and shall actively support the cooperation among the CSIRTs. (Art.12§2)*			

	The CSIRTs network shall have the following tasks: (a) exchanging information on CSIRTs' services, operations and cooperation capabilities; (b) at the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Member State's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident; (c) exchanging and making available on a voluntary basis non-confidential information concerning individual incidents; (d) at the request of a representative of a Member State's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Member State; (e) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance; (f) discussing, exploring and identifying further forms of operational cooperation, including in relation to: (i) categories of risks and incidents; (ii) early warnings; (iii) mutual assistance; (iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents; (g) informing the Cooperation Group of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard; (h) discussing lessons learnt from exercises relating to the security of network and information systems, including from those organised by ENISA; (i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT; (j) issuing guidelines in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation. (Art.12§3)			
	For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations,			

	pursued under this Article. That report shall also be submitted to the Cooperation Group. (Art.12§4)			
		The CSIRTs network shall lay down its own rules of procedure. (Art.12§5)		
OES		Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed. (Art.14§1)		
		Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services. (Art.14§2)		
	Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability. (Art.14§3)			
	Where an operator of essential services relies on a third-party digital service provider for the provision of a service which is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall be notified by that operator. (Art.16§5)			

DSP		Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements: (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards. (Art.16§1)		
		Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services. (Art.16§2)		
		Member States shall ensure that digital service providers notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability. (Art.16§3)		
	A digital service provider that is not established in the Union, but offers services referred to in Annex III within the Union, shall designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The digital service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established. (Art.18§2)			
	The designation of a representative by the digital service provider shall be without prejudice to legal actions which could be initiated against the digital service provider itself. (Art.18§3)			

Appendix 2: Types of essential entities falling within the scope of the NIS Directive

Source: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148*

SECTOR	SUBSECTOR	TYPE OF ENTITY
1. ENERGY	(a) Electricity	**Electricity undertakings**: *any natural or legal person carrying out at least one of the following functions: generation, transmission, distribution, supply, or purchase of electricity, which is responsible for the commercial, technical or maintenance tasks related to those functions, but does not include final customers.*[1]
		Distribution system operators: *a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity.*[2]
		Transmission system operators: *a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity.*[3]
	(b) Oil	**Operators of oil transmission pipelines**
		Operators of oil production, refining and treatment facilities, storage, and transmission
	(c) Gas	**Supply undertakings**: *any natural or legal person who carries out the function of supply*.[4]
		Distribution system operators: *a natural or legal person who carries out the function of distribution and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of gas.*[5]

[1] Point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC.

[2] Point (6), *ibid.*

[3] Point (4), *ibid.*

[4] Point (8), *ibid.*

[5] Point (6), *ibid.*

		Transmission system operators: *a natural or legal person who carries out the function of transmission and is responsible for operating, ensuring the maintenance of, and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transport of gas.*[1]
		Storage system operators: *a natural or legal person who carries out the function of storage and is responsible for operating a storage facility.*[2]
		LNG system operators: *a natural or legal person who carries out the function of liquefaction of natural gas, or the importation, offloading, and re-gasification of LNG and is responsible for operating an LNG facility.*[3]
		Natural gas undertakings: *a natural or legal person carrying out at least one of the following functions: production, transmission, distribution, supply, purchase, or storage of natural gas, including LNG, which is responsible for the commercial, technical and/or maintenance tasks related to those functions, but shall not include final customers.*[4]
		Operators of natural gas refining and treatment facilities
2. TRANSPORT	(a) Air transport	**Air carriers**: *an air transport undertaking holding a valid operating licence or equivalent.*[5]
		Airport managing bodies: *a body which, in conjunction with other activities or not as the case may be, has as its objective under national laws, regulations or contracts the administration and management of the airport or airport network infrastructures and the coordination and control of the activities of the different operators present in the airports or airport network concerned.*[6] **Airports**: *any land area specifically adapted for the landing, taking-off and manoeuvring of aircraft, including the ancillary installations which these*

[1] Point (4), *ibid.*

[2] Point (10), *ibid.*

[3] Point (12), *ibid.*

[4] Point (1), *ibid.*

[5] Point (4) of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

[6] Point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges.

		operations may involve for the requirements of aircraft traffic and services, including the installations needed to assist commercial air services.[1]
		Entities operating ancillary installations contained within airports
		Traffic management control operators providing air traffic control (ATC) services: *a service provided for the purpose of preventing collisions between aircraft, and in the manoeuvring area between aircraft and obstructions; and expediting and maintaining an orderly flow of air traffic.*[2]
	(b) Rail transport	**Infrastructure managers**: *any body or firm responsible in particular for establishing, managing and maintaining railway infrastructure, including traffic management and control-command and signalling; the functions of the infrastructure manager on a network or part of a network may be allocated to different bodies or firms.*[3]
		Railway undertakings: *any public or private undertaking licensed according to this Directive, the principal business of which is to provide services for the transport of goods and/or passengers by rail with a requirement that the undertaking ensure traction; this also includes undertakings which provide traction only.*[4]
	(c) Water transport	**Inland, sea and coastal passenger and freight water transport companies**: *The owner of the ship or any other organization or person such as the manager, or the bareboat charterer, who has assumed the responsibility for operation of the ship from the owner of the ship and who on assuming such responsibility has agreed to take over all the duties and responsibilities imposed by the International Safety Management Code*[5]*, not including the individual vessels operated by those companies.*
		Managing bodies of ports: *any specified area of land and water, with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial*

[1] Point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans–European transport network and repealing Decision No 661/2010/EU.

[2] Point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation).

[3] Point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area.

[4] Point (1) and (12), *ibid.*

[5] Maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security.

		maritime transport operations,[1] including their **port facilities**,[2] and **entities operating works and equipment contained within ports.**
		Operators of vessel traffic services (VTS): *a service designed to improve the safety and efficiency of vessel traffic and to protect the environment, which has the capability to interact with the traffic and to respond to traffic situations developing in the VTS area.*[3]
	(d) Road transport	**Road authorities**: *any public authority responsible for the planning, control or management of roads falling within its territorial competence.*[4]
		Operators of Intelligent Transport Systems: *systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles, and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport.*[5]
3. BANKING		**Credit institutions**: *an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account.*[6]
4. FINANCIAL MARKET INFRASTRUCTURES		**Operators of trading venues**: *operators of regulated market, an MTF or an OTF.*[7]
		Central counterparties (CCPs): *a legal person that interposes itself between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer.*[8]

[1] Point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security.

[2] a location where the ship/port interface takes place; this includes areas such as anchorages, awaiting berths and approaches from seaward, as appropriate - Point (11) of Article 2 of Regulation (EC) No 725/2004.

[3] Point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC.

[4] Point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU–wide real–time traffic information services.

[5] Point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[6] Point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.

[7] Point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

[8] Point (1) of Article 2 of Regulation (Eu) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties, and trade repositories.

5. HEALTH SECTOR	Health care settings *(including hospitals and private clinics)*	**Healthcare providers**: *any natural or legal person or any other entity legally providing healthcare on the territory of a Member State.*[1]
6. DRINKING WATER SUPPLY AND DISTRIBUTION		***Suppliers and distributors of water intended for human consumption**: all water either in its original state or after treatment, intended for drinking, cooking, food preparation or other domestic purposes, regardless of its origin and whether it is supplied from a distribution network, from a tanker, or in bottles or containers,*[2] *but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services.*
7. DIGITAL INFRASTRUCTURE		**IXPs** : *a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic.*[3] **DNS service providers**: *Providers of a hierarchical distributed naming system in a network which refers queries for domain names.* **TLD name registries**: *an entity which administers and operates the registration of internet domain names under a specific top-level domain (TLD)*

[1] Point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross–border healthcare.

[2] Point (1)(a) of Article 2 of Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption.

[3] Article 4 (13) NIS Directive.

Appendix 3: Types of essential sectors as defined by ENISA

Source: *ENISA (2014), Methodologies for the identification of Critical Information Infrastructure assets and services*

Critical Sector	Critical subsector	Critical services
1. Energy	Electricity	• Generation (all forms) • Transmission / Distribution • Electricity Market
	Petroleum	• Extraction • Refinement • Transport • Storage
	Natural Gas	• Extraction • Transport / Distribution • Storage
2. Information, Communication Technologies (ICT)	Information Technologies	• Web services • Datacentre/ cloud services • Software as a Service
	Communications	• Voice/ Data communication • Internet connectivity
3. Water	Drinking water	• Water storage • Water distribution • Water quality assurance
	Wastewater	Wastewater collection & treatment
4. Food		• Agriculture / Food production • Food supply • Food distribution • Food quality/safety
5. Health		• Emergency healthcare • Hospital care (inpatient & outpatient) • Supply of pharmaceuticals, vaccines, blood, medical supplies • Infection/epidemic control
6. Financial services		• Banking • Payment transactions • Stock Exchange

7. Public Order and Safety		• Maintenance of public order and safety • Judiciary and penal systems
8. Transport	Aviation	• Air navigation services • Airports' operation
	Road transport	• Bus / Tram services • Maintenance of the road network
	Train transport	• Management of public railway • Railway transport services
	Maritime transport	• Monitoring and management of shipping traffic • Ice-breaking operations
	Postal/ Shipping	
9. Industry	Critical industries	• Employment[18]
	Chemical / Nuclear Industry	• Storage and disposal of hazardous materials • Safety of high-risk industrial units
10. Civil Administration		• Government functions
11. Space		• Protection of space-based systems
12. Civil protection		• Emergency and rescue services
13. Environment		• Air pollution monitoring and early warning • Meteorological monitoring and early warning • Ground Water (lake/river) monitoring and early warning • Marine pollution monitoring and control
14. Defence		National defence

Appendix 4: OES Security measures Checklist

(Table made by author)

NIS Directive Security Measures Checklist		
Nr.	**Criteria's**	**Details**
1.	**Governance and Ecosystem**	
1.1	**Information System Security Risk Analysis**	Délai d'application : 3 ans pour un système d'information essentiel (SIE) mis en service antérieurement à la date de désignation de l'opérateur de services essentiels. 2 ans pour un SIE mis en service dans un délai de 2 ans à compter de la date de désignation de l'opérateur de services essentiels. Avant sa mise en service pour un SIE mis en service dans un délai supérieur à 2 ans à compter de la date de désignation de l'opérateur de services essentiels.
1.1.1	**The essential services operator performs and maintains a risk analysis of its essential information systems (EIS).**	This risk analysis takes into account, in particular, the analysis that the operator conducted to identify its information systems as EIS.
1.2	**Information System Security Policy**	Délai d'application : 1 an
1.2.1	**The Essential Services Operator develops, maintains and implements a Network and Information System Security Policy (PSSI).**	The PSSI describes the set of procedures and organizational and technical means implemented by the operator to ensure the security of its essential information systems (EIS). In the area of security governance, the PSSI defines: - strategic objectives and directions for EIS security; - the organization of security governance, including the roles and responsibilities of internal staff and external staff (contractors, suppliers, etc.) with respect to EIS security; - EIS safety awareness plans for all staff as well as EIS safety training plans for individuals with special responsibilities, including those in charge of administration and training; EIS security and users with privileged access rights to EIS; - the EIS safety approval procedure; - the procedures for the control and audit of the security of the EIS, in particular those implemented as part of the security accreditation. In the area of protection, the PSSI defines: - general security measures, in particular as regards the management and security of EIS hardware and software resources, access control to EIS, operation and administration of EIS and network security, workstations and data; - the physical and environmental security procedures and measures applicable to EIS; - the procedure for keeping the EIS resources in safe condition. In the field of defense, the PSSI defines: - the procedure for detecting security incidents; - the procedure for handling security incidents. In the area of business resiliency, the PSSI defines: - the crisis management procedure in case of security incidents having a major impact on the essential services of the operator; - continuity and recovery procedures. The PSSI and its application documents are formally approved by the operator's management.
1.2.2	**The operator prepares for his management, at least annually, a report on the implementation of the PSSI and its application documents.**	This report specifies in particular the state of the risks, the level of security of the EIS and the security actions carried out and planned.
1.2.3	**The operator keeps the PSSI, its application documents and reports on their implementation at the disposal of the NCA/SPOC**	

1.3	**Information System Security Accreditation**	Délai d'application : 3 ans pour un système d'information essentiel (SIE) mis en service antérieurement à la date de désignation de l'opérateur de services essentiels. 2 ans pour un SIE mis en service dans un délai de 2 ans à compter de la date de désignation de l'opérateur de services essentiels. Avant sa mise en service pour un SIE mis en service dans un délai supérieur à 2 ans à compter de la date de désignation de l'opérateur de services essentiels.
1.3.1	**The essential services operator performs the security accreditation of each essential information system (EIS), implementing the certification procedure provided for by its network and information systems security policy.**	The approval of a system is a formal decision taken by the operator that attests that the risks to the security of this system have been identified and that the necessary measures to protect it have been implemented. It also certifies that any residual risks have been identified and accepted by the operator. As part of the certification, an EIS security audit must be performed. The operator makes the decision to approve an EIS on the basis of the accreditation file including: - the risk analysis and security objectives of the EIS; - the procedures and security measures applied to the EIS; - EIS security audit reports; - the residual risks and the reasons justifying their acceptance.
1.3.2	**The validity of the approval shall be reviewed by the operator at least every three years and at each event or change likely to change the context described in the approval file.**	Each re-examination of the approval shall be recorded in the approval file. The operator proceeds to the renewal of the accreditation as soon as it is no longer valid.
1.3.3	**The operator keeps the decisions and accreditation files at the disposal of the NCA/SPOC.**	
1.4	**Information System Security Indicators**	Délai d'application : 2 ans
1.4.1	**The essential services operator evaluates and maintains, for each Essential Information System (EIS), the following indicators:**	- indicators relating to the maintenance in conditions of security of the resources:- the percentage of user stations whose system resources are not installed in a version supported by the supplier or the manufacturer;- the percentage of servers whose system resources are not installed in a version supported by the supplier or the manufacturer;- indicators relating to user access rights and authentication of access to resources:- the percentage of users accessing EIS through privileged accounts;- the percentage of resources whose secret authentication elements can not be modified by the operator;- indicators relating to the administration of resources:- the percentage of administered resources administered from a non-specific administration account;- The percentage of managed resources that can not be administered over a physical network link or a physical administration interface.
1.4.2	**The operator specifies for each indicator the evaluation method used and, if applicable, the uncertainty of its evaluation.**	When an indicator changes significantly compared to the previous evaluation, the operator explains the reasons.
1.4.3	**The operator communicates to the NCA/SPOC, at its request, the updated indicators on an electronic medium.**	
1.5	**Information System Security Audit**	Délai d'application : 3 ans pour un système d'information essentiel (SIE) mis en service antérieurement à la date de désignation de l'opérateur de services essentiels. 2 ans pour un SIE mis en service dans un délai de 2 ans à compter de la date de désignation de l'opérateur de services essentiels. Avant sa mise en service pour un SIE mis en service dans un délai supérieur à 2 ans à compter de la date de désignation de l'opérateur de services essentiels.

1.5.1	**The essential services operator carries out, as part of the security accreditation, an audit of the security of each essential information system (EIS). The audit must also be carried out at each renewal of approval, taking into account, in particular, the results of the update of the EIS risk analysis.**	This audit aims to verify the application and effectiveness of the EIS security measures and in particular the respect of the present security rules. It should assess the level of security of the EIS with respect to known threats and vulnerabilities and include the conduct of an architecture audit, a configuration audit and an organizational and physical audit. The operator or the service provider appointed for this purpose carries out this audit, based on the requirements of the reference system for auditing the security of information systems adopted pursuant to Article 10 of Decree No 2015-350 of the 27 March 2015, amended on the qualification of security products and trusted service providers for information system security purposes.
1.5.2	**At the end of the audit, the operator or, where applicable, the service provider draws up an audit report which sets out the findings on the measures applied and on compliance with these safety rules.**	The report specifies whether the level of security achieved is consistent with security objectives, given known threats and vulnerabilities. It formulates recommendations to remedy any nonconformities and vulnerabilities discovered.
1.6	**Human Resource Security**	Doesn't appears in french law transposition
1.6.1	**Validation of professional references of key personnel (system administrators, security officers, guards, etc...)**	Documentation of checks of professional references for key personnel.
1.6.2	**Training material provision to key personnel on security issues**	Evidence of personnel attendance to the training (e.g. Accepted invitation, date and agenda of training, signed participation list during the awareness workshop etc.)
1.6.3	**Formal appointment of key personnel formally in necessary security roles**	- List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles. - Organization's organigram in place, job descriptions signed by key personnel, relevant role trainings attended.
1.6.4	**Regular review and update of policies/procedures for the Human Resource security, taking into account possible changes**	- Comments or change logs of the policy/procedures. - Review time-plan versions of the policies/ procedures providing the changes that took place.
1.7	**Asset Management - Ecosystem mapping & relations**	Délai d'application : 1 an
1.7.1	**The essential services operator develops and maintains for each critical information system (EIS) the following mapping elements:**	- the names and functions of the applications, supporting the activities of the operator, installed on the EIS;- where applicable, the SIE output IP address ranges to the internet or a third party network, or accessible from these networks;- where applicable, the IP address ranges associated with the different subnetworks composing the EIS;- the functional description and installation locations of the EIS and its various sub-networks;- the functional description of the interconnection points of the EIS and its different sub-networks with third-party networks, in particular the description of the equipment and the filtering and protection functions implemented at these interconnections;- the inventory and the architecture of the administration devices of the EIS allowing to carry out in particular the operations of remote installation, update, supervision, management of the configurations, authentication as well as management of the accounts and access rights;- the list of accounts with privileged access rights to the SIE (called "privileged accounts"). This list specifies for each account the level and scope of associated access rights, including the accounts to which these rights bear (user accounts, e-mail accounts, process accounts, etc.);- the inventory, architecture and positioning of the hostname, messaging, Internet relay and remote access services implemented by the EIS.
1.7.2	**The operator communicates to the NCA/SPOC, at its request, updated cartographic elements on an electronic medium.**	
2.	**Network & Information System Protection**	
2.1	**IT Security Architecture**	
2.1.1	*Systems Configuration*	Délai d'application : 1 an

2.1.1.1	**The essential services operator follows the following rules when installing services and equipment on its essential information systems (EIS).**	- the operator installs on his EIS the only services and functionalities which are essential for their functioning or their security. It disables services and features that are not needed, such as those installed by default, and uninstalls them if possible. When the uninstallation is not possible, the operator mentions it in the homologation file of the concerned EIS, specifying the services and functionalities concerned and the risk reduction measures implemented; - the operator only connects to his EIS equipment, peripheral equipment and removable media which he manages and which are essential for the operation or security of his EIS; - writable removable media connected to EIS are used exclusively for operation, including maintenance and administration, or EIS security; - The operator proceeds, before each use of removable media, the analysis of their content, including the search for malicious code.
2.1.1.2	**The operator sets up, on the equipment to which these removable media are connected, protection mechanisms against the risk of execution of malicious code from these media.**	
2.1.2	***System Segregation***	Délai d'application : 2 ans
2.1.2.1	**The essential services operator is partitioning its critical information systems (EIS) to limit the spread of cyber attacks within its systems or subsystems. He respects the following rules:**	- each EIS is physically or logically partitioned vis-à-vis other information systems of the operator and information systems of third parties; - When a SIE itself consists of subsystems, they are partitioned between them physically or logically. A subsystem may be formed to provide a feature or a homogeneous set of functionality of an EIS or to isolate resources from an EIS requiring the same security requirement; - only the interconnections strictly necessary for the proper functioning and security of an EIS are established between the EIS and other systems or between subsystems of the EIS. In the particular case of an interconnection between the Internet and an EIS necessary for the provision of hosting services for domain names, hosting of top-level zones, resolution of domain names or interconnection by pairing for the Internet. exchange of Internet traffic, the operator is not required to ensure a physical or logical partitioning at the level of this interconnection but implements appropriate protection measures such as those recommended by the NCA/SPOC.
2.1.2.2	**When an essential service requires the EIS necessary for its provision to be accessible via a public network, the operator organizes this EIS, according to the principle of defense in depth, into at least two subsystems as follows:**	- a first subsystem corresponding to the part of the EIS directly accessible via this public network, to which the operator applies appropriate partitioning measures such as those recommended by the NCA/SPOC;a second subsystem corresponding to the internal part of the SIE to which the operator applies this rule on the partitioning.
2.1.2.3	**The operator describes in the homologation file of each EIS the partitioning mechanisms he sets up.**	
2.1.3	***Cryptography***	Délai d'application : 2 ans
2.1.3.1	**When an essential service requires the EIS necessary for its provision to be accessible via a public network, the operator protects this access by means of cryptographic mechanisms in accordance with the rules recommended by the NCA/SPOC.**	

2.1.3.2	**When the operator or a service provider that he has appointed for this purpose accesses an EIS via an information system that is not under the control of the operator or the service provider, the operator applies or has applied to his provides the following rules:**	- access to the EIS is protected by encryption and authentication mechanisms in accordance with the rules recommended by the NCA/SPOC; when the access to the SIE is made from a site external to that of the operator, the authentication mechanism is reinforced by implementing a double factor authentication (authentication involving both a secret element and another own element) to the user), unless technical or operational reasons, specified in the EIS approval file, do not permit this; - the equipment used to access the EIS is managed and configured by the operator or, where appropriate, by the service provider. When access to the EIS is performed from a site outside the operator's, the mass memories of these devices are permanently protected by encryption and authentication mechanisms in accordance with the rules recommended by the NCA/SPOC.
2.1.3.3	**The operator describes in the homologation file of each EIS the protection mechanisms for access to the EIS that he sets up.**	
2.1.4	***Traffic Filtering***	Délai d'application : 2 ans
2.1.4.1	**The essential services operator puts in place mechanisms for filtering the flow of data circulating in its essential information systems (EIS) in order to block the flow of unnecessary flows to the operation of its systems and likely to facilitate computer attacks.**	He respects the following rules: - the operator defines the rules for filtering the data flows (filtering on the network addresses, on the protocols, on the port numbers, etc.) making it possible to limit the flow of the streams to the only data flows necessary for the operation and the security of its EIS; - the incoming and outgoing flows of the EIS as well as the flows between subsystems of the EIS are filtered at their interconnections so as to allow the circulation only of those flows strictly necessary for the operation and security of EIS. Streams that do not conform to the filter rules are blocked by default; - the operator establishes and maintains a list of filtering rules mentioning all the rules in force or deleted for less than a year. This list specifies for each rule: - the reason and date of implementation, modification or deletion of the rule; - the technical modalities for implementing the rule.
2.1.4.2	**In the particular case of an EIS necessary for the provision of a peer interconnection service for the exchange of Internet traffic, the operator sets up filtering mechanisms only for data flows other than those corresponding to the traffic internet proper.**	
2.1.4.3	**The operator describes in the homologation file of each EIS the filtering mechanisms he sets up.**	
2.2	**IT Security Administration**	
2.2.1	***Administration Accounts***	Délai d'application : 2 ans
2.2.1.1	**The essential services operator creates accounts (called "administrative accounts") for only those people (called "administrators") responsible for performing administrative operations (installation, configuration, management, maintenance, supervision, etc..) the resources of its essential information systems (EIS).**	

