Détection, analyse contextuelle et visualisation de cyber-attaques en temps réel : élaboration de la Cyber Situational Awareness du monde maritime

Olivier Jacq

DOCTORAT BRETAGNE LOIRE / MATHSTIC

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

THESE DE DOCTORAT DE

L'ÉCOLE NATIONALE SUPERIEURE MINES-TELECOM ATLANTIQUE
BRETAGNE PAYS DE LA LOIRE - IMT ATLANTIQUE

ECOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies de l'Information et de la Communication
Spécialité : *Informatique*

Par
Olivier JACQ

Détection, analyse contextuelle et visualisation de cyberattaques en temps-réel : élaboration de la *Cyber Situational Awareness* du monde maritime

Thèse présentée et soutenue à Brest, le 11 janvier 2021
Unité de recherche : Lab-STICC – UMR CNRS 3285
Thèse N° : 2021IMTA0228

Rapporteurs avant soutenance :

Nora Boulahia-Cuppens	Professeur, École Polytechnique de Montréal
Joaquín García-Alfaro	Professeur, Institut Mines-Télécom et Institut Polytechnique de Paris

Composition du Jury :

Président :	Joaquín García-Alfaro	Professeur, Institut Mines-Télécom et Institut Polytechnique de Paris
Examinateurs :	Nora Boulahia-Cuppens	Professeur, École Polytechnique de Montréal
	David Brosset	Maître de conférences, Arts et Métiers Sciences et Technologies
	Jacques Simonin	Directeur d'études, Institut Mines-Télécom Atlantique Bretagne Pays de la Loire
	Patrick Hébrard	Responsable recherche cyber et innovation, Naval Group
Dir. de thèse :	Yvon Kermarrec	Professeur, Institut Mines-Télécom Atlantique Bretagne Pays de la Loire

Invité

Laurent Aufrechter	Ingénieur cybersécurité, Thales

Table des matières

Table des figures

Liste des tableaux

Remerciements

Mes premiers remerciements vont à mes encadrants de thèse : David Brosset et Jacques Simonin, ainsi qu'à mon directeur de thèse Yvon Kermarrec. Leur soutien et leur grande expérience ont été des amers particulièrement remarquables pour prendre le bon cap dès l'appareillage de cette thèse et pour m'aligner sur les bonnes thématiques de recherche. En « vieux » loups de mer de la recherche, ils m'ont transmis leurs conseils avisés lors de la relecture de cette thèse et des articles publiés. Le profane que je suis vous remercie de l'avoir fait naviguer sereinement sur les fabuleux océans de la recherche.

Merci aux relecteurs de ce manuscrit, Nora Boulahia Cuppens et Joaquín García-Alfaro, pour avoir accepté cette mission malgré un emploi du temps déjà saturé de relectures en cette fin d'année 2020. Je tiens également à remercier les membres du jury de thèse pour leur présence dans ces circonstances sanitaires particulières, pour leur lecture attentive de ces travaux, ainsi que pour les remarques qu'ils m'adresseront et qui me permettront de m'améliorer pour mes recherches futures.

Je remercie également la Marine nationale, mon employeur, pour m'avoir permis de progresser tout au long de mes 27 années d'engagement. Difficile de citer tout le monde, mais je remercie notamment Fabrice, Daniel, Mathieu, Julien, Olivier, Thomas, Eric, Erwan, François-Régis, Xavier, Gladys, Emmanuel, Lionel, Fabien, Loïc, Florian, Alexis, Maxime, Cédric, Laurent, François, Jean-Eudes, Hervé, Marion, Dominique et vous toutes et tous, cybercombattantes et cybercombattants qui, au quotidien, œuvrez dans le silence et la discrétion pour améliorer la cybersécurité de la Marine. Merci de votre soutien et de votre confiance : ce travail de thèse a pu impacter ma disponibilité pour travailler et échanger avec vous au quotidien, mais c'était pour une bonne cause ! Gardez le cap !