2.2.1.2	**The operator defines, in accordance with its network and information systems security policy, the management and allocation rules for the administrative accounts of its EIS, and complies with the following rules:**	- the allocation of rights to directors respects the principle of least privilege (only strictly necessary rights are granted). In particular, in order to limit the scope of individual rights, they are allocated to each director by restricting them as much as possible to the functional and technical scope of which this director is responsible;- an administration account is used exclusively to connect to an administration information system (information system used for resource administration operations) or to an administered resource;- administration operations are performed exclusively from administration accounts, and conversely, administration accounts are used exclusively for administration operations;- when the administration of a resource can not technically be carried out from a specific administration account, the operator puts in place measures to ensure the traceability and control of the administration operations carried out on this resource and risk reduction measures related to the use of an account not specific to the administration. It describes in the registration file of the EIS concerned these measures as well as the technical reasons that prevented the use of an administration account;- the operator establishes and maintains the list of the administrative accounts of his EIS and manages them as privileged accounts.
2.2.2	***Administration Information Systems***	Délai d'application : 2 ans
2.2.1.1	**The essential services operator applies the following rules to information systems (called "administrative information systems") used to perform the administration of its essential information systems (EIS):**	- the hardware and software resources of the administrative information systems are managed and configured by the operator or, where appropriate, by the service provider he has mandated to carry out the administration operations; - The hardware and software resources of the administrative information systems are used exclusively to carry out administration operations. However, where technical or organizational reasons so warrant, the administrator's physical workstation may be used to perform operations other than administration operations. In this case, hardening mechanisms of the workstation operating system and partitioning must be put in place to isolate the software environment used for these other operations from the software environment used for the operations of the workstation. administration; - a software environment used to perform administrative operations should not be used for other purposes, such as accessing sites or mail servers on the internet; - a user must not connect to an administrative information system by means of a software environment used for functions other than administration operations; - data flows associated with operations other than administration operations must, when passing through the administrative information systems, be partitioned by means of encryption and authentication mechanisms in accordance with the rules recommended by the NCA/SPOC; - The administration information systems are connected to the resources of the EIS to be administered through a physical network link used exclusively for the administration operations. These resources are administered through their physical administration interface. When technical reasons make it impossible to administer a resource through a physical network link or its physical administration interface, the operator implements implement risk reduction measures such as logical security measures. In this case, it describes these measures and their justifications in the homologation file of the concerned EIS; - when they do not circulate in the administration information system, the administration flows are protected by encryption and authentication mechanisms in accordance with the rules recommended by the NCA/SPOC. If the encryption and authentication of these flows are not possible for technical reasons, the operator implements measures to protect the confidentiality and integrity of these flows and to reinforce the control and traceability of operations. 'administration. In this case, it describes these measures and their justifications in the homologation file of the concerned EIS; the logs recording the events generated by the resources of the administrative information systems do not contain any password or other secret authentication element in the clear or in the form of a cryptographic fingerprint.
2.3	**Identity and Access Management**	

2.3.1	*Identification*	Délai d'application : 1 an
2.3.1.1	**The essential services operator creates individual accounts for all users (including users with privileged accounts or administrative accounts) and for automatic processes accessing resources in its critical information systems (EIS).**	
2.3.1.2	**When technical or operational reasons do not permit the creation of individual accounts for users or automatic processes, the operator puts in place measures to reduce the risk associated with the use of shared accounts and ensure traceability the use of these accounts. In this case, the operator describes these measures in the registration file of the EIS concerned and the reasons justifying the use of shared accounts.**	
2.3.1.3	**When an essential service requires the dissemination of information to the public, the operator is not required to create accounts for public access to this information.**	
2.3.1.4	**The operator immediately deactivates accounts where no longer needed.**	
2.3.2	*Authentification*	Délai d'application : 1 an
2.3.2.1	**The essential services operator protects access to the resources of its essential information systems (EIS), whether by a user or an automatic process, by means of an authentication mechanism involving a secret element.**	
2.3.2.2	**The operator defines, in accordance with its network and information systems security policy, the management rules for the secret authentication elements implemented in its EIS.**	
2.3.2.3	**When the resource technically allows it, the secret authentication elements must be able to be modified by the operator whenever necessary.**	In this case, the operator follows the following rules: - the operator must modify the secret authentication elements when they were installed by the manufacturer or the supplier of the resource, before being put into service. For this purpose, the operator shall check with the manufacturer or the supplier that he has the means and rights to carry out these operations; - the secret element of authentication of a shared account must be renewed regularly and each withdrawal of a user from this account; - the users who are not responsible for it, can not modify the secret authentication elements. Nor can they access these elements in the clear; - When secret authentication elements are passwords, users must not reuse them between privileged accounts or between a privileged account and a non-privileged account; - When the secret authentication elements are passwords, they are compliant with the rules of the art such as those recommended by the NCA/SPOC, in terms of complexity (length of password and character types), taking into account the maximum level of complexity allowed by the resource concerned, and in terms of renewal.
2.3.2.4	**When the resource does not technically make it possible to modify the secret authentication element, the operator sets up an appropriate access control for the resource concerned, as well as access traceability and risk reduction measures related to the authentication element. use of a secret authentication element fixed. The operator describes these measures and the technical reasons that prevented the modification of the secret authentication element in the EIS homologation file concerned.**	

2.3.2.5	**When an essential service requires the dissemination of information to the public, the operator is not required to put in place authentication mechanisms for public access to this information.**	
2.3.3	***Access Rights***	Délai d'application : 1 an
2.3.3.1	**The essential services operator defines, in accordance with its network and information systems security policy, the rules governing the management and allocation of access rights to the resources of its essential information systems (EIS).**	
2.4	**IT Security Maintenance**	
2.4.1	***IT Security Maintenance Procedure***	Délai d'application : 1 an
2.4.1.1	**The essential services operator develops, maintains and implements a procedure for maintaining the hardware and software resources of its essential information systems (EIS) in accordance with its network and system security policy. 'information.**	This procedure defines the conditions for maintaining the level of security of the EIS resources according to the evolution of the vulnerabilities and the threats and specifies in particular the policy of installation of any new version and corrective measure of security of a resource and the checks to be done before installation.It provides that:- the operator keeps abreast of vulnerabilities and security corrective measures that may affect the hardware and software resources of its EIS, which are disseminated by suppliers or manufacturers of these resources or by prevention and warning centers in terms of cyber security such as the CERT-FR (government center for watch, alert and response to computer attacks); - except in the case of justified technical or operational difficulties, the operator installs and maintains all the hardware and software resources of its EIS in versions supported by their suppliers or their manufacturers and including security updates;- prior to the installation of any new version, the operator ensures the origin of this version and its integrity, and analyzes the impact on the EIS concerned from a technical and operational point of view;- as soon as he becomes aware of a security corrective measure concerning one of his resources, and except in the case of justified technical or operational difficulties, the operator plans the installation after carrying out the checks mentioned in the previous paragraph , and proceeds to this installation within the time limits provided by the procedure of maintenance in safety conditions;- when justified by technical or operational reasons, the operator may decide, for certain resources of its EIS, not to install a version supported by the supplier or manufacturer of the resource concerned or not to install a security corrective measure . In this case, the operator implements technical or organizational measures provided by the procedure of maintenance in safety conditions to reduce the risks related to the use of an obsolete version or with known vulnerabilities. The operator shall describe in the EIS approval file those risk-reduction measures and the technical or operational reasons that prevented the installation of a supported version or a safety corrective measure.
2.5	**Physical and Environmental Security**	
2.5.1	***Physical and Environmental Security***	Délai d'application : 1 an
2.5.1	**The essential services operator defines and implements, in accordance with its network and information systems security policy, the physical and environmental security procedures and measures applicable to its essential information systems (EIS).**	These procedures and measures include control of internal and external personnel, physical access control to EIS and, where appropriate, protection of EIS from environmental hazards such as natural disasters.
3.	**Network & Information System Defence**	
3.1	**Incident Detection**	
3.1.1	***Detection***	Délai d'application : 2 ans

3.1.1.1	**The essential services operator develops, maintains and implements, in accordance with its network and information systems security policy, a procedure for detecting security incidents affecting its essential information systems (EIS).**	This procedure provides for organizational and technical measures to detect security incidents affecting EIS. The organizational measures include the operating procedures of the detection devices and describe the chain of processing of the security events identified by these devices. The technical measures specify the nature and positioning of the detection devices.
3.1.1.2	**The operator implements detection devices capable of identifying events that are characteristic of a security incident, in particular a current or future attack, and enabling the search for traces of previous incidents.**	For this purpose, these devices: - collect relevant data on the operation of each EIS (including "network" data or "system" data) from sensors positioned to identify security events related to all data flows exchanged between them SIE and third-party information systems to those of the operator; - analyze the data from the sensors, notably by searching for known technical markers of attacks, in order to identify the security events and to characterize them; - archive the metadata of the events identified in order to allow a posteriori search of technical markers of attacks or compromise over a period of at least six months.
3.1.1.3	**In the particular case of an EIS necessary for the provision of peer interconnection service for the exchange of Internet traffic, the operator implements detection devices only for data streams other than those corresponding to traffic. internet proper.**	The operator or the service provider mandated for this purpose exploits the detection devices by relying on the requirements of the reference system for the detection of security incidents taken pursuant to Article 10 of Decree No. 2015-350 of 27 March 2015 amended relating to the qualification of security products and trust service providers for the needs of information systems security.
3.1.1.4	**In particular, the operator shall ensure that the installation and operation of the detection devices does not affect the safety and operation of its EIS.**	
3.1.2	*Logging*	Délai d'application : 1 an
3.1.2.1	**The essential services operator implements on each essential information system (EIS) a logging system that records the events relating to user authentication, account management and access rights, to the user. access to resources, changes to EIS security rules and the operation of the EIS.**	The logging system helps to detect security incidents by collecting log data. The logging system covers the following devices when they generate the events mentioned in the first paragraph: - application servers supporting essential services;- the system infrastructure servers; - network infrastructure servers;- security equipment;- engineering and maintenance positions in industrial systems;- network equipment;- administrative positions.
3.1.2.2	**The events recorded by the logging system are time stamped using synchronized time sources.**	They are, for each EIS, centralized and archived for a period of at least six months. The event archive format enables automated searches on these events.
3.1.3	*Logs Correlation and Analysis*	Délai d'application : 2 ans
3.1.3.1	**The essential services operator implements a log correlation and analysis system that exploits the events recorded by the logging system installed on each of the critical information systems (EIS), in order to detect events that are likely to occur. affect the security of EIS.**	The log correlation and analysis system helps to detect security incidents by analyzing log data.
3.1.3.2	**The log correlation and analysis system is installed and operated on an information system set up solely for the purpose of detecting events that could affect the security of the information systems.**	The operator or service provider appointed for this purpose installs and exploits this log correlation and analysis system based on the requirements of the repository for the detection of security incidents taken pursuant to Article 10 of the decree. n ° 2015-350 of the modified March 27th, 2015 relating to the qualification of the security products and the trusted service providers for the needs of the security of information systems.
3.2	**Computer Security Incident Management**	
3.2.1	*Information System Security Incident Response*	Délai d'application : 1 an
3.2.1.1	**The essential services operator develops, maintains and implements, in accordance with its network and information systems security policy, a procedure for handling security incidents affecting its essential information systems (EIS).**	The operator or the service provider appointed for this purpose proceeds with the handling of incidents based on the requirements of the reference system for responding to security incidents taken pursuant to Article 10 of Decree No. 2015-350 of 27 March 2015 amended on the qualification of security products and trusted service providers for the purpose of information systems security.

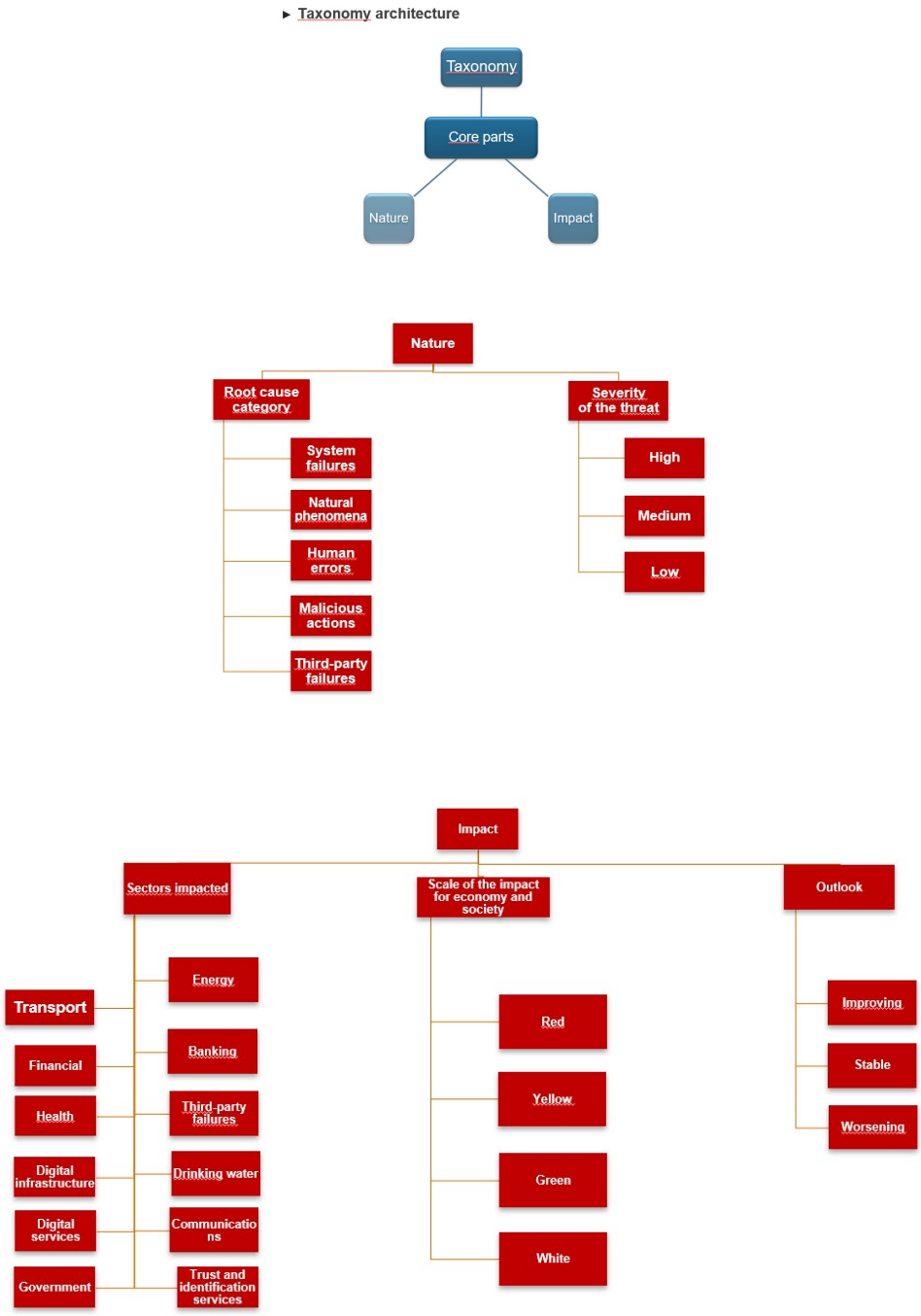
3.2.1.2	**A specific information system must be put in place to deal with incidents, in particular to store the technical records relating to the analysis of incidents.**	This system is partitioned vis-à-vis the EIS concerned by the incident.
3.2.1.3	**The operator keeps the technical records for the analysis of the incidents for a period of at least six months.**	He keeps these technical records at the disposal of the NCA/SPOC.
3.2.2	***Incident Report & Communication with NCA's and CSIRTs***	Délai d'application : 3 mois
3.2.2.1	**The essential services operator sets up a service enabling it to take cognizance, as soon as possible, of information transmitted by the NCA/SPOC relating to incidents, vulnerabilities and threats.**	
3.2.2.2	**It implements a procedure to process the information thus received and, where appropriate, to take the necessary security measures to protect its essential information systems (EIS).**	
3.2.2.3	**The operator communicates to the NCA/SPOC the coordinates (name of the service, telephone number and email address) kept up to date with the service provided for in the preceding paragraph.**	
4.	**Network & Information System Resilience**	
4.1	**Crisis Management Organisation and Process**	Délai d'application : 1 an
4.1.1	**The essential services operator develops, maintains and implements, in accordance with its network and information systems security policy, a crisis management procedure in the event of security incidents having a major impact on the services essential of the operator.**	This procedure describes the organization of crisis management set up by the operator and provides in particular for the application of the following technical measures to essential information systems (EIS):- configure the EIS to avoid attacks or limit the effects. This configuration can be used to:- to prohibit the use of removable storage media or the connection of nomadic equipment to EIS;- to install a security corrective measure on a particular EIS;- to restrict the routing;- implement filtering rules on networks or specific configurations on terminal equipment.This measure may be aimed at:- to make access restrictions in the form of whitelists and blacklists of users;- to block the exchange of files of a particular type;- to isolate from any network Internet sites, applications, or computer equipment of the operator;- Isolate the operator's EIS from the Internet. This measure requires physically or logically disconnecting the network interfaces of the concerned EIS.
4.1.2	**The procedure specifies the conditions under which these measures can be applied taking into account the technical and organizational constraints of implementation.**	
4.2	**Business Continuity Management**	French law : Mentionned in security policy but doesn't have a proper section
4.2.1	**Business continuity strategy implementation for the critical services provided by the organization**	Formally documented service continuity strategy, including recovery time objectives for key services and processes.
4.2.2	**Contingency plans implementation for the systems supporting essential services**	Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives.
4.2.3	**All personnel involvement in the continuity operations properly trained in their roles and responsibilities with regards to the information system**	Records of individual training activities as well as post-exercise reports.

4.3	**Disaster Recovery Management**	French law : Mentionned in security policy but doesn't have a proper section
4.3.1	**Organization preparness for recovery and restoration of the services affected by following disasters**	Measures in place for dealing with disasters, such as failover sites in other regions, backups of critical data to remote locations, etc.
4.3.2	**Policy in place along with related procedures for deploying disaster recovery capabilities**	Formally documented policy/procedures for deploying disaster recovery capabilities, including list of natural and/or major disasters that could affect the services, and a list of disaster recovery capabilities (either those available internally or provided by third par-ties).
4.3.3	**All personnel involvement in the disaster recovery operations**	Records of individual training activities.
5.	**Assessing of Cross-Sector & Cross-Border (inter)dependencies**	
5.1	**Indicators for Domain IMPACT**	
5.1.1	**System and application access controls provide indications of the potential number of users affected**	
5.1.2	**Operation security controls (e.g. malware controls, software restrictions, event logs, etc.) provide indications of the potential number of users affected**	
5.1.3	**The number of users informed and trained reduce drastically the number of users likely to be affected by an incident**	
5.1.4	**Security controls related to supplier relationships (including ICT supply chains) provide indications of the potential geographical distributions of incidents**	
5.1.5	**Geographical distribution as an indicator plays a role in identifying third - party stakeholders and ensure that they understand their roles and responsibilities.**	
5.1.6	**Geographical distribution as an indicator plays a role in identifying the entire workforce as well as third - party stakeholders and ensure that they understand their roles and responsibilities**	
5.1.7	**Geographical distribution as indicator is related to the establishment of critical functions and zones of dependencies for delivery of critical services**	
5.1.8	**Geographical distribution as indicator is related to the localisation and documentation of asset vulnerabilities**	
5.1.9	**Social impact is taken into account the potential impact of dependent and interdependent OES and DSPs on societal activities**	- Controls on Human Resource Security may also provide insights about the social impact of incidents - There may be a genuine link between social impact as indicator and the specific control, which consists in embedding cybersecurity in human resources practices
5.1.10	**Economic impact is taken into account the potential impact of dependent and interdependent OES and DSPs on economic activities**	- Controls on Supplier Relationships may also provide insights about the economic impact of incidents - Physical and information security personnel not being able to understand roles and responsibilities may result in major incident leading to a severe economic impact - No serious protection implementation against data leaks will more likely result in major incidents leading to an economic impact - The exercise of determining the impact of events is relevant in the sense that one of large effect may be economic - Reputation damage is more likely to be translated in economic impact
5.1.11	**Environmental impact is taken into account the potential impact of dependent and interdependent OES and DSPs on the environment**	- Physical and Environmental Security controls may also provide insights about the environmental impact of incidents - Mapping data flow may lead to the identification and localisation of environmental impact

5.2	**Indicators for Domain RELIABILITY, DEPENDABILITY AND RESILIENCE**	
5.2.1	**Controls related to "management of information security incidents and improvements"**	
5.2.2	**Controls related to "information security continuity"**	
5.2.3	**Redundancy controls**	
5.2.4	**Monitoring and review of supplier services**	
5.2.5	**Event logging**	
5.2.6	**Criticality of information**	
5.2.7	**Supplier controls**	
5.2.8	**Compliance controls**	
5.2.9	**Mean Downtime (MDT) after an incident in the offered service**	
5.2.10	**Redundancy of services (e.g. alternative services, etc.)**	This indicator takes into account various measures capturing the extent of redundancy related to dependencies and interdependencies of OES and DSPs
5.2.11	**Criticality of services in terms of security (i.e. availability, integrity and confidentiality)**	This indicator takes into account the security criticality of services (in terms of availability, integrity and confidentiality) in order to classify dependencies and interdependencies of OES and DSPs
5.3	**Indicators for Domain STRUCTURE**	
5.3.1	**Number of Service Level Agreements (SLAs) with third parties**	The number of SLAs may provide indications of the potential risks as well as structured aspects of dependent and interdependent OES and DSPs. - Service level agreements may provide information on the risks associated with incidents - Mapping data flow may lead to the identification and localisation of number of SLA
5.3.2	**Market share and structure (e.g. number of operators, number of alternative providers, multi-service market, monopoly, etc.)**	Market share and structure may provide indications of the potential risks as well as structured aspects of dependent and interdependent OES and DSPs. - Suppliers related controls may provide information about market share and structure, and the risks associated with incidents
5.3.3	**Suppliers related controls**	
5.3.4	**Information classification**	
5.3.5	**Access controls and policies**	
5.3.6	**Security requirements and specification**	
5.3.7	**Secure system engineering principles**	
5.3.8	**Mapping data flow**	
5.4	**Indicators for Domain TIME**	
5.4.1	**Seasonality of dependencies/interdependencies (e.g. variations of service levels over seasons)**	This indicator takes into account the risks associated with the seasonality (e.g. high demand of services during a particular time of the year) of dependent and interdependent OES and DSPs
5.4.2	**Temporal aspects of critical events (e.g. time criticality, time-critical dependencies, etc.)**	This indicator takes into account the temporal dimension of critical events (e.g. timeline, probabilistically independent and dependent events, etc.) associated with dependencies and interdependencies
5.4.3	**Dynamic aspects of dependencies/interdependencies (e.g. volatility, evolution, etc.)**	This indicator takes into account how dependencies and interdependencies of OES and DSPs interact in operations and evolve overtime

Appendix 5: Common taxonomy for cybersecurity incidents' notification

Source : *NIS Cooperation Group 04/2018 publication*



1. **Nature**
    - **Root cause category**, i.e. what triggered the incident, see Section 5.1:
        - System failures
        - Natural phenomena
        - Human errors
        - Malicious actions
        - Third-party failures
    - **Severity of the threat**, see Section 5.2:
        - High
        - Medium
        - Low
2. **Impact**
    - **Sectors impacted**, i.e. where services are impacted by the incident, see Section 6.1:
        - Energy
        - Transport
        - Banking
        - Finance
        - Health
        - Drinking water
        - Digital infrastructure
        - Communications
        - Trust and identification services
        - Digital services
        - Government services
    - **Scale of the impact**, nationally, for economy and society, see Section 6.2
        - Red – very large impact
        - Yellow – large impact
        - Green – minor impact
        - White – no impact
    - **Outlook**, i.e. the prognosis, regarding the impact, for economy and society:
        - Improving
        - Stable
        - Worsening

Appendix 6: Further elements to be considered by DSPs for managing the risks posed to the security of NIS (Article 2 §1 of Commission's implementing regulation (EU) 2018/151).