Merci à ceux qui ont cru en l'intérêt de créer une chaire de cyberdéfense spécifique au monde naval à l'École navale, ainsi qu'un Mastère Spécialisé ® en cybersécurité maritime et portuaire, je pense notamment au vice-amiral d'escadre Hello, au vice-amiral Pagès et

au contre-amiral Baudonnière. Je tiens tout particulièrement à remercier les membres de la chaire de cyberdéfense de l'École navale, dont la bonne humeur et les conseils sans fin m'ont conforté dans mon travail quotidien. Merci aussi aux autres doctorants : Clet, Pedro, Guillaume, Bastien, Arthur, Étienne, Benjamin, Xavier, Maël, Paul, Nico, Douraid : cela a été un plaisir de passer ces trois années avec vous, trop souvent à temps partiel. Merci beaucoup Mallorie et Perrine, nos chargées de communication successives, pour votre dynamisme et pour avoir tant contribué au rayonnement de la chaire ! Mickaël, Maxence, vous avez réalisé un superbe travail pour faire d'une pile de cartons une plate-forme d'automates fonctionnelle et réaliste ! Je remercie également l'Institut de recherche de l'École navale, les enseignants-chercheurs de l'École ainsi que le personnel de l'École navale qui ont assuré la majeure partie du soutien de cette thèse.

Merci à Mickaël Hauspie et Frédéric Cuppens pour leur participation à mon comité de suivi individuel de thèse et pour leurs suggestions avisées. Vous m'avez tous deux permis de clarifier ma pensée parfois embrouillée. Merci également au personnel d'IMT Atlantique Bretagne Pays de la Loire et notamment au laboratoire UMR CNRS 6285 Lab-STICC pour votre accueil au cours de ces trois années. Invités lors des journées scientifiques, vous avez su répondre présents et, par vos remarques et conseils bibliographiques et académiques, m'avez permis de faire avancer ma réflexion.

Enfin, je remercie bien sûr ma famille, qui a accepté tant bien que mal les sacrifices d'emploi du temps très importants liés à cette thèse tardive. À mes enfants : oui votre père sera docteur mais non, il ne portera pas de blouse blanche toute la journée et ne pourra pas vous vacciner contre les écrans (quoi que !). Il essaiera de continuer à être le même, en moins fatigué ! Merci aussi à tous ceux qui m'ont soutenu avec leur sempiternelle question sur la date de ma soutenance, bienvenue pour préciser officiellement les priorités de mon agenda ! Merci notamment au Djeuns, au Colonel et au Belge et à Frédéric pour leur soutien !

Ces remerciements ne peuvent s'achever sans une pensée pour ma première fan : ma mère ! Sa présence et ses encouragements ont été pour moi les piliers fondateurs de l'homme que je suis, de ses valeurs et de son engagement dans la vie.

Dans ce monde où tout est rapidité, urgence, stress, performance, réorganisation, notation, virtuel, ce travail de thèse a eu une vocation cathartique, m'apportant un recul indéniable et bénéfique et une projection sur des domaines en pleine construction. Elle m'a aussi permis une réflexion sur moi-même, mon parcours à mi-vie et mes envies pour le futur.

Chapitre I

Introduction

We are drowning in information, while starving for wisdom. E.O. Wilson, 1929

20 février 2020 : un paquebot avec 8 000 passagers et membres d'équipage transite en Méditerranée. Alors que les croisiéristes s'affairent à leurs activités ludiques, le navire fait l'objet d'une « prise d'otages numérique ». La cellule de crise de l'armateur est activée, les plus hautes instances de l'État sont prévenues : le capitaine ne peut plus manœuvrer et l'ensemble des écrans de la passerelle et du poste de contrôle de la machine affichent un message sans équivoque : l'armateur doit payer une rançon élevée, faute de quoi le navire ira s'échouer sur la côte à pleine vitesse. Scénario d'un mauvais film hollywoodien ? Peut-être. Incident déjà survenu ? On ne le saura probablement jamais. Événement redouté présent dans les analyses de risques de ces navires ? On l'espère.

En France, le transport maritime fait partie des secteurs d'activité d'importance vitale (SAIV) [1]. Sur les dernières années, l'amélioration du niveau de cybersécurité des secteurs d'activité d'importance vitale apparaît sensible, suite aux travaux de réglementation du Secrétariat Général de la Défense et de la Sécurité nationale (SGDSN) et plus particulièrement au dynamisme de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Dorénavant, des processus existent pour assurer la remontée d'un évènement cyber maritime dans le cadre de la Coopération Navale Volontaire (CNV) [2]. Pourtant, plusieurs études s'accordent pour souligner que le niveau de cybersécurité du secteur maritime reste insuffisant [DiR15, Tam19]. Ce constat, partagé par des acteurs français, européens et internationaux de la cybersécurité nous a interpellé. En raison du coût de transport plus faible qu'il offre, le secteur maritime constitue le premier mode de transport mondial pour les biens de consommation : ainsi, en 2019, il représentait plus des $4/5^{\text{èmes}}$ du trafic de marchandises mondial en