(Table made by author)

ARTICLE 16 NIS DIRECTIVE SECURITY MEASURES CATEGORIES	ELEMENTS TO BE TAKEN IN CONSIDERATION
SECURITY OF SYSTEMS AND FACILITIES;	(a) the systematic management of network and information systems, which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, security of operations, security architecture, secure data and system life cycle management and where applicable, encryption and its management; (b) physical and environmental security, which means the availability of a set of measures to protect the security of digital service providers' network and information systems from damage using an all-hazards risk-based approach, addressing for instance system failure, human error, malicious action or natural phenomena; (c) the security of supplies, which means the establishment and maintenance of appropriate policies in order to ensure the accessibility and where applicable the traceability of critical supplies used in the provision of the services; (d) the access controls to network and information systems, which means the availability of a set of measures to ensure that the physical and logical access to network and information systems, including administrative security of network and information systems, is authorised and restricted based on business and security requirements.
INCIDENT HANDLING;	(a) detection processes and procedures maintained and tested to ensure timely and adequate awareness of anomalous events; (b) processes and policies on reporting incidents and identifying weaknesses and vulnerabilities in their information systems; (c) a response in accordance with established procedures and reporting the results of the measure taken;

	(d) an assessment of the incident's severity, documenting knowledge from incident analysis and collection of relevant information which may serve as evidence and support a continuous improvement process.
BUSINESS CONTINUITY MANAGEMENT;	(a) the establishment and the use of contingency plans based on a business impact analysis for ensuring the continuity of the services provided by digital service providers which shall be assessed and tested on a regular basis for example, through exercises; (b) disaster recovery capabilities which shall be assessed and tested on a regular basis for example, through exercises.
MONITORING, AUDITING AND TESTING;	(a) the conducting of a planned sequence of observations or measurements to assess whether network and information systems are operating as intended; (b) inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, and efficiency and effectiveness targets are being met; (c) a process intended to reveal flaws in the security mechanisms of a network and information system that protect data and maintain functionality as intended. Such process shall include technical processes and personnel involved in the operation flow.
COMPLIANCE WITH INTERNATIONAL STANDARDS	Standards that are adopted by an international standardisation body as referred to in point (a) of Article 2(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council (2). Pursuant to Article 19 of Directive (EU) 2016/1148, European or internationally accepted standards and specifications relevant to the security of network and information systems, including existing national standards, may also be used.

Appendix 7: NCSS Analysis

(Table made by author)

		DE	FR	AU	PO	CZ	SL	HU	HR	SL	RO	BG	UK	SV	FI	EE	LV	LT	DK	MT	EL	CY	IT	ES	PT	BE	LU	NL
Objectives	Address cyber crime	x	x	x	x				x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Adopt Information Security Standards																	x										
	Balance security with privacy		x			x			x	x		x		x	x	x	x				x		x	x	x			
	Citizen's awareness	x	x		x	x	x			x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
	Critical Information Infrastructure Protection	x	x	x	x	x	x	x		x	x		x	x	x	x	x	x	x		x	x	x	x	x	x	x	x
	Develop national cyber contingency plans	x	x	x	x			x			x			x	x	x	x	x	x		x	x	x	x			x	
	Engage in international cooperation	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Establish a public-private partnership			x	x	x	x				x		x	x	x			x			x	x	x	x		x	x	x
	Establish an incident response capability	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x
	Establish an institutionalised form of cooperation between public agencies	x	x	x	x	x	x	x		x			x	x		x					x	x	x	x	x	x	x	
	Establish and implement policies and regulation capabilities																	x			x							
	Establish baseline security requirements	x	x	x	x		x	x	x		x		x		x	x	x	x	x		x		x	x	x		x	x
	Establish incident reporting mechanisms		x	x	x		x	x	x	x	x	x	x		x	x			x	x	x		x	x	x	x	x	
	Establish trusted information-sharing mechanisms																				x							
	Foster R&D	x	x	x	x	x	x		x		x	x	x	x	x	x		x	x		x		x	x	x	x		
	Organise cyber security exercises		x	x	x	x	x	x		x			x	x	x	x		x	x		x	x	x	x	x	x	x	
	Provide incentives for the private sector to invest in security measures														x								x	x				
	Risk assessment approach																	x			x							
	Set a clear governance structure																				x							
	Strengthen training and educational programmes		x	x	x		x	x		x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x

Appendix 8: National Competent Authorities for OES and DSPs by Member States

(Table made by author)

National Competent Authorities for OES							
	Digital Infrastructure	**Financial market infrastructure**	**Banking Sector**	**Transport Sector (Road, Rail, Water, Air)**	**Health Sector**	**Water supply and distribution sector**	**Energy (Oil, Gas, Electricity)**
Austria	GovCERT Austria						
Belgium	Centre for Cybersecurity Belgium						
Croatia	Central State Office for the Development of the Digital Society	Croatian Financial Services Supervisory Agency	Croatian National Bank	Ministry of the Sea, Transport and infrustructure	Ministry of Health	Ministry of Environment and Energy	
Czech Republic	National Cyber and Information Security Agency (NCISA)						
Cyprus	Digital Security Authority (DSA)						
Denmark		Danish Financial Supervisory Authority		1. The Danish Transport, Construction and Housing Authority 2. The Danish Maritime Authority	The Danish Health Data Authority	Ministry of Environment and Food	Danish Energy Agency
Estonia	Estonian Information System Authority						
Finland	National Cyber Security Centre, Finnish Transport and Communications Agency (Traficom)	Financial Supervisory Authority		Finnish Transport Safety Agency	National Supervisory Authority for Welfare and Health	Centre for Economic Development, Transport and the Environment	Energy Authority
France	National cyber-security agency ANSSI						
Germany	Federal Office for Information Security (BSI)						
Greece	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications and Media)						
Hungary	National Directorate General for Disaster Management						
Ireland	National Cyber Security Centre, Department of Communications, Climate Action & Environment						

Italy	Ministero dello Sviluppo Economico - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI)	Ministero dell'Economia e delle Finanze	Ministero dell'Economia e delle Finanze	Ministero delle Infrastrutture e dei Trasporti - Organo Centrale di Sicurezza	Ministero della Salute	Ministero dell'ambiente e della tutela del territorio e del mare	Ministero dello Sviluppo Economico - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI)
Lithuania	National Cyber Security Centre (NCSC/CERT-LT)						
Luxembourg		Commission de Surveillance du Secteur Financier		Institut Luxembourgeois de Régulation			
Latvia	Ministry of Transport	Financial and Capital Market Commission		Ministry of Transport	Ministry of Health	Ministry of Health (MoH) and the Ministry of Agriculture (MoA)	Ministry of Economics
Malta	Malta Critical Infrastructure Protection Unit (CIP)						
Netherlands	Agentschap Telecom	De Nederlandsche Bank (DNB)	De Nederlandsche Bank (DNB)		Inspectorate Healthcare and Youth	Ministry of Infrastructure and Water Management, Directorate-General Water and Soil	Agentschap Telecom
Poland	Ministry of Digital Affairs, Department of Cybersecurity	Polish Financial Supervision Authority	Minister of Finance	Minister of Maritime Economy and Inland Sailing	Minister of Health	Minister of the Environment	Minister of Energy
Portugal	Portuguese National Cybersecurity Centre						
Romania	Romanian National Computer Security Incident Response Team (CERT-RO)						
Slovakia	National Security Authority						
Slovenia	Information Security Administration						
Spain	Secretary of State for Digital Progress (for private sector) /Ministry of Defence, through the National Cryptologic Centre (for public sector)						
Sweden	Post- och telestyrelsen	Finansinspektionen		Swedish Transport Agency	Inspektionen för vård och omsorg	Livsmedelsverket	Swedish Energy Agency
UK	Office of Communications (OFCOM)	Incident notification: Financial Conduct Authority		Civil Aviation Authority (CAA), and Department for Transport	England - Department of Health and Social Care	England - Department for Environment, Food & Rural Affairs	England, Scotland and Wales - Department for Business, Energy & Industrial Strategy, and the Office of Gas and

						Electricity Markets
			England, Scotland and Wales - Department for Transport	Wales - Welsh Ministers	Wales - Welsh Ministers	England, Scotland and Wales - Department for Business, Energy & Industrial Strategy (BEIS), and Health & Safety Executive (HSE)
		Cross-border dependencies: Bank of England, Sector Resilience Team	Scotland - Scottish Ministers	Scotland - Scottish Ministers	Scotland - The Drinking Water Quality Regulator for Scotland	Northern Ireland - Department of Finance Northern Ireland
			Northern Ireland - Department of Finance Northern Ireland	**Northern Ireland - Department of Finance Northern Ireland**	**Northern Ireland - Department of Finance Northern Ireland**	

(Table made by author)

National Competent Authorities for DSP's	
Austria	GovCERT Austria
Belgium	Centre for Cybersecurity Belgium (CCB)
Croatia	Ministry of Economy, Entrepreneurship and Crafts
Czech Republic	National Cyber and Information Security Agency (NCISA)
Cyprus	Digital Security Authority (DSA)
Denmark	Danish Business Authority
Estonia	Estonian Information System Authority
Finland	National Cyber Security Centre, Finnish Transport and Communications Agency (Traficom)
France	National cyber-security agency ANSSI
Germany	Federal Office for Information Security (BSI)
Greece	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications and Media)
Hungary	National Cyber Security Centre
Ireland	National Cyber Security Centre, Department of Communications, Climate Action & Environment
Italy	Ministero dello Sviluppo Economico - Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCTI)
Latvia	Ministry of Transport
Lithuania	National Cyber Security Centre (NCSC/CERT-LT)
Luxembourg	Institut Luxembourgeois de Régulation
Malta	Malta Critical Infrastructure Protection Unit (CIP)
Netherlands	Agentschap Telecom
Poland	Ministry of Digital Affairs, Department of cybersecurity
Portugal	Romanian National Computer Security Incident Response Team (CERT-RO)
Romania	CERT-RO
Slovakia	National Security Authority
Slovenia	Information Security Administration
Spain	Secretary of State for Digital Progress (for private sector) /Ministry of Defence, through the National Cryptologic Centre (for public sector)
Sweden	Post- och telestyrelsen
United Kingdom	The Information Commissioner's Office (ICO).

Appendix 9: CSIRTs by Country

Source: *ENISA, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map*

Country	Full name	Constituency	CSIRTs Network	FIRST
Austria	ACOnet-CERT	NREN	Not member	Member
Austria	Austrian Energy CERT	CIIP	Member	Member
Austria	CERT.at	National	Member	Member
Austria	FREQUENTIS SIRT	Other commercial	Not member	Member
Austria	Government CERT Austria	Government	Member	Not member
Austria	Raiffeisen Informatik CERT	Financial	Not member	Member
Austria	WienCERT	Government	Not member	Not member
Austria	Military CERT Austria	Government, Private and Public sectors	Not member	Member
Austria	CERT der oesterreichischen Sparkassengruppe	Commercial Organisation, Financial Sector, ISP Customer Base	Not member	Not member
Belgium	BELNET CERT	NREN	Not member	Member
Belgium	CERT.be	CIIP, Government, National	Member	Member
Belgium	KBC Group CERT	Financial	Not member	Member
Belgium	NVISO Cyber Security Incident Response Team	Commercial Organisation, Service Provider Customer Base	Not member	Not member
Belgium	Proximus CSIRT (formerly BGC-CSIRT)	Commercial Organisation, ISP Customer Base	Not member	Member
Belgium	XMConsulting-CSIRT	ICT Vendor Customer Base	Not member	Not member
Bulgaria	CERT Bulgaria	Government	Member	Not member
Croatia	CERT Zavoda za Sigurnost Informacijskih Sustava	Government	Member	Member
Croatia	Croatian National CERT	NREN, National	Member	Member
Cyprus	National CSIRT-CY	CIIP, Government, National	Member	Member
Czech Republic	2 connect CSIRT	ISP Customer Base, Service Provider Customer Base	Not member	Not member
Czech Republic	ACTIVE24-CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	CSIRT ALEF NULA a.s.	Commercial Organisation, Service Provider Customer Base	Not member	Member
Czech Republic	AXENTA CSIRT	Service Provider Customer Base	Not member	Not member
Czech Republic	Accenture Cyber Fusion Center	Government, Private and Public Sectors	Not member	Member
Czech Republic	CASABLANCA.CZ-CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	Cyber Defense Center AEC	Service Provider Customer Base	Not member	Not member
Czech Republic	CDT-CERT	ISP Customer Base	Not member	Not member
Czech Republic	CESNET-CERTS	NREN	Not member	Not member
Czech Republic	CETIN CSIRT TEAM (formerly CETIN)	ISP Customer Base	Not member	Not member
Czech Republic	CRA CSIRT (formerly CRa CSIRT)	Commercial Organisation, ISP Customer Base	Not member	Not member

Czech Republic	ComSource CSIRT	Commercial Organisation, Service Provider Customer Base	Not member	Not member
Czech Republic	CSIRT CSAS	Financial	Not member	Not member
Czech Republic	CSIRT Merit Group a.s.	ISP Customer Base	Not member	Not member
Czech Republic	CSIRT of the University of Ostrava	NREN	Not member	Not member
Czech Republic	CSIRT EDERA Group a.s.	Commercial Organisation, ISP Customer Base	Not member	Not member
Czech Republic	CSIRT of Masaryk University	NREN	Not member	Not member
Czech Republic	CSIRT-NETX	Commercial Organisation	Not member	Not member
Czech Republic	CSIRT-SPCSS	Government	Not member	Not member
Czech Republic	CSIRT-VUT	NREN	Not member	Not member
Czech Republic	CSIRT.CZ	Government, National, Private and Public Sectors	Member	Member
Czech Republic	CSOB-Group-CSIRT	Financial	Not member	Not member
Czech Republic	CZ.NIC-CSIRT	Non-Commercial Organisation	Not member	Not member
Czech Republic	Coolhousing.net - CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	Dial Telecom CERT Team	ISP Customer Base	Not member	Not member
Czech Republic	Dial Telecom CSIRT Team	ISP Customer Base	Not member	Member
Czech Republic	ELAT CSIRT	ICT Vendor Customer Base	Not member	Not member
Czech Republic	FORPSI-CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	GovCERT.CZ	Government, Private and Public Sectors	Member	Member
Czech Republic	INTERNEXT CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	ISP ALLIANCE.CZ-CSIRT (formerly ISPA-CSIRT)	ISP Customer Base	Not member	Not member
Czech Republic	Kaora s.r.o. CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	KBM CSIRT	Commercial Organisation, Government, ISP Customer Base, Non-Commercial Organisation, Research & Education	Not member	Not member
Czech Republic	KERNUN CSIRT	Commercial Organisation, Service Provider Customer Base, Vendor Customer Base	Not member	Not member
Czech Republic	MASTER.CZ-CSIRT	Commercial Organisation, ISP Customer Base	Not member	Not member
Czech Republic	NETBOX CSIRT Team	ISP Customer Base	Not member	Not member
Czech Republic	NIX.CZ-CSIRT	Non-Commercial Organisation	Not member	Not member
Czech Republic	O2 Czech Republic CERT	ISP Customer Base	Not member	Not member
Czech Republic	ITSELF.CZ-CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	SEZNAM.CZ-CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	SOC-Corpus Solutions a.s.	Commercial Organisation	Not member	Not member

Czech Republic	Security Operation center 365 CSIRT	Private and Public Sectors	Not member	Not member
Czech Republic	SOC ANECT	Commercial Organisation, ISP Customer Base, Service Provider Customer Base	Not member	Not member
Czech Republic	SPCSS-CSIRT TEAM	ISP Customer Base	Not member	Not member
Czech Republic	T-Mobile Czech CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	CSIRT TELCO PRO SERVICES a.s.	ISP Customer Base	Not member	Not member
Czech Republic	TOTAL SERVICE CSIRT	Commercial Organisation, Service Provider Customer Base	Not member	Not member
Czech Republic	CSIRT VSHosting s.r.o	Commercial Organisation, ISP Customer Base	Not member	Not member
Czech Republic	WEB4U-CSIRT	ISP Customer Base	Not member	Not member
Czech Republic	WIA spol. s r.o. CSIRT	Commercial Organisation, ISP Customer Base, Service Provider Customer Base	Not member	Not member
Czech Republic	ha-vel CSIRT	Commercial Organisation, ISP Customer Base, Service Provider Customer Base	Not member	Not member
Denmark	Centre for Cyber Security (formerly Danish GovCERT)	Government, National	Member	Member
Denmark	CSIS.DK	Commercial Organisation	Not member	Not member
Denmark	Danish CERT	NREN	Not member	Member
Denmark	Ezenta	Service Provider Customer Base	Not member	Not member
Denmark	JN Data Cyber Defense Center	Financial	Not member	Not member
Denmark	KMD-CERT (formerly KMD IAC)	ISP Customer Base	Not member	Member
Denmark	NetsCERT	Financial	Not member	Not member
Denmark	Orsted SAC	Other commercial	Not member	Member
Denmark	SWAT	Commercial Organisation	Not member	Not member
Denmark	Secunia Research	Commercial Organisation, Vendor Customer Base	Not member	Member
Denmark	TDC Security Operations Center	ISP Customer Base	Not member	Member
Estonia	CERT Estonia	CIIP, Financial, Government, National	Member	Member
Estonia	Estonian Defence Forces Cyber Incident Response Capability	Government, Military	Not member	Member
Europe	Airbus CERT	CIIP, Commercial Organisation	Not member	Member
Europe	EC DIGIT CSIRC	Government	Not member	Member
Europe	NORDUnet CERT	NREN	Not member	Member
European Union	CERT-EU	EU Institutions	Member	Member
Finland	Ericsson Product Security Incident Response Team	Vendor Customer Base	Not member	Member
Finland	F-Secure Security Response	Commercial Organisation	Not member	Not member
Finland	Funet CERT	NREN	Not member	Member
Finland	National Cyber Security Centre Finland	CIIP, Government, National	Member	Member
France	AXA Global Security Incident Response Team	Commercial Organisation, Financial	Not member	Member
France	Alliacom Computer Emergency Response Team	Commercial Organisation, Service Provider Customer Base	Not member	Member
France	CERT CYBERPROTECT	Commercial Organisation	Not member	Member
France	CERT Credit Agricole (CERT-AG)	Financial	Not member	Member

France	CERT ESEC SOGETI / CAPGEMINI	Commercial Organisation, Service Provider Customer Base	Not member	Not member
France	CERT Groupe BPCE	Financial	Not member	Not member
France	Computer Emergency Response Team - La Poste	Commercial Organisation, Financial	Not member	Not member
France	CERT Michelin	Commercial Organisation	Not member	Not member
France	CERT OSIRIS	NREN	Not member	Not member
France	CERT Orange Cyberdefense	ICT Vendor Customer Base	Not member	Member
France	SEKOIA Computer Emergency Response Team	Commercial Organisation, Service Provider Customer Base	Not member	Not member
France	CERT-Societe Generale	Financial	Not member	Member
France	CERT Credit Agricole	Financial sector	Not member	Member
France	CERT-AKAOMA	Commercial Organisation, NREN, Service Provider Customer Base	Not member	Not member
France	CERT Banque de France	Financial	Not member	Member
France	CERT Caisse des Depots	Financial	Not member	Not member
France	CERT-Conix	Service Provider Customer Base	Not member	Not member
France	CERT digital.security	Commercial Organisation, Service Provider Customer Base	Not member	Not member
France	CERT-DEVOTEAM (formerly APOGEE SecWatch)	Service Provider Customer Base	Not member	Not member
France	CERT-FR	CIIP, Government	Member	Member
France	CERT-Intrinsec	Commercial Organisation	Not member	Not member
France	CERT-LEXSI	Service Provider Customer Base	Not member	Member
France	Renater CERT / Le CERT Renater	NREN	Not member	Member
France	CERT-SNCF	Commercial Organisation	Not member	Not member
France	CERT-UBIK	Commercial Organisation, Service Provider Customer Base	Not member	Not member
France	CERT-Wavestone (formerly CERT-SLC)	Commercial Organisation, Service Provider Customer Base	Not member	Not member
France	CERT-XMCO	Service Provider Customer Base	Not member	Not member
France	Centre Operationnel de Securite RTE	CIIP, Commercial Organisation	Not member	Not member
France	Corporate Security Incident Response Team BNP Paribas	Financial	Not member	Member
France	CSIRT-POLICE JUDICIAIRE	Government	Not member	Not member
France	Cert-IST	Service Provider Customer Base	Not member	Member
France	CERT La Poste	Other commercial	Not member	Member
France	FRANCE MILITARY CERT	Government & military	Not member	Member
France	Naval Group CERT	Non-Commercial Organisation, Vendor Customer Base	Not member	Not member
France	Orange-CERT Coordination Center	Commercial Organisation	Not member	Member
France	Securite Operationnelle SI	Commercial Organisation	Not member	Not member
France	STMicroelectronics Corporate SIRT	Commercial Organisation, Vendor Customer Base	Not member	Not member
Germany	Airbus CyberSecurity and CSIRT	Commercial Organisation	Not member	Member
Germany	Global BASF CERT	Commercial Organisation	Not member	Member