1. http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf
2. Lire notamment http://www.sgdsn.gouv.fr/uploads/2018/08/20180627-instruction-interministerielle-nxx-230-surete-maritime-portuaire.pdf et http://www.sgdsn.gouv.fr/uploads/2019/05/20190429-sgdsn-iim-165-cooperation-navale-volontaire-vf.pdf

volume [SHJ+19]. Des vulnérabilités cyber exploitées par des attaquants pourraient, compromettre des pans entiers de l'économie en causant un déni d'accès à de nombreuses matières premières ou manufacturées. Ce constat a fortement motivé l'ensemble de nos travaux : nous avons donc axé nos efforts de recherche sur la conception de modèles et de solutions qui permettent d'améliorer concrètement les capacités de détection et d'analyse d'évènements cyber dans le milieu maritime et de renforcer la sécurité maritime dans son ensemble.

Contexte de l'étude

Avec l'arrivée du numérique, le secteur maritime vit, depuis une dizaine d'années, une transformation en profondeur et durable des navires, infrastructures portuaires, de leurs équipements et de leurs modes de fonctionnement. Le secteur mue comme l'ont fait d'autres secteurs avant lui, mais à son propre tempo, plutôt lent, lié au long cycle de vie des navires et infrastructures portuaires. Si les passerelles des navires plus anciens conservent encore une mixité entre commutateurs, boutons, écrans analogiques et informatique, les infrastructures portuaires récentes et les constructions neuves sont d'ores et déjà beaucoup plus numérisées et les premiers essais à la mer de navires autonomes sont devenus une réalité [Lev17]. Cette évolution majeure se retrouve également dans le secteur maritime militaire. Au sein d'une marine moderne, plus aucune opération d'envergure ne pourrait être réalisée sans recours au numérique. Avantage stratégique pour la connaissance et l'anticipation, la dissuasion, la protection, la prévention et l'intervention, le numérique a démultiplié les capacités de nos forces armées.

Les systèmes d'information maritimes qui participent à ces opérations numérisées présentent une surface d'attaque importante, notamment en raison de leur interconnexion, et se retrouvent aussi bien exposés à des attaques qui proviennent de sources de menaces liées à la cybercriminalité qu'à des ressources de niveau étatique. Parfois mal conçus, mal exploités, fragilisés par la nature faillible des solutions logicielles, les systèmes maritimes peuvent souffrir de faiblesses organisationnelles, environnementales, humaines, technologiques ou techniques. Lorsque ces vulnérabilités sont combinées et exploitées par des personnes mal intentionnées ou par accident, le fonctionnement des systèmes d'information et des installations peut être directement touché. Le spectre des conséquences est vaste, de la simple infection virale bénigne à des impacts cyber physiques, environnementaux, humains, à la destruction d'installations, voire à la compromission de la conduite d'une action militaire.

Les moyens de cybersécurité se déploient progressivement au sein de certains systèmes d'information maritimes. Ils s'appuient sur trois piliers : la cyberprotection, la cyberdéfense et la cyber résilience. La cyberprotection correspond aux mesures organisationnelles et techniques de défense en profondeur qui permettent de renforcer un système lors des phases de conception et d'exploitation, pour garantir un haut niveau de sécurité. La cyberdéfense regroupe l'ensemble des moyens qui permettent d'assurer la détection et la réponse à un évènement de cybersécurité [3]. La cyber résilience apporte les moyens de Maintien en Conditions de Sécurité (MCS), pour apporter des capacités de mise à jour régulière, de correction des vulnérabilités des systèmes et, *in fine*, de continuité et de reprise d'activité en cas d'évènement de cybersécurité. Si l'apport de cette thèse se concentre essentiellement sur la cyberdéfense, une partie des conclusions de recherche et des informations obtenues peuvent concourir à améliorer la cyberprotection et la cyber résilienc des systèmes maritimes. Elles peuvent également être extrapolées pour servir d'autres domaines d'emploi, comme les véhicules autonomes ou les objets connectés. L'amélioration notable des capacités de collecte, d'analyse et de compréhension d'évènements cyber apportée par notre modèle permet également de répondre à des problématiques de détection d'anomalies, comme l'usure prématurée d'installations cyber physiques, ou la valorisation de données opérationnelles, localement ou à distance.

Cadre théorique de la recherche

Les difficultés de mise en œuvre des mesures traditionnelles de cybersécurité à bord des navires et des infrastructures maritimes trouvent leurs origines dans trois problématiques spécifiques au milieu. La première est liée au cycle de vie particulièrement long des navires. Un navire ou un système industriel présent sur une infrastructure portuaire sont conçus pour être exploités plusieurs dizaines d'années, avec une refonte possible à mi-vie. Cette échelle de temps long se heurte avec la réalité opérationnelle du quotidien pour optimiser l'exploitation du navire, mais aussi avec sa phase de conception qui ne peut souffrir de retard, sous peine de conséquences économiques importantes. La multiplicité des acteurs (chantiers navals, opérateur, maintenancier...) complexifie également l'optimisation du cycle de vie. Dans un cyberespace dynamique, aux menaces et aux évolutions permanentes, l'obsolescence des systèmes est donc une réalité avec laquelle il faut vivre. Concrètement, il est ainsi souvent

3. Par évènement de cybersécurité, on entendra une situation inattendue et non conforme dans le cyberespace, volontaire ou involontaire, qui pourraient avoir un impact sur le fonctionnement ou l'intégrité du système, des données qu'il contient ou des installations dont il assure la conduite.

impossible de mettre à jour et sécuriser l'ensemble des systèmes pour faire face aux menaces : il convient d'identifier d'autres parades pour les protéger. La seconde problématique est liée à l'intégration de systèmes maritimes hétérogènes et à leur interconnexion nécessaire à l'exploitation opérationnelle : le navire est un système de systèmes complexes. Il convient d'acquérir une vision globale et exhaustive de ses systèmes dès la conception, puis tout au long du cycle de vie du navire et de ses évolutions [For13]. Les solutions de cyberprotection classiques s'adaptent aussi difficilement au milieu particulièrement contraint des systèmes d'information maritimes, car ils ne prennent pas en compte leurs spécificités *a priori*. Enfin, hormis dans de très rares cas, aucun spécialiste en informatique, réseau et encore moins en cyberdéfense n'est présent à bord. Le secteur maritime est donc confronté à une multitude de verrous, organisationnels et technologiques, endogènes et exogènes, qui freinent l'intégration d'une cybersécurité efficace à bord de navires de plus en plus complexes et numérisés.

Aucune réponse ne saurait être considérée comme parfaite, car ce constat souligne des difficultés durables, structurelles, parfois exogènes : il est ainsi déraisonnable d'émettre l'hypothèse qu'un jour, le navire sera moins numérisé ou que des experts cyber seront présents en permanence à bord de tous les navires. Dans le cadre de cette thèse, tout en suivant délibérément une approche holistique, nous avons souhaité nous orienter sur la détection, la collecte, l'analyse et la compréhension d'évènements cyber dans un contexte maritime. Cette capacité pourrait en effet permettre d'anticiper, de détecter rapidement et d'apporter une compréhension et une réponse à la suite d'évènements qui aboutit au scénario catastrophe présenté en début d'introduction. En effet, si des travaux ont déjà été réalisés ou se poursuivent sur les sujets relatifs à la cyberprotection ou la cyber résilience des systèmes d'information, la centralisation d'évènements de cyberdéfense dans un contexte maritime à des fins de détection reste un domaine de recherche encore peu développé à l'heure actuelle. Cette thèse, qui se concentre sur les enjeux de la cyberdéfense maritime, apporte une réponse éprouvée sur le terrain et qui a fait l'objet de plusieurs publications lors de conférences internationales. En mettant en œuvre la cybersurveillance des systèmes d'information maritimes, la détection temps-réel des menaces et l'évaluation des risques prennent une dimension concrète, facilitant la défense et le traitement des évènements cyber et améliorant la sécurité maritime dans son ensemble.

Questions de recherche

Dans le contexte maritime, le problème de recherche qui motive cette thèse est avant tout d'améliorer la qualité et la rapidité de détection, de compréhension et de réaction face à une menace cyber. Pour répondre à cette problématique, trois questions de recherche ont été identifiées pour étayer cette thèse.