Germany	BFK edv consulting	Commercial Organisation	Not member	Member
Germany	BMW Group CSIRT	Other commercial	Not member	Member
Germany	Bayern-CERT	Government	Not member	Not member
Germany	Bosch CERT and PSIRT	Commercial Organisation	Not member	Not member
Germany	CERT BWI	Military	Not member	Member
Germany	CERT Nordrhein-Westfalen	Government	Not member	Not member
Germany	CERT der Bundesagentur fÃ¼r Arbeit	Government, Private and Public sectors	Not member	Member
Germany	CERT-BPOL	Law Enforcement	Not member	Not member
Germany	CERT-Bund	CIIP, Government, National	Member	Member
Germany	CERT-VW	Commercial Organisation	Not member	Member
Germany	CERT Rheinland-Pfalz	Government	Not member	Not member
Germany	CERT@VDE	NREN, Non-Commercial Organisation	Not member	Not member
Germany	Computer Emergency Response Team Bundeswehr	Military	Not member	Member
Germany	innogy SE Cyber Security Analysis and Incident Response	CIIP	Not member	Member
Germany	CSIRT - European Central Bank	Financial	Not member	Member
Germany	innogy SE Cyber Security Analysis & Incident Response	Industrial sector	Not member	Member
Germany	Commerzbank CERT	Financial	Not member	Member
Germany	Crytek CERT	Commercial Organisation, Vendor Customer Base	Not member	Not member
Germany	Deutsche Bahn CSIRT	Commercial Organisation	Not member	Member
Germany	DFN-CERT	NREN	Not member	Member
Germany	Deutsche Bank Cyber Threat Response Team	Financial	Not member	Member
Germany	Deutsche Telekom Group CERT	ISP Customer Base	Not member	Member
Germany	E.ON Cyber Emergency Response Team	Commercial Organisation	Not member	Member
Germany	Evonik CERT	Commercial Organisation	Not member	Member
Germany	CERT of Fujitsu Technology Solutions	Commercial Organisation	Not member	Member
Germany	IHK-CERT	Service Provider Customer Base	Not member	Not member
Germany	Infineon Cyber Defense Center	Commercial Organisation	Not member	Member
Germany	Karlsruhe Institute of Technology CERT	NREN	Not member	Member
Germany	Lufthansa Group CERT	Commercial Organisation	Not member	Member
Germany	Oneconsult International CERT	Service Provider Customer Base	Not member	Member
Germany	PRESECURE Computer Emergency Response Team	Service Provider Customer Base	Not member	Member
Germany	Stabsstelle DV-Sicherheit der Universitaet Stuttgart (RUS-CERT)	NREN	Not member	Member
Germany	Computer Notfallteam der Sparkassen-Finanzgruppe	Financial	Not member	Member
Germany	SAP Cybersecurity (formerly SAP CERT)	Vendor Customer Base	Not member	Member
Germany	Siemens CERT	Commercial Organisation	Not member	Member
Germany	ThyssenKrupp CERT	Service Provider Customer Base	Not member	Member

Germany	CERT@VDE	Commercial Organisation, Service Provider Customer Base	Not member	Not member
Germany	Vodafone Global Security Operations Centre	Commercial Organisation, ISP Customer Base	Not member	Member
Germany	CERT der Universitaet Muenster	NREN	Not member	Not member
Germany	XING Security Team	Commercial Organisation	Not member	Not member
Germany	adidas Cyber Security Incident Response Team	Other commercial	Not member	Member
Germany	civitec CERT	Government	Not member	Not member
Germany	dCERT Computer Emergency Response Team	Service Provider Customer Base	Not member	Member
Germany	gematik CERT der Telematikinfrastruktur	CIIP	Not member	Not member
Germany	SECUNET CERT	Service Provider Customer Base	Not member	Member
Greece	Aristotle University of Thessaloniki CERT	NREN	Not member	Not member
Greece	FORTHcert	Service Provider Customer Base	Not member	Member
Greece	Hellenic Cyber Security Incident Response Team	Government	Member	Not member
Greece	GRNET-CERT	NREN	Not member	Not member
Greece	Greek National Authority Against Electronic Attacks	Government	Not member	Not member
Hungary	Hungarian Research and Educational CSIRT	Research & Education	Not member	Not member
Hungary	HUN-CERT	Service Provider Customer Base	Not member	Not member
Hungary	National Cyber Security Center of Hungary	CIIP, Energy, Government, ISP Customer Base, National	Member	Member
Ireland	National Cyber Security Centre (IE) (formerly NCSC (IE))	Government, National	Member	Member
Ireland	HEANET-CERT	NREN	Not member	Not member
Ireland	Irish Reporting and Information Security Service CERT	Non-Commercial Organisation	Not member	Not member
Italy	D3Lab CERT Team	Commercial Organisation	Not member	Not member
Italy	CERT-Difesa	Military	Not member	Not member
Italy	CERT-ENAV	CIIP, Commercial Organisation	Not member	Member
Italy	CERT Pirelli	Commercial Organisation	Not member	Not member
Italy	CERT Pubblica Amministrazione	Government	Not member	Not member
Italy	CERT-RAFVG	Local Agencies	Not member	Not member
Italy	CERT Banca d'Italia	Financial	Not member	Not member
Italy	CERTEGO Incident Response Team	Commercial Organisation	Not member	Member
Italy	CERT Finanziario Italiano	Financial	Not member	Not member
Italy	D3Lab CERT Team	Commercial Organisation	Not member	Not member
Italy	Enel CERT - Cyber Emergency Readiness Team	Energy	Not member	Member
Italy	GARR-CERT. - Servizio sicurezza rete GARR	NREN	Not member	Not member

Italy	Grimaldi Computer Security Incident Response Team	Commercial Organisation	Not member	Not member
Italy	Intesa Sanpaolo CERT - Computer Emergency Readiness Team	Financial sector	Not member	Member
Italy	CERT Nazionale Italia	Government, National	Member	Not member
Italy	Leonardo Computer Emergency Response Team	CIIP	Not member	Member
Italy	CERT Poste Italiane	Commercial Organisation, Financial, Government	Not member	Member
Italy	SIA CERT	Financial	Not member	Not member
Italy	GSE Security Operation Center	Government	Not member	Not member
Italy	Computer Emergency Readiness Team - Terna	CIIP	Not member	Member
Italy	TS-WAY Cyber Intelligence Operation Center	Service Provider Customer Base	Not member	Not member
Italy	Yarix Computer Emergency Response Team	Commercial Organisation, Service Provider Customer Base	Not member	Member
Italy	YOROI-CSDC	Commercial Organisation	Not member	Not member
Latvia	CERT.LV	Government, National	Member	Member
Lithuania	National Cert of Lithuania - CERT-LT	National	Member	Member
Lithuania	The Core Center of State Telecommunications CERT	Government	Not member	Not member
Lithuania	LITNET CERT (formerly LITNET NOC-CERT)	NREN	Not member	Member
Lithuania	Lithuanian National Cyber Security Center	Government, Military	Not member	Member
Lithuania	NRD CIRT	Commercial Organisation	Not member	Member
Lithuania	Secure State Data Communication Network - CERT	Government	Not member	Not member
Lithuania	TEO-CERT	ISP Customer Base	Not member	Member
Luxembourg	CERT-EBRC	Commercial Organisation, Financial	Not member	Not member
Luxembourg	Excellium CSIRT	Commercial Organisation	Not member	Not member
Luxembourg	Computer Incident Response Center Luxembourg	National	Member	Member
Luxembourg	Computer Security Research and Reponse Team	NREN	Not member	Not member
Luxembourg	Clearstream - Deutsche Boerse CERT	Financial	Not member	Not member
Luxembourg	Governmental CERT of Luxembourg	CIIP, Government, Law Enforcement, Military, National	Member	Member
Luxembourg	HealthNet-CSIRT (formerly HealthNet)	Government	Not member	Not member
Luxembourg	Malware.lu CERT	Service Provider Customer Base	Not member	Not member
Luxembourg	CERT national Luxembourg	National	Member	Not member
Luxembourg	RESTENA Computer Security Incident Response Team	NREN	Not member	Not member
Luxembourg	Telindus Cyber Security Incident Response Team	Commercial Organisation, ISP Customer Base	Not member	Not member
Malta	AFM Communication Information System	Military	Not member	Not member
Malta	CSIRTMalta	National	Member	Not member

Malta	MITA Computer Security Incident Response Team	Government	Not member	Member
Netherlands	NN-GROUP CSIRT	Commercial Organisation, Financial Sector	Not member	Not member
Netherlands	Rabobank Group CSIRT	Financial sector	Not member	Member
Netherlands	SIDN Computer Security Incident Response Team		Not member	Member
Netherlands (The)	ABN AMRO Global CIRT	Financial	Not member	Member
Netherlands (The)	AMC-CERT	NREN	Not member	Not member
Netherlands (The)	CERT Radboud Universiteit (formerly CERT-KUN)	NREN	Not member	Not member
Netherlands (The)	CERT-RUG Security Kernel Group	NREN	Not member	Not member
Netherlands (The)	CERT-UU	NREN	Not member	Not member
Netherlands (The)	University of Amsterdam CERT (formerly UvA-CERT)	NREN	Not member	Not member
Netherlands (The)	CERT-WaterManagement	Government	Not member	Not member
Netherlands (The)	CSIRT-DSP	National	Member	Not member
Netherlands (The)	Defensie Computer Emergency Response Team	Military	Not member	Member
Netherlands (The)	Edutel Security Team	Commercial Organisation, ISP Customer Base	Not member	Not member
Netherlands (The)	Fox-IT CERT	Commercial Organisation	Not member	Not member
Netherlands (The)	Informatiebeveiligingsdienst voor gemeenten	Government	Not member	Not member
Netherlands (The)	ING CCERT	Financial	Not member	Member
Netherlands (The)	Computer Emergency Response Team of KPN	ISP Customer Base	Not member	Member
Netherlands (The)	Nationaal Cyber Security Centrum	National	Member	Member
Netherlands (The)	Nikhef CSIRT	Private and Public Sectors	Not member	Not member
Netherlands (The)	PGGM-CERT	Financial, Non-Commercial Organisation	Not member	Not member
Netherlands (The)	RIPE Network Coordination Centre CSIRT	Non-Commercial Organisation	Not member	Not member
Netherlands (The)	Rabobank Group CSIRT	Financial	Not member	Member
Netherlands (The)	SIDN Computer Security Incident Response Team	Service Provider Customer Base	Not member	Member
Netherlands (The)	Security Incident Response Team NS	CIIP, Commercial Organisation	Not member	Not member
Netherlands (The)	SURFcert (formerly SURFnet-CERT)	NREN	Not member	Member
Netherlands (The)	Z-CERT	Non-Commercial Organisation	Not member	Not member
Poland	CERT ALLEGRO	Commercial Organisation	Not member	Not member
Poland	CERT Alior	Financial	Not member	Not member
Poland	Computer Emergency Response Team BIK	Financial	Not member	Not member
Poland	Computer Emergency Response Team ENEA	CIIP	Not member	Not member

Poland	Computer Emergency Response Team Energa	CIIP	Not member	Not member
Poland	CERT Orange Polska	ISP Customer Base	Not member	Member
Poland	CERT PKO Bank Polski	Commercial Organisation, Financial	Not member	Member
Poland	CERT POLSKA	NREN, National	Member	Member
Poland	CERT PSE	Private and Public Sectors	Not member	Member
Poland	CERT T-Mobile Polska	ISP Customer Base	Not member	Not member
Poland	CERT mBank	Financial	Not member	Not member
Poland	CERT.GOV.PL	Government	Not member	Not member
Poland	CERT ALLEGRO	Commercial Organisation	Not member	Not member
Poland	CSIRT-GOV	Government, National	Member	Not member
Poland	CSIRT-MON	Military	Member	Not member
Poland	ComCERT.PL	Commercial Organisation, Financial	Not member	Not member
Poland	Exatel CERT	Private and Public Sectors	Not member	Not member
Poland	Polish Financial CERT	Financial Sector	Not member	Not member
Poland	GAZ-SYSTEM CERT	CIIP	Not member	Not member
Poland	PGE-CERT	Government, Private and Public Sectors	Not member	Member
Poland	CSIRT of Pol34/155 National Network	NREN	Not member	Not member
Poland	Soc24 Sp. z o.o.	Service Provider Customer Base	Not member	Not member
Poland	StillSec iSOC	Commercial Organisation	Not member	Not member
Portugal	CERT.PT	Government, National	Member	Member
Portugal	CSIRT Vodafone Portugal	ISP Customer Base	Not member	Not member
Portugal	CSIRT University of Porto (formerly CSIRT.FEUP)	NREN	Not member	Not member
Portugal	Dognaedis Incident Response Team (formerly CERT-IPN)	Commercial Organisation, ISP Customer Base, Service Provider Customer Base, Vendor Customer Base	Not member	Not member
Portugal	Euronext Computer Security Incident	Financial	Not member	Not member
Portugal	RCTS CERT	NREN	Not member	Member
Portugal	CSIRT Portugal Telecom	ISP Customer Base	Not member	Not member
Romania	Amgen Cyber Security Incident Response Team	Government, Private and Public Sectors	Not member	Member
Romania	CERT-RO	National	Member	Member
Romania	CORIS-STS	Government	Not member	Not member
Romania	Agency ARNIEC/RoEduNet CSIRT	NREN	Not member	Member
Romania	Safetech Computer Emergency Response Team	Commercial Organisation, Service Provider Customer Base	Not member	Not member
Romania	UTI Computer Emergency Response Team	Commercial Organisation	Not member	Not member
Slovakia	ANTIK CSIRT	Commercial Organisation, ISP Customer Base, Service Provider Customer Base	Not member	Not member
Slovakia	Beset-Cirt	ICT Vendor Customer Base	Not member	Not member

Slovakia	Binary Confidence Cyber Defense Center	Commercial Organisation, ISP Customer Base, Service Provider Customer Base	Not member	Not member
Slovakia	CSIR of Pavol Jozef Safarik University in Kosice	NREN	Not member	Not member
Slovakia	Military CSIRT Slovakia	CIIP, Law Enforcement, Military	Not member	Not member
Slovakia	CSIRT Slovakia (formerly CERT-SK)	Government	Member	Member
Slovakia	GOV CERT SK	Government, Non-Commercial Organisation, Service Provider Customer Base	Not member	Not member
Slovakia	SK-CERT (formerly GovCERT-SK)	CIIP, National	Member	Member
Slovakia	VNET CSIRT	ISP Customer Base	Not member	Not member
Slovakia	VOID SOC	Commercial Organisation, Service Provider Customer Base	Not member	Not member
Slovenia	Slovenian Computer Emergency Response Team	NREN, National	Member	Member
Slovenia	Slovenian Governmental CERT	Government	Not member	Not member
Spain	Ackcent CERT	ICT vendor customer base	Not member	Member
Spain	Centro de Seguridad TIC de Andalucia	Government	Not member	Not member
Spain	BBVA CERT	Financial	Not member	Member
Spain	Basque Cybersecurity Centre	Government, Non-Commercial Organisation	Not member	Member
Spain	Agencia Catalana de Ciberseguretat	Government, Private and Public sectors	Not member	Member
Spain	Spanish Governmental National Cryptology Center - CSIRT	Government	Member	Member
Spain	CERT OESÃ	Government, Private and Public sectors	Not member	Member
Spain	Aiuken Cybersecurity	Other commercial	Not member	Member
Spain	CERT-UAM	NREN	Not member	Not member
Spain	CERT-UC3M	NREN	Not member	Not member
Spain	Centre de Seguretat de la Informacio de Catalunya	Government	Not member	Member
Spain	CSA Equipo de Seguridad	Government, Private and Public Sectors	Not member	Member
Spain	CSIRT INDITEX	Commercial Organisation	Not member	Not member
Spain	Centro de Seguridad TIC de la Comunitat Valenciana	Government & military	Not member	Member
Spain	CSIRT.gal	Government	Not member	Not member
Spain	Centre de Seguretat TIC de la Comunitat Valenciana	Government	Not member	Not member
Spain	CSUC-CSIRT (formerly CESCA-CSIRT)	NREN	Not member	Not member
Spain	CAIXABANK TEAM CSIRT	Financial sector	Not member	Member
Spain	Caixabank CSIRT (formerly e-LC CSIRT)	Financial	Not member	Member
Spain	Ciber Security Operation Center	Service Provider Customer Base	Not member	Member
Spain	Cipher CERT	ISP customer base	Not member	Member
Spain	DXC Technology Iberia CSIRT	Service Provider Customer Base	Not member	Member
Spain	Deloitte EDC	Commercial Organisation, Service Provider Customer Base, Vendor Customer Base	Not member	Member
Spain	ENTELGY-CSIRT InnoTec System	Commercial Organisation, Service Provider Customer Base	Not member	Member
Spain	Equipo de Respuesta a Incidentes - Sothis	Commercial Organisation	Not member	Member

Spain	ESP DEF CERT	Military	Not member	Member
Spain	EULEN Seguridad-CCSI-CERT	ICT vendor customer base	Not member	Member
Spain	Grupo ICA CiberSOC	Industrial sector	Not member	Member
Spain	IBERDROLA Cyber-Security Incident Response Team	Service Provider Customer Base	Not member	Member
Spain	ICA Sistemas y Seguridad CiberSOC	Industrial sector	Not member	Member
Spain	INCIBE-CERT	CIIP, National	Member	Member
Spain	ITS Industrial Cybersecurity CERT	Commercial Organisation	Not member	Member
Spain	CSIRT INDITEX	Commercial Organisation	Not member	Not member
Spain	MAPFRE-CCG-CERT	Financial	Not member	Member
Spain	Minsait CSIRT	Private and Public Sectors	Not member	Member
Spain	NUNSYS-CERT	Private and Public Sectors	Not member	Not member
Spain	NestlÃ© Cyber Security Operations Center	Other commercial	Not member	Member
Spain	PROSEGUR CERT	ISP Customer Base	Not member	Member
Spain	RENFE-Operadora	Other commercial	Not member	Member
Spain	REPSOL CERT	Industrial sector	Not member	Member
Spain	RedIRIS	NREN	Not member	Member
Spain	S2 Grupo CERT	Service Provider Customer Base	Not member	Member
Spain	S21sec CERT	Service Provider Customer Base	Not member	Member
Spain	SIA-CEC CERT	ICT vendor customer base	Not member	Member
Spain	Santander Global CERT	Financial sector	Not member	Member
Spain	Telefonica CSIRT	Commercial Organisation, ISP Customer Base	Not member	Member
Spain	Telefonica CSIRT	Other commercial	Not member	Member
Spain	Versia-CSIRT	Government, Private and Public sectors	Not member	Member
Spain	eSOC Ingenia	ICT vendor customer base	Not member	Member
Spain	CERT of the Polytechnic University of Catalonia	NREN	Not member	Member
Spain	everis CERT	Other commercial	Not member	Member
Sweden	2Secure CSIRT	Service Provider Customer Base	Not member	Not member
Sweden	Baffin Bay Networks SIRT	ISP Customer Base, Service Provider Customer Base, Vendor Customer Base	Not member	Not member
Sweden	Basefarm SIRT	Commercial Organisation, Service Provider Customer Base	Not member	Member
Sweden	CERT-SE (formerly SITIC)	Government, National	Member	Member
Sweden	Swedish Armed Forces CERT	Military	Not member	Member
Sweden	Handelsbanken SIRT	Financial	Not member	Member
Sweden	Linkoping University Incident Response Team	NREN	Not member	Member
Sweden	Region Stockholm CERT	Government, Private and Public Sectors	Not member	Member
Sweden	SBAB-SIRT	Financial	Not member	Not member
Sweden	SEB Computer Security Incident Response Team	Financial	Not member	Not member
Sweden	Swedish National Infrastructure for Computing IT Security Team	NREN	Not member	Not member
Sweden	SUNet CERT	NREN	Not member	Member
Sweden	Swedbank Security Incident Response Team	Financial	Not member	Not member

Sweden	Telia Company CERT (formerly TS-CERT)	Commercial Organisation, ISP Customer Base, Service Provider Customer Base	Not member	Member
Sweden	Uppsala University CSIRT	NREN	Not member	Not member
Sweden	Umea University Incident Response Team	NREN	Not member	Not member

Appendix 10: Identified essential services by Finland

(Table made by author)

Energy[1]	Electricity	Transmission system operators
	Gas	Transmission system operators
Transport	Air Transport[2]	Airport managing bodies
		Traffic management control operators providing air traffic control (ATC)
	Rail Transport	Infrastructure managers
		Traffic management services
	Water Transport[3]	Managing bodies of port
		Operators of vessel traffic services
	Road transport	Operators of Intelligent Transport Systems
Banking		Credit institutions
Financial market infrastructures[4]		Operators of trading venues
Health sector		The state and municipal authority and any other body governed by public law, the Social Insurance Institution, the Finnish Centre for Pensions, the Patient Injury Board, the Pension Foundation and other pension providers, the insurance institution, the body, or institution engaged in maintenance or medical activities, the producer of private social services and the pharmacy.
Drinking water supply and distribution		Water supply company that supplies water or receives at least 5,000 cubic meters of wastewater per day.[5]
Digital infrastructure[6]		TLD name registries

Appendix 11: Identified essential services by France

(Table made by author)

[1] In the oil sector, OES have not been identified in accordance with the criteria set out in the Directive.

[2] Government Decree of May 9th, 2018 on airports and ports relevant to the functioning of society: Airports and ports included in the EU TEN-T transport network are defined in Annex II to Regulation (EU) No 1315/2013 on Union guidelines for the development of the trans-European transport network. Available at https://valtioneuvosto.fi/delegate/file/40914, accessed on March 23rd, 2021.

[3] *Ibid*

[4] There is no Central counterparties (CCPs) in Finland.

[5] There are approximately 40 such plants in Finland.

[6] Information gathered from the 'Report from The Commission To The European Parliament And The Council assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148 on security of network and information systems, Brussels, 28.10.2019, COM(2019) 546 final.

Sector	Subsector	Type of Entity
Energy	Electricity	Electricity undertakings
		Distribution system operators
		Transmission system operators
	Oil	Operators of oil transmission pipelines
		Operators of oil production, refining and treatment facilities, storage, and transmission
		Operators of digital logistics data transfer platforms
	Gas	Supply undertakings
		Distribution system operators
		Transmission system operators
		Storage system operators
		LNG system operators
		Natural gas undertakings
		Operators of natural gas refining and treatment facilities
Transport	Air Transport	Air carriers
		Airport managing bodies and entities operating ancillary installations contained within airports
		Traffic management control operators
		Aircraft maintenance companies
		Operators of passenger flow management systems
	Rail Transport	Infrastructure managers
		Infrastructure maintenance companies
		Railway undertakings
		Rails' equipment maintenance companies
	Guided Transport	Companies of guided transport
	Water Transport	Inland, sea and coastal passenger and freight water transport companies
		Vessels maintenance companies
		Water transport infrastructure operating companies
		Managing bodies of ports including their port facilities
		Operators of vessel traffic services
		Operators of fluvial traffic services
	Road transport	Road authorities responsible for traffic management control
		Road infrastructure operation and management companies
		Operators of Intelligent Transport Systems
		Freight transport companies
		Collective road transport companies
	Freight transport	Organization of transport operators
		Charter carriers operators
Logistics		Logistics platform managers
Banking		Credit institutions

Financial market infrastructures[1]		Operators of trading venues
		Central counterparties (CCPs)
		Central depositories
Financial services		Financial service providers, payment institutions, electronic money institutions
		CIT companies[2]
Insurance		Insurance and mutual insurance companies, provident institutions, reinsurers
Social		Social organizations[3]
Employment and vocational training		Payment operators[4]
Health sector	Health care settings	Healthcare providers (including hospitals and private clinics)
		Emergency medical assistance providers[5]
	Pharmaceutical products	Pharmaceutical wholesale distributors
Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption
Waste waters treatment		Wastewater collection, disposal, or treatment companies
		Flood and storm water managers
Education		Operators responsible for the national educational path, operators responsible for the organization of national exams
Food		Collective catering companies for the health, children, and prison sectors
Digital Infrastructure		IXPs
		DNS service providers
		TLD name registries

Appendix 12: Identified essential services by Greece

(Table made by author)

[1] There is no Central counterparties (CCPs) in Finland.

[2] Planning and operation of cash transport and Management of collection and supply requests.

[3] Calculation and payment of social benefits (health insurance, old age, family allowances and unemployment) and Management of collection and cash flow of social organizations.

[4] Calculation and payment of employment aid.

[5] Reception and regulation of calls and mobile emergency and intensive care service.

Sector	Subsector	Type of entity	Thresholds
1. Energy	Electricity	Electricity undertakings	Supplying electricity to more than 10% of the total customers of the electricity distribution network or to have more than 500.0 customers or to supply 10% of the total electricity power to the National Electricity Transmission System (NETS)[1] or to supply the NETS with a power of at least 1.5 GW.
		Distribution system operators	Supplying electricity to more than 10% of the total customers of the distribution network or to have more than 500,000 customers connected to the electricity distribution network.
		Transmission system operators	Managing at least 10% of the TWh circulating annually in the NETS or to manage the 5TWh circulating annually in the NETS.
	Oil	Operators of oil transmission pipelines	Operating a pipeline or pipelines capable of transporting more than 10% of the country's annual oil needs or at least 1.5 million cubic meters of oil per year.
		Operators of oil production, refining and treatment facilities, storage, and transmission	Managing 10% of the country's annual oil needs or at least 1.5 million cubic meters of oil per year.
	Gas	Supply undertakings	Introducing more than 500,000,000 cubic meters of natural gas into the National Natural Gas Transmission System (NNGTS).[2]
		Distribution system operators	Supplying gas to more than 10% of the total distribution network customers or to have more than 50,000 customers connected to the gas distribution network or the jurisdiction to cover the boundaries of a geographical region.
		Transmission system operators	Managing at least 10% or 500,000,000 cubic meters of natural gas that circulate annually in the NNGTS.

[1] Εθνικό Σύστημα Μεταφοράς Ηλεκτρικής Ενέργειας (ΕΣΜΗΕ)

[2] Εθνικό Σύστημα Μεταφοράς Φυσικού Αερίου (ΕΣΜΦΑ)

		Storage system operators	Having gas storage facilities with a capacity of more than 100,000 cubic meters of liquefied natural gas (LNG).
		LNG system operators	Having the technological capacity to import more than 10% of the annual consumption or 500,000,000 cubic meters of natural gas per year into the NNGTS.
		Natural gas undertakings	Having more than 10% of the total customers of the gas distribution network or to have at least 50,000 customers connected to the gas distribution network.
		Operators of natural gas refining and treatment facilities	Having the capacity of refining and processing at least 500,000,000 cubic meters of gas.
2. Transport	Air transport	Air carriers	Having an annual passenger traffic of at least 4,000,000 passengers or to handle more than 10% of the annual total number of passengers at Greek airports.
		Airport managing bodies, and entities operating ancillary installations contained within airports	Managing an airport with an annual passenger traffic of at least 4,000,000 passengers or an airport that handles more than 10% of the annual total number of Greek passengers' airports.
		Traffic management control operators providing air traffic control (ATC) services	Operating an airport with an annual passenger traffic of at least 4,000,000 passengers or an airport that handles more than 10% of the annual total number of passengers at Greek airports.
	Rail transport	Infrastructure managers	Managing transport infrastructure, per year, over 125 million passenger-kilometres or 25 million tonne-kilometres or more than 10% of the annual passenger-kilometres or more 10% of the tonne-kilometres of the railway network.
		Railway undertakings	Having transport work per year, more than 125 million passenger-kilometres each km or 25 million tonne-kilometres or more than 10% of the annual passenger-kilometres or more than 10% of the tonne-kilometres of the railway network.

	Water transport	Inland, sea and coastal passenger and freight water transport companies	Carrying at least 3,000,000 passengers per year or to carry at least 400,000 containers (TEUS) per year; or carry at least 100,000 trucks a year.
		Managing bodies of ports and entities operating works and equipment contained within ports	Managing a port carrying at least 3,000,000 passengers per or carry at least 400,000 containers (TEUS) per year or transport at least 100,000 trucks per year.
		Operators of vessel traffic services	Having under the supervision of the port or ports carrying at least 3,000,000 passengers per year or carrying at least 400,000 containers (TEUS) per year or to transport at least 100,000 trucks per year.
	Road transport	Road authorities	Being responsible for managing the traffic of motorways with passenger traffic of at least 10 million kilometres per year or at least 10,000 average daily vehicle traffic per year or 50 km total length of national highway.
		Operators of Intelligent Transport Systems	Being responsible for managing the intelligent transport systems (ITS) of vehicles with passenger traffic of at least 10 million kilometres per year or at least 10,000 average daily vehicle traffic per year or 50 km total length of national highway.
3. Banking		Credit institutions	Being licensed to operate in Greece and has been designated by the Bank of Greece as a systemically important credit institution.[1]
4.Financial market infrastructures		Operators of trading venues	Carrying out at least 10% of the total transactions carried out on an annual basis.
		Central counterparties (C	Carrying at least 10% of total transactions on an annual basis.
5. Health sector	Health care settings (including	Healthcare providers	Being a General Hospital, with at least 40,000 patients treated per year, or a General Hospital with at least 500 beds.

[1] The Bank of Greece, based on the Greek law 4261/2014 (article 124), is responsible for identifying other systemically important credit institutions among the credit institutions that have received an operating license in Greece.

	hospitals and private clinics)		
6.Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption	Supplying drinking water to a population of more than 500,000 consumers per year or to distribute more than 50,000,000 cubic meters of water per year.
7.Digital Infrastructure		IXPs	Having a daily traffic average of more than 5Gbit / second or to hold at least 10% of the total traffic of all IXP Operators operating in Greece .
		DNS service providers	Serving at least 1,000,000,000 requests per day or to have at least 50,000 different active domain names registered in its domain name registries or hold at least 10% of all queries between all DNS providers.
		TLD name registries	Serving at least 50,000,000 queries per day or to hold at least 10% of the total queries between all registrars of the TLD Registry.

Appendix 13: Identified essential services by Luxembourg

(Table made by author)

Sector	Sub-Sector	Type of entity
Energy	Electricity	Electricity undertakings
		Distribution system operators
		Transmission system operators
		Balancing supply and demand
	Oil	Operators of oil transmission pipelines
		Operators of oil production, refining and treatment facilities, storage, and transmission
	Gas	Supply undertakings
		Distribution system operators
		Transmission system operators
		Balancing supply and demand
		Storage system operators
		LNG system operators
		Natural gas storage
		Operators of natural gas refining and treatment facilities
Transport	Air Transport	Air carriers (freight and passenger)
		Airport managing bodies
		Traffic management control operators
	Rail Transport	Infrastructure managers
		Distribution of capacities
		Operators of service facility
		Railway undertakings (freight and passenger)
	Water Transport	Inland, sea and coastal passenger and freight water transport companies
		Managing bodies of ports including their port facilities
		Operators of vessel traffic services
	Road transport	Road authorities responsible for traffic management control
		Operators of Intelligent Transport Systems
Banking		Depositary bank activity
		Deposit management
		Credit granting activity
		Investment services
		Payment services
Financial market infrastructures		Operators of trading venues

Health sector	Health care settings	Hospital activity
		Medical analysis laboratory activity
		Blood transfusion
		Emergency intervention service
		Pharmaceutical distribution
Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption
Digital Infrastructure		IXPs
		DNS service providers
		TLD name registries

Appendix 14: Identified essential services by Poland

(Table made by author)

Sector	Subsector	Type of Entity	Thresholds[1]
Energy	Mining[2]	Natural gas extraction entities	The amount of natural gas extracted in the territory of the country in the previous year amounting to a minimum of 11 TWh or the share of the annual volume of natural gas production in the total domestic consumption of natural gas in the previous year amounting to at least 15%.
		Oil extraction entities	The share of the extracted raw material in the supply of crude oil to individual refineries located in the territory of the Republic of Poland, defined as a percentage of annual deliveries of at least 10%.
		Lignite extraction entities	The amount of lignite extracted in tonnes of at least 10 million tonnes per year.
		Coal extraction entities	The amount of hard coal mined in tonnes, amounting to a minimum of 8 million tonnes per year.
		Copper extraction entities	The amount of copper production of at least 50,000 tons per year.
	Electricity[3]	Electricity undertakings	Installed electricity capacity of at least 120 MW gross or the percentage share of generated and sold electricity in the total electricity production in the country, at least 0.4% in the annual electricity production, including the possession of a Centrally Dispatched Generation Unit.
		Distribution system operators	1) Number of users dependent on the essential service provided by a given entity: number of recipients of at least 500 thousand. annually, 2) market share of the entity providing the essential service: the percentage share of the recipients of a given operator in relation to the total number of recipients in the country: minimum 2.5%, 3) other factors specific to a given sub-sector: length of distribution / traction network of at least 50 km
		Transmission system operators	The minimum length of the transmission network is 5 km or the management of a Main Power Unit.
		Trading systems operators[4]	1) number of users dependent on the essential service provided by a given entity: number of end users of at least 500,000 annually, 2) other factors specific to a given sub-sector: the share of the amount of electricity sold by the enterprise in relation to the total amount of electricity supplied to end users in the country, amounting to at least 3.5%.
		Storage systems operators[5]	The storage capacity is at least 50 MW gross.
		System and quality services & Energy infrastructure management	1) the number of users dependent on the essential service provided by a given entity: the percentage share of the recipients of a given operator in relation to the total number of recipients in the country, not less than 2.5%, 2) other factors specific to a given sub-sector: the length of the transmission network of at least 5 km or the management of the Main Power Unit.

[1] For the purposes of maintaining a coherent presentation, only the defined criteria are presented in this table.

[2] On the basis of the concession referred to in Art. 22 sec. 1 of the 'Ustawa z dnia 9 czerwca 2011 r. Prawo geologiczne i górnicze, Dz.U. 2011 Nr 163 poz. 981'

[3] Cover Polskie Sieci Energetyczne S.A., five distribution network operators (Innogy Stoen Operator Sp. z o.o., PGE Dystrybucja S.A., ENEA Operator Sp. z o.o., Tauron Dystrybucja S.A., ENERGA – Operator S.A.), nine largest for the market of enterprises.

[4] As referred in Art. 3 point 12 of the 'Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, Dz.U. 1997 Nr 54 poz.348'

[5] As referred in Art. 3 point 12 of the 'Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, Dz.U. 1997 Nr 54 poz.348'

	Heating[1]	Heating undertakings	1) number of users dependent on the essential service provided by a given entity: minimum 15,000 end users and users of residential and commercial premises in multi-unit buildings, inhabited or used by persons who are not consumers (for whom the contract with the energy company has been concluded by the customer), 2) the impact that the incident, in terms of its scale and duration, could have on economic and social activity or public safety: impact on at least 50% of the recipients referred to in point (1). and, 3) market share of the entity providing the key service: above 50%, 4) other factors specific to a given sub-sector: installed thermal capacity of at least 50 MWt.
		Trading systems operators	1) number of users dependent on the essential service provided by a given entity: at least 15,000 thousand end users and users of residential and commercial premises in multi-unit buildings, inhabited or used by non-customers (for which the contract with the energy company has been concluded by the customer), 2) the impact that the incident, in terms of its scale and duration, could have on economic and social activity or public safety: impact on at least 50% of the recipients referred to in point (1). and, 3) market share of the entity providing the key service: above 50%,
		Transmission systems operators	1) the number of users dependent on the essential service provided by a given entity: at least 15,000 end-users and users of residential and commercial premises in multi-unit buildings, inhabited or used by non-consumers (for which the contract with the energy company was concluded by the customer) , 2) the impact that the incident, in terms of its scale and duration, could have on economic and social activity or public safety: impact on at least 50% of the recipients referred to in point a 3) market share of the entity providing the key service: above 50%, 4) other factors specific to a given sub-sector: the length of the heating network is at least 50 km.
		Distribution systems operators	1) the number of users dependent on the essential service provided by a given entity: at least 15,000 end-users and users of residential and commercial premises in multi-unit buildings, inhabited or used by non-consumers (for which the contract with the energy company was concluded by the customer), 2) the impact that the incident, in terms of its scale and duration, could have on economic and social activity or public safety: impact on at least 50% of the recipients referred to in point (1), d) market share of the entity providing the key service: above 50%, 3) other factors specific to a given sub-sector: the length of the heating network is at least 50 km.
	Oil[2]	Operators of oil production, refining and treatment facilities, storage, and transmission	The amount of produced liquid fuels in the previous year, amounting to a minimum of 5 million tonnes, or the volume of crude oil processed in the previous year, amounting to a minimum of 5 million tonnes.
		Operators of oil transmission pipelines	The average volume of crude oil transmission is at least 10 million tonnes annually for the last 3 years.

[1] As referred in Art. 3 point 12 of the 'Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, Dz.U. 1997 Nr 54 poz.348'

[2] Cover: PERN S.A.; Polish Oil and Gas Mining and LOTOS Petrobaltic S.A. and PKN 'Orlen', LOTOS S.A. Group

		Crude oil storage	Storage of at least 500,000 tonnes of crude oil per year on average over the last 3 years.
		Crude oil transhipment	Cargo handling at least 1 million tonnes of crude oil on average for the last 3 years.
		Operators of oil transmission pipelines	The average volume of crude oil transmission is at least 10 million tonnes annually for the last 3 years.
		Liquid fuels storage[1]	The sum of the nominal capacity of the warehouses of the entity providing the storage service, amounting to at least 100 thousand. m³.
		Liquid fuels transhipment[2]	Transhipment volume in the previous year made by the service provider handling of minimum 500 thousand. m3 per year
		Liquid fuels trading or foreign trading abroad[3]	Import of a minimum of 400 thousand. m3 of liquid fuels in the previous year or the number of liquid fuel stations used to operate in the previous year: at least 250 stations
		Operators of Synthetic fuels production	Producing a minimum of 100,000 m3 of synthetic fuels on an annual average over the last 3 years
	Gas[4]	Supply undertakings	The number of gaseous fuels produced in the previous year was at least 11 TWh
		Distribution system operators	The number of gaseous fuels distributed in the previous year, amounting to at least 90 TWh
		Transmission system operators	The amount of gas fuels transferred in the previous year, amounting to at least 110 TWh.
		Trade in gaseous fuels and natural gas trade with foreign countries	The amount of imported natural gas in the previous year, at least 100 TWh or the percentage ratio of the volume of natural gas imported to the domestic consumption of natural gas in the previous year, at least 60%, or the amount of gas fuels sold to end users in the previous year, at least 27 TWh
		Storage system operators	The level of working capacity made available to users in the previous year was at least 30 TWh
		LNG liquefaction and regasification	The amount of re-gasified liquefied gas in the previous year amounting to a minimum of 10 TWh
	Supplies and services to the energy sector	Operators supply of systems, machinery, equipment, materials, raw materials, and services to the energy sector	- supply of IT systems - market share of at least 20% or - supply of high-voltage power cables with a minimum length of 100 km per year, or - supply of power cables for high voltage with a length of at least 20 km per year
	Organisational units	Manufacture of radiopharmaceuticals	Producing radiopharmaceuticals with a sales value of at least PLN 24 million per year
		Treatment with radioactive waste	1) number of users dependent on the key service provided by the entity: at least 180 users from which radioactive waste is collected, 2) market share of the provider of the essential service: minimum 50%.

[1] As referred to in Art. 3 point 12 and Art. 32 sec. 1 of the 'Ustawa z 10 kwietnia 1997 r. Prawo energetyczne, Dz.U. 1997 Nr 54 poz.348'

[2] As referred to in Art. 3 point 12 and Art. 32 sec. 1 of the 'Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, Dz.U. 1997 Nr 54 poz.348'

[3] As referred to in Art. 3 point 12 and Art. 32 sec. 1 of the 'Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, ZDz.U. 1997 Nr 54 poz.348'

[4] Cover PSG sp. z o.o.; Gaz-System S.A.; PGNiG, which operates the seven largest gas storage facilities in Poland

		Maintaining strategic and back-up reserves of oil, oil, and natural gas products	1) market share of the entity providing the key service: above 50%, 2) geographic scope related to the area that could be affected by the incident: provision of the service throughout the country, 3) other factors specific to a given sub-sector: maintaining strategic reserves or agency reserves of crude oil with a book value of at least PLN 500 million per year.
		Research and development or investment or technological research for the energy sector	Conducting innovative, research and development or implementation works for the energy sector with a value of at least PLN 2 million per year.
Transport	Air Transport[1]	Air carriers (passengers)	Transport of at least 500 thousand passengers per year, determined: - on the basis of averaged statistical data for 3 years preceding the decision on recognizing the operator as the key service operator or - in the case of entities operating on the market for less than 3 years, on the basis of statistical data for 2 full years or 1 full year the year preceding the decision.
		Air carriers (freights)	A minimum market share of 25% of freight transport flights on the domestic market, calculated: - on the basis of averaged statistical data for the 3 years preceding the decision on recognizing the operator as the key service operator, or - in the case of entities operating on the market for less than 3 years, on the basis of statistical data for 2 full years or 1 full year preceding the decision.
		Airport managing bodies	Service at least 500,000 passengers annually determined: - on the basis of averaged statistical data for 3 years preceding the decision on recognition as the operator of a key service or - in the case of entities operating on the market for less than 3 years, on the basis of statistical data for 2 full years or 1 full year preceding the issuance of the decision or - in the case of new entities, the expected scope of activities of which meets the requirements of the threshold for recognition as an operator of a key service, on the basis of the master plan referred to in Art. 55 sec. 6 of the Act of July 3, 2002 - Aviation Law,
		Entities with the status of a registered agent	- Performance by the entity of security control of cargo or air mail together with assigning the inspected loads the statuses SPX, SCO and SHR in accordance with Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards of civil aviation security, or - Provision of the service of electronic transmission of information about the security status granted to the consignment, transmitted by air to the point of destination.
		Entities with the status of a ground-handling agent	The proper operation of other essential services at the airport depends on the services provided by the ground handling agent, while being unable to be provided by another entity.
		Traffic management control operators	The service is provided for more than 10,000 flights per year, irrespective of the maximum take-off weight and the number of passenger seats in the aircraft, with flights calculated as the sum of take-offs and landings and calculated as an average over the previous 3 years.
	Rail Transport[2]	Infrastructure managers	1) dependency with other sectors on the service provided by this entity: dependence of at least two of the

[1] Cover one air carrier, 8 airport managers, as well as an air navigation service provider.