1. QR1 : Architecture de collecte et modélisation : quels sont les processus à concevoir, développer et mettre en œuvre pour permettre la détection d'anomalie sur des systèmes distants et hétérogènes qui disposent de circuits de télécommunications contraints ? Quelle modélisation globale pourrait être retenue pour créer une connaissance à partir des données collectées ? Le premier objectif poursuivi dans cette thèse sera de démontrer que le concept de *situational awareness* appliqué à la cybersécurité maritime permet de répondre à ces enjeux. Notre travail aura aussi pour objectif d'attester que les verrous liés à la collecte, à la normalisation, à la fusion et à la visualisation de données multi-capteurs peuvent être résolus.
2. QR2 : Analyse et représentation des données : quelles sont les modalités de traitement, d'analyse et de présentation des données pour disposer d'une visualisation pertinente et compréhensible de la situation d'une flotte de navires à des fins de suivi, de projection, de partage et d'aide à la décision ? Face à la masse de données collectée par les multiples capteurs, nos travaux doivent identifier les outils pertinents de visualisation et d'analyse afin de disposer d'une compréhension d'ensemble du contexte pour faciliter la prise de décision humaine.
3. QR3 : Détection d'anomalies dans un contexte maritime : le monde maritime utilise des protocoles parfois peu sécurisés par conception, peu évolutifs et vulnérables à une multitude d'attaques. Comment détecter des anomalies dans ce contexte ? Nous proposons d'appliquer les technologies de détection à un système et à des standards spécifiques au monde maritime et de présenter de manière simplifiée l'information de détection à leurs exploitants.

Démarche adoptée et apports de la thèse

Dans la cadre de la première question de recherche sur l'architecture de collecte et la modélisation, nous nous sommes concentrés sur la notion de situation : l'homme qui fait face à des évènements, des circonstances et des relations entre objets se trouve face à

une situation. Les recherches liées à la perception, la compréhension et la projection de la situation ont permis de retenir le concept de *Situational Awareness (SA)*, déjà utilisé pour d'autres domaines de lutte. Nous nous sommes appuyés sur ces travaux pour définir le concept de *Maritime Cyber Situational Awareness (MCSA)*. En premier lieu, nous avons précisément modélisé les différents processus qui permettent d'aboutir à cet état de connaissance que permet la MCSA. Par la suite, en partant des informations nécessaires à l'élaboration de ces processus, nous avons défini une architecture adaptée au monde maritime afin d'assurer leur collecte à bord et leur transfert vers la terre. Afin d'évaluer nos travaux, nous avons directement participé à la création d'une plate-forme expérimentale, dont l'un des objectifs était d'intégrer les caractéristiques spécifiques du milieu, comme les contraintes liées aux raccordements par satellite ou la variété des systèmes embarqués. Enfin, pour permettre la prise de décision adéquate, ces informations doivent faire montre d'un niveau de qualité élevé, se basant sur plusieurs critères que nous avons également précisément définis. Le concept de MCSA pour le secteur maritime et les navires du futur a fait l'objet de plusieurs articles et publications dans des revues ou conférences internationales.

Pour répondre à la deuxième question de recherche sur l'analyse et la représentation des données, nous avons travaillé sur la détection d'anomalies dans un contexte maritime, la compréhension du chemin d'attaque et la participation à la remédiation en aidant l'utilisateur à visualiser et comprendre les évènements dans leur contexte. Nos travaux de recherche ont notamment apporté des réponses sur les évolutions nécessaires sur les capteurs réseau pour permettre la réalisation de cartographies dynamiques. Nous avons également élaboré des tableaux de bord dynamiques et contextuels, permettant d'afficher des situations tactiques selon plusieurs dimensions, en fonction des besoins des opérateurs et du niveau d'abstraction attendu. La cartographie et l'identification de chemins d'attaque dynamiques dans un contexte de traitement de données en masse en temps réel représentent des apports importants pour le domaine de recherche. Ces travaux ont fait l'objet de plusieurs publications scientifiques et d'améliorations du code source de capteurs.

Enfin, la troisième question de recherche relative à la détection d'anomalies dans un contexte maritime nous a permis de définir une architecture de détection temps-réel sur des systèmes et protocoles spécifiques. Nous avons été en mesure d'identifier et de démontrer les faiblesses de certains standards utilisés à bord des navires. Nous avons proposé et expérimenté des capacités avancées de détection et d'alerte de l'opérateur du système ou y avons directement contribué.