[2] Cover mainly: PKP Polskie Linie Kolejowe S.A., Regional Transport, Mazowiecki Railways, PKP SKM Downtown, PKP Intercity; m.in. PKP Cargo, DB Cargo Polska.

			following sectors or subsectors on the service provided by the entity: - energy sector, electricity sub-sector, - energy sector, oil sub-sector, - energy sector, heat sub-sector, 2) the impact that the incident, in terms of its scale and duration, could have on economic and social activity or public safety: a) financial loss due to non-performance of transport: amounting to 500,000 zlotys a day, b) no possibility to run trains: 5,000 pieces per day, c) no possibility of delivering fossil fuels (coal), liquid fuels (fuel) for more than 12 hours, d) it is not possible to run passenger trains (public transport) longer than 12 hours 3) market share of the entity providing the key service: market share of railway infrastructure managers: over 50% of the length of the operated railway lines (according to current data published by the President of the Office of Rail Transport), 4) other factors specific to a given sub-sector: the number of applications submitted by railway undertakings for the construction of the timetable - not less than 800,000. annually
		Railway carriers (passengers)	1) market share of the entity providing the key service: the carrier's market share exceeding 25%, calculated according to the transport performance or the number of passengers (based on data published by the President of the Office of Rail Transport), 2) associated with the geographic coverage area, which could relate to the incident: provision of services in the area of at least 9 provinces.
		Railway carriers (freights)	The carrier's market share exceeds 25%, calculated according to the transport performance or weight of goods transported (based on data published by the President of the Office of Rail Transport).
	Water Transport[1]	Sea transport carriers (passengers)	Carriage of at least 100,000 passengers a year.
		Sea transport carriers (freights)	Transport of a minimum of 1 million tons of goods per year
		Inland passenger water transport	Carriage of at least 30% of inland waterway passenger transport passengers.
		Inland freights water transport	Carrying out at least 40% of goods transport per year in domestic inland transport.
		Managing bodies of ports including their port facilities	Management of a port belonging to the TEN-T core network as referred to in Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010 / UE (Journal of Laws UE L 348/1 of 20.12.2013, p. 1)
		Sea transport services for passengers and goods	1) number of users dependent on the essential service provided by a given entity: handling at least 100,000 maritime passengers annually, 2) other subsector specific factors: handling a minimum of 3 million tonnes of maritime goods per year
		Support activities for maritime transport	Each entity performing the services referred to in Art. 1 clause 2 letters a, c, f, and g of Regulation (EU) 2017/352 of the European Parliament and of the Council of 15 February 2017 establishing a framework for the

[1] Seaports in Gdynia, Gdansk, Szczecin, Elbląg, Kolobrzeg.

			provision of port services and common rules regarding the financial transparency of ports (Journal of Laws UE L 57 / 1 of 03.03.2017, p. 1)
		Operators of vessel traffic services	Collection and distribution of information related to the safety of maritime traffic in the territorial scope of activities of the directors of maritime offices specified in the regulations issued on the basis of art. 40 sec. 1 and 2 of the Act of March 21, 1991, on the maritime areas of the Republic of Poland and maritime administration
	Road transport	Road authorities responsible for traffic management control	1) the impact that an incident, in terms of scale and duration, could have on economic and social activities or public safety: any negative impact on road safety 2) geographical coverage related to the area that could be affected by the incident: minimum 15% of all national roads, 3) the entity's ability to maintain a sufficient level of the provision of the key service, considering the availability of alternative ways of providing it: there is no alternative to the service in the event of an incident, 4) other factors specific to a given sub-sector: minimum 500,000 motor vehicles on national roads per year.
		Operators of Intelligent Transport Systems	1) the impact that an incident, in terms of scale and duration, could have on economic and social activities or public safety: any negative impact on road safety or the correctness of the collection of tolls 2) geographical coverage related to the area that could be affected by the incident: minimum 15% of all national roads, 3) the entity's ability to maintain a sufficient level of the provision of the key service, considering the availability of alternative ways of providing it: there is no alternative to the service in the event of an incident, 4) other factors specific to a given sub-sector: minimum 500,000 motor vehicles on national roads per year
Banking		Credit institutions	Any credit institution that provides services: 1) accepting money deposits or other repayable funds from clients or 2) lending on its own account
		National Bank	1) market share of the essential service provider: provision of an essential service by a bank that is significant in terms of size, internal organization and type, scope, and complexity of its activity, which meets at least one of the following conditions: - the bank's share in the banking sector assets is not less than 2%, - the bank's share in banking sector deposits is not less than 2%, - the bank's share in the banking sector's own funds is not less than 2%, 2) other factors specific to the subsector: 1) provision of a key service by a bank that is significant in terms of size, internal organization, type, scope, and complexity activities, whose shares have been admitted to trading on a regulated market within the meaning of the provisions of the Act of July 29, 2005, on Trading in Financial Instruments (Journal Of Laws of 2017, item 1768, as amended died 6)), 3) provision of a key service by a bank that is significant in terms of size, internal organization and the type, scope, and complexity of its activity, which has been recognized as a significant bank by the Polish Financial Supervision Authority by way of an administrative

			decision in accordance with Art. 4b of the Act of August 29, 1997 - Banking Law.
		A branch of a foreign bank	Provision of an essential service by a branch of a foreign bank that is significant in terms of size, internal organization and the type, scope, and complexity of its activities, which meets at least one of the following conditions: - the share of a branch of a foreign bank in the assets of the banking sector is not less than 2%, - the share of a branch of a foreign bank in deposits of the banking sector is not less than 2%, - the share of a branch of a foreign bank in the own funds of the banking sector is not less than 2%.
		A Branch of a credit institution	Provision of the essential service by a branch of a credit institution, recognized by an administrative decision by the Polish Financial Supervision Authority as a significant branch of a credit institution in accordance with Art. 141f paragraph. 13 of the Act of August 29, 1997 - Banking Law.
		Cooperative savings and credit unions	Provision of the essential service by a cooperative savings and credit union whose average annual number of members exceeds 600 thousand people
Financial market infrastructures		Operators of trading venues	All entities providing this service
		Central counterparties (CCPs)	All entities providing this service
		Central depositories	All entities providing this service
Health sector	Health care settings	Healthcare providers (including hospitals and private clinics)	A healthcare provider qualified for the basic hospital system for securing healthcare services under the so-called 'Hospital networks' and having a Hospital Emergency Department.
		State's Emergency Medical Assistance system providers[1]	Providing access to services for all users
		Epidemiological Data Management	Providing access to services for all users
		Operators collecting and accessing electronic medical records	Providing access to services for all users
	National health Fund	National health insurance systems	All operators having concluded a contract for the provision of health care.
	Trade and distribution of medicinal products	Therapeutic entity, which operates the hospital pharmacy department	A healthcare provider qualified for the basic hospital system for securing healthcare services under the so-called 'Hospital networks' and having a Hospital Emergency Department
	Pharmaceutical warehouse	Pharmaceutical wholesale distributors	The number of permits issued for operating pharmaceutical wholesalers - at least 6.
		Entity running a business in a Member State of the European Union or a Member	The amount of the refund medicinal products over PLN 1 billion in the last calendar year.

[1] Available at https://www.gov.pl/web/zdrowie/system-panstwowe-ratownictwo-medyczne (accessed on March 23rd, 2021)

		State of the European Free Trade Association (EFTA) - parties to the Agreement on the European Economic Area, who obtained a marketing authorization for a medicinal product.	
	Importer of the medicinal product / active substance	Trade and distribution of medicinal products	The amount of the refund medicinal products included in the lists of medicinal products, medical devices and foods for particular nutritional uses risk of lack of availability on the territory of the Republic of Poland, issued pursuant to art. 37av paragraph. 14 of the Act of 6 September 2001 - Pharmaceutical Law - over PLN 50 million for the last calendar year
	Manufacturer of the medicinal product / active substance	Trade and distribution of medicinal products	The amount of the refund medicinal products included in the lists of medicinal products, medical devices and foods for particular nutritional uses risk of lack of availability on the territory of the Republic of Poland, issued pursuant to art. 37av paragraph. 14 of the Act of 6 September 2001 - Pharmaceutical Law - over PLN 50 million for the last calendar year
	Parallel importer	Trade and distribution of medicinal products	The amount of the refund medicinal products included in the lists of medicinal products, medical devices and foods for particular nutritional uses risk of lack of availability on the territory of the Republic of Poland, issued pursuant to art. 37av paragraph. 14 of the Act of 6 September 2001 - Pharmaceutical Law - over PLN 50 million for the last calendar year
	Distributor of active substance	Trade and distribution of medicinal products	A distributor of an active substance that meets all of the following conditions: • distributor of the active substance with a storage system and a system for maintaining storage conditions, • distributor of an active substance who is the sole distributor of a given active substance, • distributor of an active substance used in the production of a medicinal product included in the list of medicinal products, medical devices and foodstuffs for particular nutritional uses at risk of unavailability in the territory of the Republic of Poland.
	An entity running a generally accessible pharmacy	Trade and distribution of medicinal products	An entrepreneur running a business consisting in running at least 4 generally accessible pharmacies ensuring the availability of services at night, on Sundays, public holidays, and other days off on the basis of a resolution of the district council in the manner specified in art. 94 sec. 1 and 2 of the Act of 6 September 2001 - Pharmaceutical Law.
Drinking water supply and distribution	Water and sewage company	Water supply, treatment, and distribution	water supply, treatment for a minimum of 500,000 connected residents through a collective water supply.
		Wastewater collection and treatment	Operating in an agglomeration with an equivalent number of inhabitants over 500,000
Digital Infrastructure		IXPs	At least 100 interconnected autonomous systems, calculated as an annual average, considering the average of the last 3 years.
		DNS service providers	At least 100,000 domain names for which the server is authoritative.
		TLD name registries	Maintaining at least one Top Level Domain Registry (TLD) every 100,000 subscribers.

Appendix 15: Security provisions by Finland

(Table made by author)

Regulation	Article	Provision Title	Provision Content
Electricity Market Act (588/2013)	29a	Obligation of the network operator to manage the risks to communication networks and information systems and to	The network operator shall take care of the management of the risks to the networks and information systems it uses.

		report information security disruptions	
Natural Gas Market Act (587/2017)	34 a	Obligation of the transmission system operator to manage the risks to communications networks and information systems and to report data security disruptions	The transmission system operator shall manage the risks to the networks and information systems it uses.
Aviation Act (864/2014)	128a	Obligation to manage risks to NIS	The air navigation service provider and the socially relevant airport operator shall be responsible for managing the risks to the networks and information systems they use.
Railway Act (304/2011)	41 a	Obligation to manage risks to communications networks and information systems and to report security breaches	The state infrastructure manager and the traffic control service provider must take care of the management of the risks to the networks and information systems they use.
Act on Security and Surveillance of Certain Ships and Ports Serving Them (485/2004)	7e	Obligation of the port authority to manage the risks to communication networks and information systems	A port authority that is important for the operation of society must take care of managing the risks to the networks and information systems it uses
Vessel Traffic Services Act (623/2005)	16	Preservation of vessel traffic services	The VTS authority shall take care of the management of risks to the networks and information systems it uses.
Act on Transport Services (320/2017)	7	Obligation of the Information Transport Services (ITS) operator to manage the risks NIS and to report security breaches	The ITS operator must manage the risks to the networks and information systems it uses.
Act on the Operation of Credit Institutions (610/2014)	Chapter 9, Section 2	General requirements for the risk management system	The credit institution shall have effective and reliable corporate governance systems, as described in writing, for identifying, managing, limiting, monitoring and reporting on current and future risks to the credit institution and its operations. These include: 1) a clear organizational structure in which competencies and responsibilities are defined comprehensively and clearly; 2) effective risk management reporting processes; 3) sound internal control, management and accounting processes; 4) policies and procedures for remuneration schemes that are consistent with and promote sound and effective risk management. The systems referred to in subsection 1 must be comprehensive and proportionate to the quality, scope, and diversity of the plant's operations

	Chapter 9, Section 16	Operational risk	The credit institution must have methods for identifying, assessing and managing operational risks. It must at least be prepared for the occurrence of modelling risk as well as rare, serious risk events. The institution must clearly describe what it considers to be operational risks. It shall have written policies and procedures for operational risk management. The credit institution must have adequate, secure, and reliable payment, securities and other information systems. The credit institution must have contingency and continuity plans in place to prepare for serious business disruptions, to ensure business continuity and to limit losses in the event of disruptions.
	Section 24	Power to issue regulations by the Financial Supervision Authority	The Financial Supervision Authority may issue more detailed regulations on the credit risk assessment methods referred to in section 9 (1) and (2), credit and counterparty risk referred to in section 10, market risk referred to in section 14, operational risk referred to in section 16, liquidity risk referred to in section 17 and 21 Of the plan referred to in
Law on the Financial Supervision Authority (878/2008)	Section 18(2)	The right to obtain information from supervised and other financial market jurisdiction	The Financial Supervision Authority may issue regulations on the regular submission to the Financial Supervisory Authority of information concerning the supervised entity's financial position, owners, internal control and risk management, members of administrative and supervisory bodies and employees, as well as information necessary for performing the tasks referred to in section 3 (3) 3–5. (29.12.2016 / 1442).
Investment Services Act (744/2012)	Chapter 7a, Section 1	stock exchange	The Stock Exchange must ensure that the systems and procedures it uses ensure the reliability and continuity of the trading systems' operations even in the event of disruptions. The stock exchange must be able to ensure that it has sufficient resilience of trading systems, sufficient capacity to deal with peaks in-peaks of activity and messages and ensure proper trading in severe market stress conditions. The stock exchange shall regularly test the operation of the trading platform in order to meet the requirements described above. The Stock Exchange is required to notify Finanssivalvonta without undue delay of any system malfunction related to the financial instrument.
Health Care Act (1326/2010)[1]	Chapter 1, Section 8	Quality requirements for health care activities and patient safety	Healthcare activities must be based on evidence and good care and practice. Healthcare activities must be of high quality, safe and properly implemented.

[1] Terveydenhuoltolaki (1326/2010) 30/12/2010

			Municipal primary health care must be responsible for coordinating the patient's care as a whole, unless otherwise agreed. The healthcare unit must draw up a plan for quality management and the implementation of patient safety. The plan must consider the promotion of patient safety in cooperation with social care services. A decree of the Ministry of Social Affairs and Health stipulates matters that must be agreed in the plan.
Act on the Electronic Processing of Customer Data in Social Welfare and Health Care (159/2007)[1]	Chapter 5a, Section 19a	The essential requirements of the information system used in the processing of customer data in social welfare or health care.	The information system used to process social or health care customer data must meet the essential requirements for interoperability, data security and data protection, and functionality. If necessary, the National Institute for Health and Welfare may issue more detailed regulations on the content of the essential requirements. Before issuing an order, the Department of Health and Welfare must consult the Advisory Board for Electronic Information Management of Social and Health Care.
Act on Medical Devices and Supplies (629/2010)[2]	Chapter 1, Section 5	Definitions	1) health care device means an instrument, apparatus, instrument, software, material or other device or accessory used alone or in combination, the manufacturer of which is intended for human use: (a) the diagnosis, prevention, monitoring, treatment or alleviation of a disease; (b) the diagnosis, monitoring, treatment, alleviation or compensation of an injury or defect; (c) to study, replace or modify anatomy or physiological function; or (d) fertility control;
	Chapter 2, Section 6	Essential requirements	The device must be suitable for its intended use and, when used in accordance with its intended use, must achieve the functionality and performance designed for it. Proper use of the device must not unnecessarily endanger the health or safety of the patient, user, or other person.
	Chapter 3, Section 17	Obligations of the operator	The operator must follow the information and instructions provided by the manufacturer for the transport, storage, installation, maintenance, and other handling of the healthcare device. The operator must ensure that, when handing over the healthcare device to the end user, the device is in the

[1] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) 09/02/2007

[2] Terveydenhuollon laitteista ja tarvikkeista annetun lain (629/2010) 24/06/2010

			condition in which the manufacturer intended the device to be used. If necessary, the device to be handed over to an end user other than a professional user must be properly serviced before handing over.
Act on the Licensing and Supervision Agency for the Social and Health Sector (669/2008)			
Water Supply Act (119/2001)[1]	15a	Securing the services of a water supply plant in the event of a breakdown	The water utility prepares and keeps up-to-date a plan for preparedness for incidents and takes the necessary measures on the basis of the plan. The department submits the plan to the supervisory authorities, the rescue authority and the municipality.
			The provisions of subsections 1 and 2 also apply to a plant that supplies water to a water supply plant or treats wastewater from a water supply plant.
			A Government decree may lay down more detailed provisions on the criteria according to which a water supply company plans to prepare for disturbances.
Information Society Act (917/2014)[2]	243	Quality requirements for communications networks and services	Public communications networks and services and the communications networks and services connected to them shall be designed, constructed, and maintained in such a way that: 1) electronic communications are of good technical quality and data security; 2) they withstand the normal expected climatic, mechanical, electromagnetic and other external disturbances as well as security threats; 4) significant security breaches and threats to them and defects and disturbances that significantly interfere with their operation can be detected; 7) no one's data protection, data security or other rights are compromised;
			Measures to ensure the information security referred to in subsection 1 (1), (2), (4), (7) and (9) shall mean measures to ensure operational security, telecommunications security, hardware and software security and data security. The measures shall be proportionate to the seriousness of the

[1] Vesihuoltolaki (119/2001) 09/02/2001, viimeksi muutettuna (290/2018) 04/05/2018

[2] Laki sähköisen viestinnän palveluista (917/2014) 07/11/2014, viimeksi muutettuna (281/2018) 04/05/2018

			threat, the cost of the measures and the technical capabilities available to counter the threat.

Appendix 16: OES Notification obligations by Finland

(Table made by author)

Regulation	Article	Provision Title	Provision Content
Electricity Market Act (588/2013)	29a	Obligation of the network operator to manage the risks to communication networks and information systems and to report information security disruptions	The network operator shall immediately notify the Agency of any significant information security disruption to the communication networks or information systems used by it, as a result of which the distribution of electricity in the distribution network may be interrupted to a significant extent.

			If it is in the public interest to report a disturbance, the Energy Agency may oblige the service provider to inform the public or, after consulting the notifier, to inform the matter itself.
			The Energy Agency shall assess whether the disturbance referred to in subsection 2 affects other Member States of the European Union and, if necessary, notify the other Member States.
			The Energy Agency may issue more detailed regulations on when the disturbance referred to in subsection 1 is significant, as well as on the content, form, and submission of the notification.
Natural Gas Market Act (587/2017)	34 a	Obligation of the transmission system operator to manage the risks to communications networks and information systems and to report data security disruptions	The transmission system operator shall immediately notify the Agency of any significant information security disruption to the communication networks or information systems it uses, as a result of which the transmission of natural gas may be interrupted in the transmission network to a significant extent.
			If it is in the public interest to report a disturbance, the Energy Agency may oblige the transmission system operator to inform the matter or, after consulting the notifier, to inform the matter itself.
			The Energy Agency shall assess whether the disturbance referred to in subsection 2 affects other Member States of the European Union and, if necessary, notify the other Member States.
			The Energy Agency may issue more detailed regulations on when the disturbance referred to in subsection 1 is significant, as well as on the content, form, and submission of the notification.
Act on the Supervision of the Electricity and Natural Gas Market (590/2013)	27	Supervisory cooperation between authorities	The Agency has the right to co-operate in matters within its competence with the Financial Supervision Authority, the Competition and Consumer Authority, FICORA, the Consumer Ombudsman, the Agency for the Cooperation of Energy Regulators, the regulatory authority of another EEA State and the European Commission. control or inspection function.
	28	The right of the Energy Agency to disclose information to another authority	The Agency shall be entitled to disclose only such information as is necessary for the performance of the tasks of the relevant authority and, if the information is disclosed to a foreign authority or international body, provided that it is subject to the same confidentiality obligations as the Agency.
			The Agency shall not disclose confidential information received from an authority of another State or an international body without the express consent of the notifying authority. Such information may be used only for the performance of tasks in accordance with this Act or for the purposes for which consent has been given.
Aviation Act (864/2014)	128a	Obligation to manage risks to NIS	The Finnish Transport Safety Agency shall assess the effects of the risk management referred to in subsection 1 on aviation safety.
			The air navigation service provider and the managing body of the airport, which is important for the operation of society, shall provide the Finnish Transport Safety Agency with the information necessary for the assessment.
			The Agency may oblige an air navigation service provider and a publicly relevant airport operator to take remedial action to eliminate a significant risk to aviation safety.
			Notwithstanding secrecy provisions and other restrictions on the disclosure of information, the Finnish Transport Safety Agency has the right to

			disclose a document received or prepared in connection with the performance of its duties provided for in subsection 2 and to disclose confidential information to FICORA if it is necessary to perform information security tasks.
	128b	Reporting security breaches	The air navigation service provider and the managing body of an airport which is important for the operation of society shall immediately notify the Finnish Transport Safety Agency of any significant information security incident affecting communications networks or information systems.
			If it is in the public interest to report a deviation, the Finnish Transport Safety Agency may oblige the service provider to inform the matter or, after consulting the person required to report, to inform the matter itself.
			The Finnish Transport Safety Agency shall assess whether the deviation referred to in subsection 1 applies to other Member States of the European Union and, if necessary, notify the other Member States concerned.
Railway Act (304/2011)	§ 41 a	Obligation to manage risks to communications networks and information systems and to report security breaches	The state infrastructure manager and the traffic control service provider shall immediately notify the Finnish Transport Safety Agency of any significant information security-related disruption to communications networks or information systems.
			If it is in the public interest to report a disturbance, the Finnish Transport Safety Agency may oblige the service provider to inform the matter or, after consulting the person required to report, to inform the matter itself.
			The Finnish Transport Safety Agency shall assess whether the disturbance referred to in subsection 2 affects other Member States of the European Union and, if necessary, notify the other Member States concerned.
			Notwithstanding confidentiality provisions and other restrictions on the disclosure of information, the Finnish Transport Safety Agency shall have the right to disclose a document received or prepared in the course of performing its duties provided for in this section and to disclose confidential information to FICORA if it is necessary for information security tasks.
			The Finnish Transport Safety Agency may issue more detailed regulations on when the disturbance referred to in subsection 2 is significant, as well as on the content, form, and delivery of the notification.
Act on Security and Surveillance of Certain Ships and Ports Serving Them (485/2004)	7e	Obligation of the port authority to manage the risks to communication networks and information systems	A port authority that is significant for the operation of society shall immediately notify the Finnish Transport Safety Agency of any significant information security-related disruption to the communication networks or information systems used by it.
			If it is in the public interest to report a disturbance, the Finnish Transport Safety Agency may oblige the service provider to inform the matter or, after consulting the person required to report, to inform the matter itself.
			The Finnish Transport Safety Agency shall assess whether the disturbance referred to in subsection 1 affects other Member States of the European Union and, if necessary, notify the other Member States concerned.
			The Finnish Transport Safety Agency may issue more detailed regulations on when the disturbance referred to in subsection 1 is significant, as well as on the content, form, and delivery of the notification.