L'engagement des différents acteurs sollicités dans le cadre de cette thèse et un contexte

favorable nous ont permis de valider l'ensemble de ces apports en réalisant une mise en œuvre opérationnelle de nos travaux sur une architecture dédiée et réaliste : le *Naval Cyber Range* de l'École navale, développé en parallèle de cette thèse. Le retour d'expérience particulièrement précieux nous a été essentiel pour valider notre méthodologie, nos propositions et vérifier la conformité et la réalité de nos apports. En effet, en parallèle de la création du *Naval Cyber Range*, nous avons mis en œuvre une architecture globale de cybersurveillance représentative de ce qui pourrait être déployé à bord d'un navire et d'un centre à terre pour assurer la cybersécurité d'un navire ou d'une flotte de navires. L'instrumentation du *Naval Cyber Range* en tant que prototype nous a permis, d'une part, de générer des métadonnées de cybersécurité et de les collecter afin d'effectuer nos mesures de qualité et, d'autre part, de mener nos travaux sur les questions d'analyse, de visualisation et de détection d'anomalie sur des systèmes maritimes particulièrement proches de la réalité, afin de vérifier la conformité de nos travaux de recherche.

Les domaines de recherche traités dans le cadre de nos travaux sont synthétisés en figure I.1.

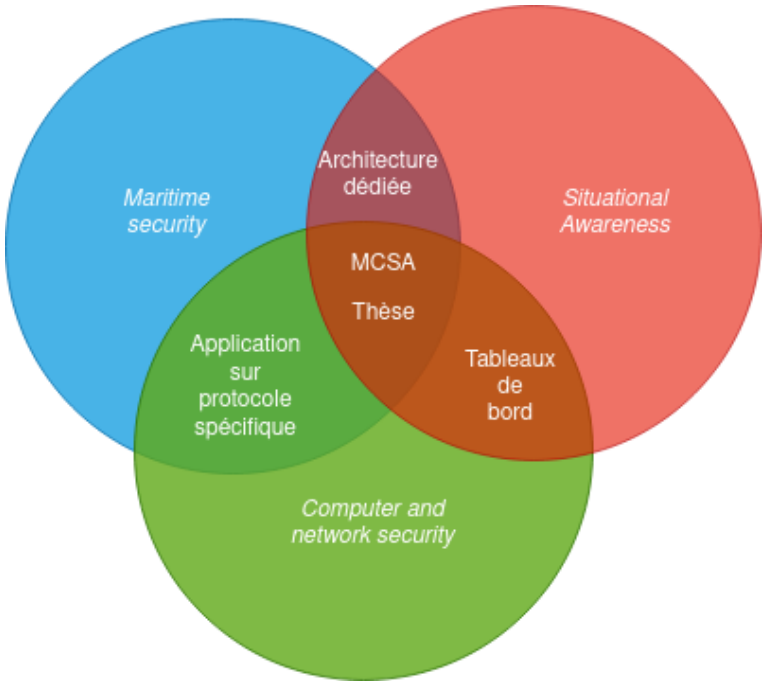

FIGURE I.1 : Domaines de recherche de la présente thèse (source : archives personnelles).

Plan du manuscrit

Le manuscrit est composé de cinq chapitres (figure I.2).