Vessel Traffic Services Act (623/2005)	18a	Reporting security incidents	The VTS authority shall immediately notify the Finnish Transport Safety Agency of any significant information security disruption to the communication networks or information systems used by it.
			If it is in the public interest to report a disturbance, the Finnish Transport Safety Agency may oblige the service provider to inform the matter or, after consulting the person required to report, to inform the matter itself.
			The Finnish Transport Safety Agency shall assess whether the disturbance referred to in subsection 1 affects other Member States of the European Union and, if necessary, notify the other Member States concerned.
			The Finnish Transport Safety Agency may issue more detailed regulations on when the disturbance referred to in subsection 1 is significant, as well as on the content, form, and delivery of the notification.
			Notwithstanding confidentiality provisions and other restrictions on the disclosure of information, the Finnish Transport Safety Agency shall have the right to disclose a document received or prepared in the course of performing its duties provided for in this section and to disclose confidential information to FICORA if it is necessary for information security tasks.
	28	Enforcement	The Finnish Transport Safety Agency shall assess the effects of the risk management referred to in section 16 (5) on maritime safety. The Finnish Transport Safety Agency may order corrective measures to eliminate a significant risk to maritime safety. A penalty payment may be imposed as an effect of the obligation. The penalty payment is regulated by the Penalty Act (1113/1990).
Act on Transport Services (320/2017)	7	Obligation of the Information Transport Services (ITS) operator to manage the risks NIS and to report security breaches	The ITS operator shall immediately notify the Finnish Transport Safety Agency of any significant information security disruption to the communication networks or information systems used by it.
			If it is in the public interest to report a disturbance, the Finnish Transport Safety Agency may oblige the service provider to inform the matter or, after consulting the person required to report, to inform the matter itself.
			The Finnish Transport Safety Agency shall assess whether the disturbance referred to in subsection 2 affects other Member States of the European Union and, if necessary, notify the other Member States concerned.
			Notwithstanding secrecy provisions or other restrictions on the disclosure of information, the Finnish Transport Safety Agency shall have the right to disclose a document received or prepared in the course of performing its duties provided for in this section and to disclose confidential information to FICORA if necessary for information security purposes.
Investment Services Act (744/2012)	Chapter 7a, Section 1	Stock Exchange	The Stock Exchange is required to notify Finanssivalvonta without undue delay of any system malfunction related to the financial instrument.
Act on the Electronic Processing of Customer Data in Social Welfare and	Chapter 5b	Reporting deviations	If the provider of social or health services finds that there are significant deviations from the fulfilment of the essential requirements of the information system, the provider shall inform the manufacturer of the information system. If the deviation may pose a significant risk to patient safety, data security or data protection, the Social Licensing and Supervision Agency must also be notified.

Health Care (159/2007)[1]			
Act on Medical Devices and Supplies (629/2010)[2]	Chapter 3, Section 17	Obligations of the operator	The operator shall inform the manufacturer or his authorized representative of any dangerous situation which has come to his notice or is suspected of being due to a defect or defect in the equipment.
	Chapter 5, Section 25	Notification of incidents	The professional user shall inform the Social and Health Licensing and Supervision Agency and the manufacturer or his authorized representative of any incidents which have led or could have led to a risk to the health of the patient, user, or other person and which result from the healthcare device: 1) characteristics; 2) performance deviation or disturbance; 3) insufficient marking; 4) insufficient or incorrect instructions for use; or 5) off. The Social and Health Licensing and Supervision Agency may issue regulations on how incidents are reported and what information must be reported about them
Act on the Licensing and Supervision Agency for the Social and Health Sector (669/2008)	6	Provision of information	State and municipal authorities and other public bodies, the Social Insurance Institution, the Finnish Canter for Pensions, the Patient Injury Board, the pension fund and other pension institution, the insurance institution, the community or institution providing maintenance or medical care, the provider of private social services and the pharmacy are obliged upon request to provide the Agency, free of charge, with the information and explanations necessary for the performance of the tasks referred to in section 2, notwithstanding the provisions on professional secrecy.
			Notwithstanding the secrecy provisions, the authority, association, and institution referred to in subsection 1 above and a pharmacy have the right to notify it without a request from the agency of a circumstance that may endanger the safety of customers or patients, the health or safety of the living environment or the public.
			Notwithstanding the provisions on secrecy, the Agency and regional administrative agencies have the right to provide each other with the information and explanations necessary for the performance of the tasks referred to in section 2.
			The Agency has the right to disclose information to FICORA, without prejudice to confidentiality provisions, if it is necessary for the performance of tasks related to information security.
			The information and reports referred to in subsection 3 above may also be disclosed by means of a technical user interface. Prior to opening the technical connection, proper data protection must be ensured.
Water Supply Act (119/2001)	15b	Notification of water supply disturbances	A water supply company that supplies water or receives at least 5,000 cubic meters of wastewater per day shall immediately notify the Centre for Economic Development, Transport and the Environment of a significant disruption in water supply.
			If it is in the public interest to report a disturbance, the Centre for Economic Development, Transport, and the Environment may oblige the water supply undertaking to inform the matter or, after consulting the water supply undertaking, to inform the matter itself.

[1] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) 09/02/2007

[2] Terveydenhuollon laitteista ja tarvikkeista annetun lain (629/2010) 24/06/2010

			What is provided in subsection 1 for a water supply plant also applies to a plant that supplies water to a water supply plant or receives wastewater from a water supply plant.
			The Centre for Economic Development, Transport and the Environment shall submit the notification referred to in subsection 1 to the Ministry of Agriculture and Forestry for information. In addition, the Centre for Economic Development, Transport, and the Environment shall assess whether the disturbance referred to in subsection 1 affects other Member States of the European Union and, if necessary, notify the relevant authority of the Member State of the disturbance.
			The Ministry of Agriculture and Forestry may, by decree, issue more detailed provisions on when the water supply disturbance referred to in subsection 1 must be considered significant, and on the content, form and submission of the notification referred to in subsection.
	35	Duty of secrecy	Notwithstanding the obligation of professional secrecy laid down in the Act on the Publicity of the Activities of Public Authorities, information obtained in the performance of duties under this Act concerning the financial position, business or professional secrecy or personal circumstances of an individual or entity may be disclosed: 1) the supervisory authority for the performance of tasks pursuant to this Act; 2) to investigate the crime to the prosecuting and police authorities; 3) FICORA if it is necessary for the performance of tasks related to information security.
Information Society Act (917/2014)	275	Fault notifications to FICORA	The telecommunications operator shall immediately notify FICORA if its service is subjected to or threatened with a significant security breach or other event that prevents the operation of the communications service or substantially interferes with it. The telecommunications operator shall also indicate, without undue delay, the estimated duration and effects of the disruption or threat thereof, the remedial measures and the measures taken to prevent a recurrence of the disruption. If it is in the public interest to report a disturbance, FICORA may oblige the telecommunications operator to notify the matter.
			FICORA may issue more detailed regulations on when the disturbance referred to in subsection 1 is significant and regulations on the content, form, and submission of the notification.

Appendix 17: OES Notification obligations by France

(Table made by author)

	Undue delay	**Significant impact**	**Notification to public**	**Cross-border notification**	**Confidentiality**

Article 7, para. 1 of the Law 2018-133	The operators declare, without delay after having taken cognizance of them, to the [ANSSI], the incidents affecting the [NIS] necessary for the provision of essential services…	… when these incidents have or are likely to have, considering in particular the number of users and the geographical area affected as well as the duration of the incident , a significant impact on the continuity of these services.			
Article 7, para. 2 of the Law 2018-133			After consulting the operator concerned, the administrative authority can inform the public of an incident [having a significant impact], when this information is necessary to prevent or deal with an incident.	When an incident has a significant impact on the continuity of essential services provided by the operator in other Member States of the European Union, the administrative authority informs the competent authorities or bodies of these States.	
Article 3, para. 2 of the Law 2018-133					When informing the public or the Member States of the European Union of incidents under the conditions provided for in Articles 7 and 13, the competent administrative authority shall consider the economic interests of these operators and digital service providers and ensure that they do not reveal information likely to endanger their security and commercial and industrial secrecy.'

Article 11 of the Ministerial Decree 2018-384	Without prejudice to the sectoral provisions providing for other incident reporting regimes, the operators of essential services report to the [ANSSI], as soon as they become aware of the incidents (…).			As soon as they become aware of additional information relating to the causes of the incident or its consequences, in particular, where applicable, those on the provision of the service in other Member States of the European Union, the operators shall communicate this information to the agency. They also respond to requests for information from the agency concerning the incident as it evolves.	
Article 12 of the Ministerial Decree 2018-384 **Article 12 of the Ministerial Decree 2018-384**				The [ANSSI] informs the competent authorities or bodies of other Member States of the European Union of the incidents mentioned in the first paragraph having a significant impact on the continuity of essential services provided in these States.	
			Under the conditions provided for by Article 7, para. 2 of the Law 2018-133, it may, at the request of the Prime Minister, inform the public of the incidents [having a significant impact].		

Appendix 18: Security provisions by Ireland

(Table made by author)

Sector	Subsector	Type of entity	Incident Reporting Level
1. Energy	Electricity	Electricity undertakings	Loss of 10 GWh or greater of generation capacity in a seven-day period
		Distribution system operators	Loss of 10 GWh or greater of electricity distribution in a seven-day period
		Transmission system operators	Loss of 10 GWh or greater of electricity transmission in a seven-day period
	Oil	Operators of oil transmission pipelines	Not Applicable
		Operators of oil production, refining and treatment facilities, storage, and transmission	Loss of oil production, refining and treatment, or storage and transmission greater than 50,000 barrels (or BOE) per day.
	Gas	Supply undertakings	Not Applicable
		Distribution system operators	Loss of 200 GWh of gas distributed in a 7 day-Period
		Transmission system operators	Loss of 200 GWh of gas transmitted in a 7 day-Period
		Storage system operators	Not Applicable
		LNG system operators	Not Applicable
		Natural gas undertakings	Loss of 200 GWh of gas transmitted in a 7 day-Period
		Operators of natural gas refining and treatment facilities	Not Applicable
2. Transport	Air transport	Air carriers	Any incident which results in more than 25% of the air carrier's scheduled flights in the State being cancelled in a 24 hour-period
		Airport managing bodies, and entities operating ancillary installations contained within airports	Any incident which results in more than 25% of the airport managing bodies scheduled flights in the State being cancelled in a 24 hour-period
		Traffic management control operators providing air traffic control (ATC) services	Any incident that has an effect on the operation of Air Traffic Management Services within the State
	Rail transport	Infrastructure managers	Any incident which results in 25% of a train operator’s services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations

		Railway undertakings	Any incident which results in 25% of a train operator's services being cancelled in a 24-hour period or in an amended timetable being run that is equivalent to that number of cancellations
	Water transport	Inland, sea and coastal passenger and freight water transport companies	Any incident which results in the suspension of sailings from any port within the State for a period of two hours or more; or Any incident which results in 25% of scheduled sailings from a port being cancelled or delayed by 2 hours or more
		Managing bodies of ports and entities operating works and equipment contained within ports	For passengers and roll-on roll-off traffic: Any incident that results in the port being closed for two hours or more; or 25% of scheduled sailings being cancelled or delayed by 2 hours or more. For LOLO, Liquid Bulk, Dry Bulk and Break Bulk traffic: Any incident which results in suspension of throughput at the port for 4 hours or more.
		Operators of vessel traffic services	Any incident which results in the loss or disruption of a VTS system that causes delays in excess of two hours for 20% of ship movements within a 24 hour period or the port being closed for two hours or more
	Road transport	Road authorities	Not Applicable
		Operators of Intelligent Transport Systems	For Operators of ITS in area over 500,00 people; A single incident that results in a loss of capacity of 100% to the flow of traffic on a road in one or both directions for a period of more than 2 hours. For Operators of ITS in area under 500,000 people; A single incident that results in a loss of capacity of 100% to the flow of traffic on a road in one or both directions for a period of more than 6 hours
3. Banking		Credit institutions (Payment Services provided to non-Monetary Financial Institutions in the State, Cash Services provided in the State and Access to retail payment systems provided to credit institutions in the State)	Based on transactions affected; > 25% of the Credit Institution's regular level[1] of transactions (in terms of number of transactions) or > EUR 5 million Based on payment services users > 50 000 or > 25% of the credit institution's payment service users Based on economic impact; > Max. (0.1% Tier 1 capital,* EUR 200 000)

[1] Regular level is the daily annual average of transactions, taking the previous year as the reference period for calculations

			or > EUR 5 million.
4.Financial market infrastructures		Operators of trading venues	Any incident affecting the institution's ability to list or trade Irish equities in the State
5.Health sector		Healthcare providers	Any incident that affects the ability of an operator to provide continuity of essential services to users and where applicable the operator has greater than 500 total beds (In-Patient and Day Bed Spaces)
6.Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption	Any incident that effects the ability of an OES to supply and distribute water intended for human consumption to greater than 200,000 users within the state
7.Digital Infrastructure		IXPs	Loss or significant degradation of connectivity to 25% of connected global routes for greater than 1 hour or loss of greater than 75% of total port capacity for greater than 1 hour
		DNS service providers	Loss or significant degradation of the service to greater than 50% of clients in 30 minutes or loss or significant degradation of service for greater than 25% of domains
		TLD name registries	Loss or significant degradation of greater than 25% of name resolution capability for greater than 1 hour

Appendix 19: Security provisions by Poland

(Table made by author)

Sector	**Subsector**	**Type of Incident**	**Thresholds**
Energy	Mining	Incident relating to Mining minerals	1. number of users whom concerns a disruption of performance core service: not applicable;

			2. time of impact of the incident for the essential service provided: the incident led to interruption of production for a period longer than 72 hours; 3. the geographical scope of the area, affected by the incident: no concerns; 4. other factors specific to a given subsector: the incident caused what one of the following the circumstances mentioned: a) human death, b) serious damage to health, c) other than serious damage to health of more than one person, d) financial losses over 250 thousand PLN.
	Electricity	Incident relating to coverage demand on a local scale	1. number of users concerned by a disruption on the provisions of the essential service; 2. time of impact of the incident for the essential service provided: loss for at least 3 minutes power consumers above 10% actual demand system in the period preceding the incident; 3. the geographical scope of the area, affected by the incident: not applicable; 4. other factors specific to a given subsector: not applicable.
		Incident relating to coverage demand on a national scale	1. number of users concerned by a disruption on the provisions of the essential service: not applicable; 2. time of impact of the incident for the essential service provided: loss for at least 3 minutes power consumers above 10% actual demand system in the period preceding the incident; 3. the geographical scope of the area, affected by the incident: not applicable; 4. other factors specific to a given subsector: not applicable.
		Incident concerning the transmission network	1. number of users concerned by a disruption on the provisions of the essential service: not applicable; 2. time of impact of the incident for the essential service provided: not applicable; 3. the geographical scope of the area, affected by the incident: not applicable; 4. other factors specific to a given subsector: emergency, simultaneous shutdown of at least two elements of the transmission network, resulting in: a) a significant deterioration in system operating conditions or b) restricting the capacity of cross-border exchange, or c) announcement by the Transmission System Operator of the state threats to the transmission system or the state of power failure or the state of restoration of the system.[1]
		Power generating modules incident	1. number of users concerned by the disruption of the essential service: not applicable; 2. time of impact of the incident for the essential service provided: lasting more than 15 minutes: a) simultaneous, unplanned exclusion of at least two power generating modules in one power plant with a total power above 400 MW gross or b) simultaneous, unplanned power limitation or disabling modules total energy generation power size above 1500 MW gross; 3. the geographical scope of the area, affected by the incident: not applicable; 4. other factors specific to a given subsector: not applicable.
		Incident relating to devices and tools used for monitoring and work control system	1.Number of users affected by the disruption of essential service: not applicable;

[1] In accordance with the classification of system states specified in Art. 18 of the Regulation (EU) 2017/1485

			2.time of the incident's impact on the essential service provided: the loss of one of the following real-time devices or tools, while primary and backup devices and tools are not available: a) means of dispatch communication, for a period of at least 1 hour, or b) remote control systems for substation equipment and production sources for a period exceeding 15 minutes, or c) systems for monitoring the system operation (including system state estimation) for a period exceeding 15 minutes, d) tools used to assess the safety of the system operation for a period exceeding 15 minutes, or e) 'smart metering' class systems if it is not possible to obtain data from at least 30% of the measuring systems planned for reading, for a period exceeding 48 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. other factors specific to a given subsector: not applicable.
	Heating	Incident relating to heat generation	1.Number of users affected by the disruption of essential service: not applicable; 2.time of the incident's impact on the essential service provided: the incident led to an interruption of heat production for more than 24 hours; 3. Geographical Coverage of the Incident Area: Not applicable; 4.other factors specific to a given sub-sector: the incident caused at least one of the following circumstances: a) human death, b) serious damage to health, c) other than serious damage to health of more than one person, d) financial losses exceeding PLN 250,000 PLN.
		Incident relating to the trading or transmission or distribution of heat	1.Number of users affected by the disruption of essential service: not applicable; 2.time of the incident's impact on the essential service provided: the incident led to an interruption of heat production for more than 24 hours; 3. Geographical Coverage of the Incident Area: Not applicable; 4.other factors specific to a given sub-sector: the incident caused at least one of the following circumstances: a) human death, b) serious damage to health, c) other than serious damage to health of more than one person, d) financial losses exceeding PLN 250,000 PLN.
	Oil and Gas	Incident related to the transmission of crude oil and liquid fuels	1. Number of users affected by the disruption of essential service: not applicable; 2. duration of impact of the incident on the essential service provided: the incident results in the impossibility of timely and in nominated supply and transmission of crude oil for a period exceeding 20 hours; 3. Geographical Coverage of the Incident Area: Not applicable; 4. other subsector-specific factors: uncontrolled spill of crude oil or other hazardous substances into the atmosphere or soil.
		Incident related to the production, extraction, production of liquid fuels, crude oil storage, crude oil handling, storage of liquid fuels, handling of liquid fuels, trade in liquid fuels and foreign trade in liquid fuels, production of synthetic fuels	1.Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident results in a disruption to the production or refining or to the functioning of processing equipment or the storage and transmission of crude oil for more than 20 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other sub-sector-specific factors: a) significant loss of station integrity, or b) loss of protection of the station against the effects of explosion, or c) loss of maintenance station in the case of mobile installations, or d) uncontrolled leakage of crude oil or other hazardous substances into the atmosphere or land.
		An incident concerning the	1.Number of users affected by the disruption of essential service: not applicable;

		production of gaseous fuels, transmission of gaseous fuels, distribution of gaseous fuels, trade in gaseous fuels or trade in natural gas with foreign countries, storage of gaseous fuels, liquefaction or regasification of LNG or the import and unloading of LNG	2.time of the incident's impact on the essential service provided: the incident results in the impossibility of proper supply and transmission of natural gas for a period of at least 24 hours or a disruption in the production or operation of processing equipment or the storage or transmission of natural gas for a period longer than 20 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sub-sector: a) unplanned leakage of gas or other dangerous substances, regardless of whether they have ignited, posing an immediate danger of: - loss of life or damage to health, or - large-scale damage, or b) uncontrolled decrease or increase in pressure in the gas network, or c) stoppage of the gas compressor station or gas station, or d) uncontrolled closure or opening of fittings in gas network facilities.
	Supplies and services to the energy sector	Incident related to the supply of systems, machines, devices, materials, raw materials, and the provision of services to the energy sector.	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: a) the incident results in a disruption in the production of liquid fuels or the refining of liquid fuels, or in the operation of liquid fuel processing equipment, or liquid fuel reloading, or liquid fuels trading, or foreign trade in liquid fuels, or the production of synthetic fuels or the storage and transmission of crude oil for a period longer than 4 hours, or b) the incident results in an interruption in the supply of electricity to the crude oil transmission system for a period of more than 8 hours, or c) the incident results in an interruption in the supply of electricity to crude oil storage system for a period exceeding 8 hours, or d) the incident results in a break in the provision of services in rail and road transport (rail tankers and road cisterns) for a period exceeding 24 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given subsector: not applicable.
		Incident involving the maintenance of strategic reserves or agency stocks of crude oil, petroleum products and natural gas	1.Number of users affected by the disruption of essential service: not applicable; 2.Dduration of impact of the incident on the essential service provided: the incident results in the interruption of the process of providing strategic reserves or the release of agency stocks of crude oil, petroleum products and natural gas for a period longer than 4 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given subsector: not applicable.
		Radioactive waste management incident	1. Number of users affected by the disruption of essential service: minimum 200 users from which radioactive waste is collected; 2. Duration of the incident's impact on the essential service provided: not applicable; 3. geographic scope of the area concerned: the territory of the whole country; 4. other factors specific to a given sub-sector: the incident results in an immediate danger of causing damage to health or long-term contamination of the environment.
Transport	Air Transport	An air transport incident (passenger)	1.Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. other factors specific to the subsector: a) the interruption of the service by the air carrier for more than 2 hours, or b) damage to the aircraft or information systems essential to its control and operation, or c) the incident resulted in death or damage to human health.

		An air transport incident (freight)	1.Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to the subsector: a) the interruption of the service by the air carrier for more than 2 hours, or b) damage to the aircraft or information systems essential to its control and operation, or c) the incident resulted in death or damage to human health.
		An incident involving an entity with the status of a registered agent	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. other factors specific to the subsector: a) the regulated agent interrupted the security control process for more than 2 hours; or b) the security status information transmission service disrupted for more than 2 hours.
		Incident related to the availability of ground service	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. other sub-sector specific factors: the incident led to the lack of availability of the ground handling agent service for more than 2 hours or to the unavailability of essential services provided by other entities in the sub-sector.
		Incident involving the airport operator	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. other factors specific to the subsector: a) disruption of air operations for more than 2 hours, or b) the incident resulted in death or damage to human health, or c) the incident led to the unavailability of essential services provided by other entities in the subsector.
		Air navigation service provider incident	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other subsector-specific factors: the incident disrupted the air traffic management system and reduced airspace capacity by at least 30%.
	Rail Transport	Incident related to the construction of the train timetable	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sub-sector: the impossibility of constructing train timetables due to: a) software failure exceeding 12 hours, or b) power failure resulting in unavailability of the service for more than 2 hours, or c) failure of tele-informatic networks for more than 12 hours.
		Incident involving trains running	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable;

			4. Other factors specific to a given sub-sector: the inability to start trains and run rail traffic due to the inability to construct the timetable for journeys exceeding 2 hours.
		Incident in rail transport (passengers)	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sub-sector: a) interruption of services by the carrier for more than 2 hours, or b) damage to information systems essential for the control and operation of the rail vehicle.
		Incident in rail transport (freights)	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sub-sector: a) interruption of services by the carrier for more than 6 hours, or b) damage to information systems essential for the control and operation of the rail vehicle.
	Water Transport	Incident concerning shipowners in sea transport of passengers, while sailing	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: the incident has damaged information systems essential for the control and operation of the ship, posing a threat to human health or life, the environment or property.
		Incident concerning shipowners in sea transport of passengers, during berth	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident prevented the provision of the essential service for a period longer than 48 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		An incident involving shipowners in the maritime transport of goods, during shipping	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to the sector or subsector concerned: the incident has damaged information systems essential for the control and operation of the ship, posing a risk to human health or life, the environment or property.
		Incident concerning shipowners in sea transport of goods ,while at berth	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident resulted in the inability to provide the essential service in more than 48 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Incident concerning shipowners in inland waterway transport passenger	1. Number of users affected by the disruption of the essential service: at least 30% of inland waterway passenger transport passengers per year, determined on the basis of GUS data from the previous year;

			2. Duration of impact of the incident on the essential service provided: the incident resulted in a lack of access to the ICT system for a period longer than 72 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Incident concerning shipowners in inland waterway transport of goods	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident resulted in a lack of access to the ICT system in more than 72 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Incident related to the functioning of the managing bodies of the ports	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident resulted in the inability to provide the essential service for more than 12 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Incident related to the security of port authorities	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other sector or subsector specific factors: the incident damaged information systems essential to the operation of the port, resulting in the inaccessibility of the port or the limited availability of the port.
		An incident involving the functioning of the managing bodies of port facilities	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident resulted in the inability to provide the essential service for a period longer than 12 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		An incident related to the security of port facility management bodies	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other sector or subsector specific factors: the incident has damaged information systems essential to the operation of the port facility, posing a threat to human health or life, the environment or property, or to the operation of the port.
		An incident related to the functioning of entities operating in the port area supporting maritime transport	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident resulted in the inability to provide the essential service for a period longer than 12 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		An incident related to the functioning of entities operating in the port	1. Number of users affected by the disruption of essential service: not applicable;

		area supporting maritime transport	2. Duration of impact of the incident on the essential service provided: the incident resulted in the inability to provide the essential service for a period longer than 12 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Incident related to the operation of VTS (Vessel Traffic Control Service)	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident resulted in the inability to provide the essential service for a period longer than 12 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		VTS safety incident (Vessel Traffic Control Service)	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or sub-sector: the incident caused damage to information systems essential for the functioning of the VTS Service, causing a threat to human health or life, the environment or property, or to the port operation.
	Road transport	Road management incident	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sub-sector: the incident caused the failure of traffic lights or the failure of other devices used to inform road users that resulted in an accident where the number of killed or injured exceeds 11.
		Intelligent Transport Systems incident	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given subsector: a) the incident caused the failure of traffic lights or the failure of other devices used to inform road users, as a result of which the accident occurred, where the number of killed or injured more than 11 people or tolls for tolls on national roads, representing financial losses exceeding PLN 10 million.
Banking and Financial market infrastructures		Incident related to the functioning of banks, credit institutions and financial market infrastructure	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of the incident's impact on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: a) the estimated financial loss exceeds EUR 5 million, or b) the incident would harm the interests of third parties, or c) the incident led to the activation of a contingency plan enabling restoration of operational readiness following an emergency.
		Transaction incident	1. Number of users affected by the disruption of service core service: not applicable; 2. Duration of the incident's impact on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable;

			4. Other sector or subsector specific factors: the incident covers 25% of the payments (in terms of number of transactions) or 5 million euros realized by a given entity[1]
		Incident relating to users of payment services	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other sector or subsector specific factors: the incident covers 50,000 users or 25% of payments made by users of the entity.
Health sector		Incident related to the National health insurance systems	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident led to the non-availability of the service for more than 24 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to the sector or subsector concerned: a) the incident led to the lack of confidentiality of the data processed in the service or b) the incident led to the lack of data integrity processed in the service.
		Incident relating to the provision of healthcare services	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of the incident's impact on the essential service provided: the incident led to a service unavailable for more than 24 hours 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: the incident caused at least one of the following circumstances: a) death of a person, b) serious damage to health, c) other than serious damage to health of more than one person, d) lack of confidentiality of data processed in the service, e) lack of integrity of data processed in the service.
		Incident concerning the collection and sharing of Electronic Medical Records	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident led to the non-availability of the service for more than 1 hour; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to the sector or subsector concerned: a) the incident led to the lack of confidentiality of the data processed in the service or b) the incident led to the lack of integrity of the data processed in the service.
		Epidemiological Data Management Incident	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident led to the non-availability of the service for more than 2 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to the sector or subsector concerned: a) the incident led to the lack of confidentiality of the data processed in the service or b) the incident led to the lack of integrity of the data processed in the service.

[1] Which is a) a credit institution referred to in Art. 4, sec. 1, point 17 of the Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe, Dz.U. 1997 Nr 140 poz. 939, b) a domestic bank referred to in Art. 4, sec. 1, point 1 of the Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe, Dz.U. 1997 Nr 140 poz. 939 , c) a branch of the credit institution referred to in Art. 4, sec. 1, point 18 of the Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe, Dz.U. 1997 Nr 140 poz. 939, d) a cooperative savings and credit union within the meaning of the Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, Dz. U. z 2012 r. poz. 855

		Incident related to the marketing and distribution of medicinal products	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident led to the non-availability of the service for more than 24 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: the incident caused at least one of the following circumstances: a) death of a person, b) serious damage to health, c) other than serious damage to health of more than one person, d) lack of confidentiality of data processed in the service, e) lack of integrity of data processed in the service.
		Incident concerning the command of units of the State Medical Rescue system	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: the incident led to the non-availability of the service for more than 1 hour; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: the incident caused at least one of the following circumstances: a) death of a person, b) serious damage to health, c) other than serious damage to health of more than one person, d) lack of confidentiality of data processed in service, e) lack of integrity of data processed in the service.
Drinking water supply and distribution		Incident concerning water consumption	1. Number of users affected by the disruption of essential service: the incident led to the unavailability of the service for at least 100,000 users for more than 8 hours; 2. Duration of the incident's impact on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Water treatment incident	1. Number of users affected by the disruption of essential service: the incident led to service unavailability for at least 100,000 users for more than 8 hours 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Water supply incident	1. Number of users affected by the disruption of essential service: the incident led to service unavailability for at least 100,000 users for more than 8 hours 2. Duration of the incident's impact on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Wastewater Discharge Incident	1. Number of users affected by the disruption of essential service: the incident led to service unavailability for at least 100,000 PE for more than 8 hours; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.

		Wastewater treatment incident	1. Number of users affected by the disruption of essential service: the incident led to service unavailability for at least 100,000 PE for more than 8 hours; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
Digital Infrastructure		Incident relating to the operation of an Internet Exchange Point (IXP)	1. Number of users affected by the disruption of service core service: not applicable; 2. Duration of the incident's impact on the essential service provided: unplanned unavailability of the service for at least 8 hours; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to a given sector or subsector: not applicable.
		Incident involving running an authoritative DNS server	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other factors specific to the sector or subsector concerned: unplanned unavailability of the service for more than 4 hours or an unauthorized change in the authoritative DNS server database.
		Incident involving maintaining a Top Level Domain Registry (TLD)	1. Number of users affected by the disruption of essential service: not applicable; 2. Duration of impact of the incident on the essential service provided: not applicable; 3. Geographical Coverage of the Incident Area: not applicable; 4. Other sector or subsector specific factors: a) unplanned loss of record management for at least 72 hours or b) unplanned unavailability of top-level domain DNS servers (TLDs) for more than 1 hour or c) unauthorized change to the DNS server database TLD Registry; or (d) an unauthorized change to the TLD Registry database.

Appendix 20: Policy Misfit in Finland

(Table made by author)

Policy Misfit

H1: *The higher is the policy misfit, the greater will be the extent of the modifications by Member States and the divergences upon transposition outcome.*			
Article	**Finland**		
	Degree of misfit	**Extent of Usage of 'Discretionary Room'**	**Hypothesis Test**
Art. 5 §2	Medium	Low	Reject
Art. 5 §3	Medium	Low	Reject
Art. 6 §1	Low	Medium	Reject
Art. 7 §1	Low	High	Reject
Art. 8 §1	Medium	High	Reject
Art. 8 §2	High	Medium	Confirmed
Art. 8 §5 al. 1	Medium	Low	Reject
Art. 9 §2	Low	Low	No indication
Art. 9 §3	Low	Low	No indication
Art. 14 §1	High	Low	Reject
Art. 14 §2	Low	Low	Reject
Art. 14 §3	High	Medium	Confirmed
Art. 14 §4	High	Low	Reject
Art. 14 §5 Al. 2	Low	Medium	Reject
Art. 15 §2	High	Medium	Confirmed
Art. 15 §4	High	Medium	Confirmed

Appendix 21: Policy Misfit in France

(Table made by author)

Policy Misfit

H1: *The higher is the policy misfit, the greater will be the extent of the modifications by Member States and the divergences upon transposition outcome.*			
Article	**France**		
	Degree of misfit	**Extent of Usage of 'Discretionary Room'**	**Hypothesis Test**
Art. 5 §2	High misfit	Medium	Confirmed
Art. 5 §3	High misfit	High	Confirmed
Art. 6 §1	High misfit	Medium	Confirmed
Art. 7 §1	Low misfit	Low	No indication
Art. 8 §1	Low misfit	Medium	Rejected
Art. 8 §2	Low misfit	High	Rejected
Art. 8 §5 al. 1	Low misfit	Low	No indication
Art. 9 §2	Low misfit	Low	No indication
Art. 9 §3	Low misfit	Low	No indication
Art. 14 §1	High misfit	High	Confirmed
Art. 14 §2	High misfit	High	Confirmed
Art. 14 §3	High misfit	Medium	Confirmed
Art. 14 §4	High misfit	Medium	Confirmed
Art. 14 §5 Al. 2	High misfit	Medium	Confirmed
Art. 15 §2	High misfit	High	Confirmed
Art. 15 §4	Low misfit	High	Rejected

Appendix 22: Policy Misfit in Greece

(Table made by author)

Policy Misfit

H1: *The higher is the policy misfit, the greater will be the extent of the modifications by Member States and the divergences upon transposition outcome.*			
Article	**Greece**		
	Degree of misfit	**Extent of Usage of 'Discretionary Room'**	**Hypothesis Test**
Art. 5 §2	High misfit	High	Confirmed
Art. 5 §3	High misfit	Medium	Confirmed
Art. 6 §1	High misfit	High	Confirmed
Art. 7 §1	High misfit	Medium	Confirmed
Art. 8 §1	High misfit	Medium	Confirmed
Art. 8 §2	High misfit	Medium	Confirmed
Art. 8 §5 al. 1	High misfit	Low	Rejected
Art. 9 §2	High misfit	Medium	Confirmed
Art. 9 §3	High misfit	Medium	Confirmed
Art. 14 §1	High misfit	High	Confirmed
Art. 14 §2	High misfit	High	Confirmed
Art. 14 §3	High misfit	Medium	Confirmed
Art. 14 §4	High misfit	High	Confirmed
Art. 14 §5 Al. 2	High misfit	High	Confirmed
Art. 15 §2	High misfit	High	Confirmed
Art. 15 §4	High misfit	High	Confirmed

Appendix 23: Policy Misfit in Ireland

(Table made by author)

Policy Misfit

H1: *The higher is the policy misfit, the greater will be the extent of the modifications by Member States and the divergences upon transposition outcome.*			
Article	**Ireland**		
	Degree of misfit	**Extent of Usage of 'Discretionary Room'**	**Hypothesis Test**
Art. 5 §2	High misfit	High	Confirmed
Art. 5 §3	High misfit	Medium	Confirmed
Art. 6 §1	High misfit	Medium	Confirmed
Art. 7 §1	High misfit	Medium	Confirmed
Art. 8 §1	High misfit	High	Confirmed
Art. 8 §2	High misfit	Low	Reject
Art. 8 §5 al. 1	Low misfit	Low	Reject
Art. 9 §2	High misfit	Medium	Confirmed
Art. 9 §3	High misfit	Medium	Confirmed
Art. 14 §1	High misfit	Medium	Confirmed
Art. 14 §2	High misfit	Medium	Confirmed
Art. 14 §3	High misfit	High	Confirmed
Art. 14 §4	High misfit	Medium	Confirmed
Art. 14 §5 Al. 2	High misfit	Medium	Confirmed
Art. 15 §2	High misfit	Medium	Confirmed
Art. 15 §4	High misfit	High	Confirmed

Appendix 24: Policy Misfit in Luxembourg

(Table made by author)

Policy Misfit

H1: *The higher is the policy misfit, the greater will be the extent of the modifications by Member States and the divergences upon transposition outcome.*			
Article	**Luxembourg**		
	Degree of misfit	**Extent of Usage of 'Discretionary Room'**	**Hypothesis Test**
Art. 5 §2	High misfit	Medium	Confirmed
Art. 5 §3	High misfit	High	Confirmed
Art. 6 §1	High misfit	High	Confirmed
Art. 7 §1	High misfit	Medium	Confirmed
Art. 8 §1	High misfit	High	Confirmed
Art. 8 §2	High misfit	High	Confirmed
Art. 8 §5 al. 1	High misfit	Medium	Confirmed
Art. 9 §2	Low misfit	Low	No indication
Art. 9 §3	Low misfit	Medium	Rejected
Art. 14 §1	High misfit	Medium	Confirmed
Art. 14 §2	High misfit	Medium	Confirmed
Art. 14 §3	High misfit	Medium	Confirmed
Art. 14 §4	High misfit	Medium	Confirmed
Art. 14 §5 Al. 2	High misfit	Medium	Confirmed
Art. 15 §2	High misfit	Medium	Confirmed
Art. 15 §4	High misfit	Medium	Confirmed

Appendix 25: Policy Misfit in Poland

(Table made by author)

Policy Misfit

H1: *The higher is the policy misfit, the greater will be the extent of the modifications by Member States and the divergences upon transposition outcome.*			
Article	**Poland**		
	Degree of misfit	**Extent of Usage of 'Discretionary Room'**	**Hypothesis Test**
Art. 5 §2	High misfit	Medium	Confirmed
Art. 5 §3	High misfit	High	Confirmed
Art. 6 §1	High misfit	High	Confirmed
Art. 7 §1	High misfit	Medium	Confirmed
Art. 8 §1	High misfit	High	Confirmed
Art. 8 §2	High misfit	Medium	Confirmed
Art. 8 §5 al. 1	Low misfit	Low	No indication
Art. 9 §2	High misfit	High	Confirmed
Art. 9 §3	High misfit	High	Confirmed
Art. 14 §1	High misfit	High	Confirmed
Art. 14 §2	High misfit	High	Confirmed
Art. 14 §3	High misfit	High	Confirmed
Art. 14 §4	High misfit	Medium	Confirmed
Art. 14 §5 Al. 2	High misfit	High	Confirmed
Art. 15 §2	High misfit	High	Confirmed
Art. 15 §4	High misfit	High	Confirmed

Appendix 26: Cross Countries Policy Misfit Analysis

(Table made by author)

Policy Misfit

H1: *The higher is the policy misfit, greater will be the use of the discretionary room by the Member state.*						
Article	**Hypothesis Test**					
	Finland	**France**	**Greece**	**Ireland**	**Luxembourg**	**Poland**
Art. 5 §2	Reject	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 5 §3	Reject	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 6 §1	Reject	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 7 §1	Reject	No indication	Confirmed	Confirmed	Confirmed	Confirmed
Art. 8 §1	Reject	Rejected	Confirmed	Confirmed	Confirmed	Confirmed
Art. 8 §2	Confirmed	Rejected	Confirmed	Reject	Confirmed	Confirmed
Art. 8 §5 al. 1	Reject	No indication	Rejected	Reject	Confirmed	No indication
Art. 9 §2	No indication	No indication	Confirmed	Confirmed	No indication	Confirmed
Art. 9 §3	No indication	No indication	Confirmed	Confirmed	Rejected	Confirmed
Art. 14 §1	Reject	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 14 §2	Reject	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 14 §3	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 14 §4	Reject	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 14 §5 Al. 2	Reject	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 15 §2	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed	Confirmed
Art. 15 §4	Confirmed	Rejected	Confirmed	Confirmed	Confirmed	Confirmed
Result	**Rejected**	**Confirmed**	**Confirmed**	**Confirmed**	**Confirmed**	**Confirmed**

Appendix 27: Average ranks and scores of corporatism in 42 countries

Source: *Detlef, J. (2016). Changing of the guard: trends in corporatist arrangements in 42 highly industrialized societies from 1960 to 2010. Socio-Economic Review, 14:(1), 47–71*

Average ranks and scores of corporatism in 42 countries (indices are z-standardized)

Rank	Country	Mean	Minimum	Maximum	Standard deviation	Years covered
1	Austria	2.06	1.61	2.38	0.20	1960–2010
2	Sweden	1.26	0.72	1.56	0.27	1960–2010
3	Belgium	1.21	0.72	1.57	0.20	1960–2010
4	Netherlands	1.08	0.58	1.65	0.30	1960–2010
5	Norway	1.03	0.37	1.92	0.34	1960–2010
6	Germany	1.01	0.91	1.25	0.11	1960–2010
7	Finland	0.99	−0.79	1.70	0.85	1960–2010
8	Slovenia	0.96	−0.07	1.61	0.63	1990–2010
9	South Africa	0.96	0.90	0.97	0.02	1994–2010
10	Denmark	0.68	0.08	0.99	0.23	1960–2010
11	Spain	0.59	0.06	1.08	0.32	1978–2010
12	Singapore	0.56	−0.08	0.92	0.35	1960–2010
13	Greece	0.43	0.09	0.61	0.15	1974–2010
14	Luxembourg	0.24	−0.44	0.73	0.46	1960–2010
15	Chile	0.13	−0.16	0.32	0.21	1989–2010
16	Israel	0.09	−0.81	2.05	0.92	1960–2010
17	Portugal	−0.02	−0.63	0.57	0.41	1976–2010
18	Slovakia	−0.09	−0.64	0.35	0.28	1990–2010
19	Italy	−0.11	−0.68	0.52	0.46	1960–2010
20	Switzerland	−0.20	−0.45	−0.04	0.17	1960–2010
21	Australia	−0.22	−1.21	1.02	0.64	1960–2010
22	France	−0.23	−0.42	−0.09	0.08	1960–2010
23	South Korea	−0.27	−0.59	0.33	0.28	1987–2010
24	India	−0.43	−0.51	−0.39	0.05	1960–2010
25	Ireland	−0.46	−1.57	0.99	0.91	1960–2010
26	Cyprus	−0.52	−0.57	−0.28	0.09	1990–2010
27	Brazil	−0.55	−0.55	−0.55	0.00	2000–2010
28	New Zealand	−0.55	−1.31	−0.06	0.41	1960–2010
29	Czech Rep.	−0.59	−0.95	−0.28	0.19	1990–2010
30	Bulgaria	−0.73	−0.97	−0.29	0.24	1992–2010
31	Romania	−0.76	−1.05	−0.16	0.29	1993–2010
32	Latvia	−0.80	−1.01	−0.25	0.24	1993–2010
33	Lithuania	−0.90	−1.31	−0.60	0.23	1993–2010
34	Mexico	−0.91	−0.91	−0.91	0.00	1997–2010
35	Hungary	−0.93	−1.61	−0.40	0.36	1990–2010
36	Japan	−1.03	−1.10	−0.90	0.05	1960–2010
37	Poland	−1.03	−1.31	−0.66	0.16	1990–2010
38	Estonia	−1.13	−1.65	−0.50	0.46	1991–2010
39	Malta	−1.21	−1.27	−1.20	0.02	1990–2010
40	U. Kingdom	−1.33	−1.80	−0.07	0.49	1960–2010
41	Canada	−1.55	−1.62	−1.41	0.06	1960–2010
42	United States	−1.65	−1.77	−1.50	0.10	1960–2010

Appendix 28: ‘Government effectiveness’ indicator

Source: *World Bank (https://databank.worldbank.org/source/worldwide-governance-indicators#)*

Country	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Austria	1,67	1,84	1,62	1,58	1,59	1,57	1,48	1,51	1,46	1,45	1,49
Belgium	1,57	1,58	1,66	1,60	1,61	1,38	1,44	1,33	1,18	1,17	1,03

Bulgaria	0,17	0,11	0,11	0,14	0,16	0,08	0,21	0,30	0,26	0,27	0,34
Croatia	0,60	0,62	0,56	0,71	0,70	0,69	0,51	0,49	0,57	0,46	0,41
Cyprus	1,42	1,53	1,56	1,39	1,37	1,14	1,05	0,96	0,92	0,92	0,99
Czech Republic	0,88	0,91	0,93	0,93	0,89	1,02	1,05	1,04	1,01	0,92	0,89
Denmark	2,23	2,10	2,10	1,98	1,99	1,82	1,85	1,88	1,80	1,87	1,94
Estonia	1,01	1,09	1,08	0,95	0,97	1,02	1,07	1,09	1,11	1,19	1,17
Finland	2,23	2,23	2,24	2,22	2,17	2,00	1,81	1,83	1,94	1,98	1,93
France	1,48	1,43	1,36	1,34	1,48	1,40	1,44	1,41	1,35	1,48	1,38
Germany	1,58	1,57	1,55	1,59	1,54	1,73	1,74	1,73	1,72	1,62	1,59
Greece	0,62	0,56	0,51	0,32	0,46	0,40	0,26	0,23	0,31	0,34	0,41
Hungary	0,67	0,67	0,67	0,63	0,65	0,53	0,50	0,46	0,52	0,49	0,50
Iceland	1,64	1,59	1,58	1,49	1,49	1,49	1,49	1,39	1,45	1,47	1,52
Ireland	1,34	1,35	1,46	1,55	1,49	1,60	1,53	1,33	1,29	1,42	1,28
Italy	0,42	0,44	0,38	0,42	0,46	0,37	0,45	0,53	0,50	0,41	0,46
Latvia	0,62	0,71	0,70	0,84	0,89	0,96	1,09	1,01	0,90	1,04	1,11
Lithuania	0,69	0,74	0,70	0,83	0,83	0,98	1,18	1,07	0,97	1,07	1,04
Luxembourg	1,75	1,72	1,75	1,67	1,63	1,65	1,72	1,69	1,68	1,78	1,73
Netherlands	1,74	1,73	1,79	1,81	1,78	1,82	1,83	1,83	1,85	1,85	1,80
Poland	0,53	0,64	0,62	0,68	0,72	0,83	0,80	0,71	0,64	0,66	0,60
Portugal	1,16	1,01	0,95	1,04	1,23	0,99	1,22	1,21	1,33	1,21	1,15
Romania	-0,36	-0,27	-0,33	-0,31	-0,07	-0,03	-0,06	-0,17	-0,17	-0,25	-0,28
Slovak Republic	0,87	0,84	0,83	0,84	0,79	0,88	0,84	0,89	0,80	0,71	0,67
Slovenia	1,15	1,03	0,99	1,03	1,01	1,01	0,97	1,13	1,17	1,13	1,08
Spain	0,95	0,99	1,03	1,12	1,15	1,16	1,17	1,12	1,03	1,00	1,00
Sweden	2,05	2,00	1,97	1,96	1,91	1,80	1,82	1,77	1,84	1,83	1,83
Ukraine	-0,83	-0,78	-0,82	-0,58	-0,65	-0,41	-0,52	-0,57	-0,46	-0,42	-0,30
United Kingdom	1,51	1,57	1,56	1,55	1,50	1,63	1,74	1,60	1,41	1,34	1,44

Table of Contents