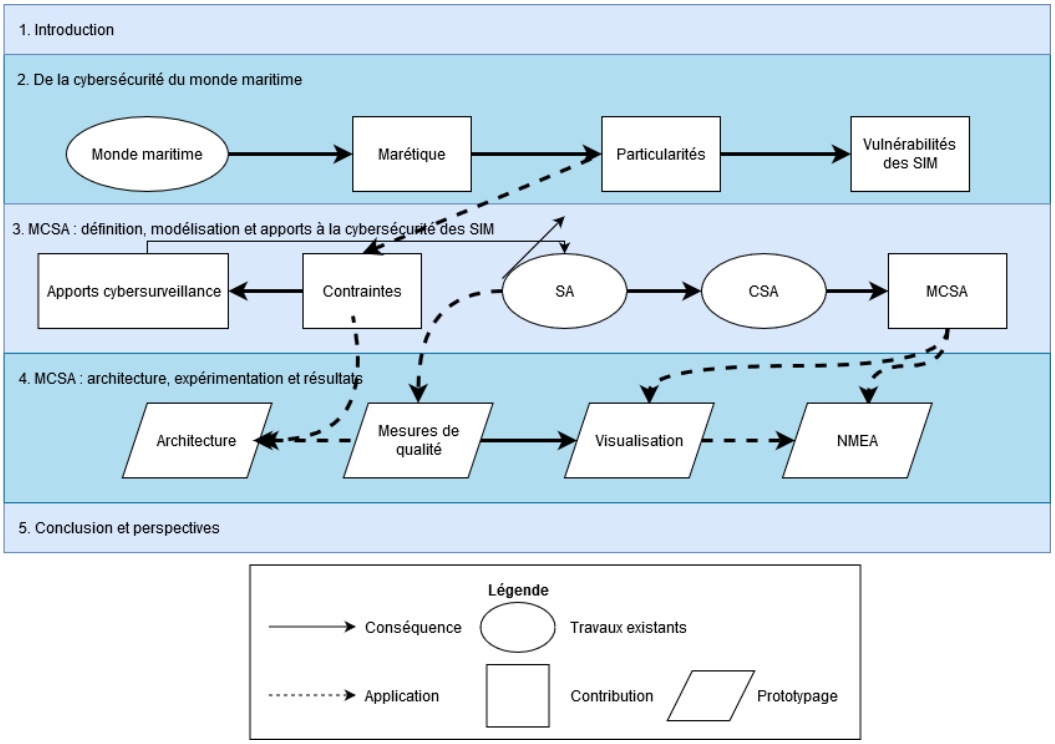

FIGURE I.2 : Description des relations entre les chapitres du manuscrit de la présente thèse (source : archives personnelles).

Après avoir dressé un état de l'art succinct du monde maritime, de ses systèmes d'information et de leur cybersécurité au chapitre 2, nous décrirons lors du chapitre 3 les points durs rencontrés pour la conception d'une architecture de cybersurveillance maritime, ainsi que les apports de nos travaux pour modéliser une architecture qui réponde aux différentes contraintes. Au chapitre 4, nous détaillerons les résultats obtenus sur plate-forme expérimentale et identifierons les moyens nécessaires à l'analyse et à la présentation contextuelle des données comme une aide à la décision, ainsi que les apports identifiés dans le domaine de la visualisation des données pour un centre opérationnel de cybersurveillance maritime. Enfin, nous y présenterons nos travaux et résultats relatifs à la détection d'anomalies dans le contexte maritime. Au chapitre 5, la conclusion dressera un bilan de l'apport de notre travail de recherche sur les verrous scientifiques identifiés et ouvrira les enjeux vers plusieurs perspectives de recherche, notamment sur les navires et de manière plus générale, sur les véhicules autonomes et sur l'applicabilité des travaux à d'autres domaines contraints, comme à l'Internet des objets.

Chapitre II

De la cybersécurité du monde maritime

Dans ce chapitre, nous rappelons les grandes caractéristiques du secteur maritime civil et militaire et les raisons de son importance stratégique pour la France. La transformation numérique du secteur est ensuite détaillée, en précisant les origines de cette transformation et en expliquant l'emploi des systèmes d'information maritimes. Puis, les particularités de la marétique sont identifiées et quelques perspectives d'évolutions à court et moyen terme dressées. Enfin, nous listons les vulnérabilités et évènements redoutés du domaine.

II.1 L'importance stratégique du secteur maritime en France

Après avoir brossé un portrait du secteur maritime mondial sous ses aspects géographiques et géopolitiques, nous aborderons les particularités de la France dans ce domaine, sous les aspects civils et militaires.

II.1.1 Le monde maritime

Les océans couvrent 71 % de la surface du globe. Historiquement, l'homme les exploite pour le transport de marchandises et de passagers, mais aussi pour s'en approprier les ressources halieutiques, pétrolières ou gazières. L'emploi des capacités maritimes pour le transport de quantités importantes de marchandises constitue un moyen efficace et économique. C'est une des raisons pour lesquelles 90 % du volume du trafic de marchandises emprunte la voie maritime [oS]. Pour réduire encore le coût induit par ce mode de transport,

le secteur maritime conçoit puis exploite des navires toujours plus grands. C'est ainsi que les plus grands portes-conteneurs construits aujourd'hui sont capables de transporter plus de 23 000 conteneurs [Ins]. La figure II.1 montre l'évolution du tonnage des navires au cours des trente dernières années. L'augmentation du tonnage global sur les dernières années est particulièrement significative. Ainsi, une récente étude de l'Organisation de coopération et de développement économiques (OCDE) indique des augmentations remarquables des tonnages sur la période 1996 à 2015, notamment pour les porte-containers (+80 %), les vraquiers (+60 %) et les navires à passagers (+30 %) [Mer15].

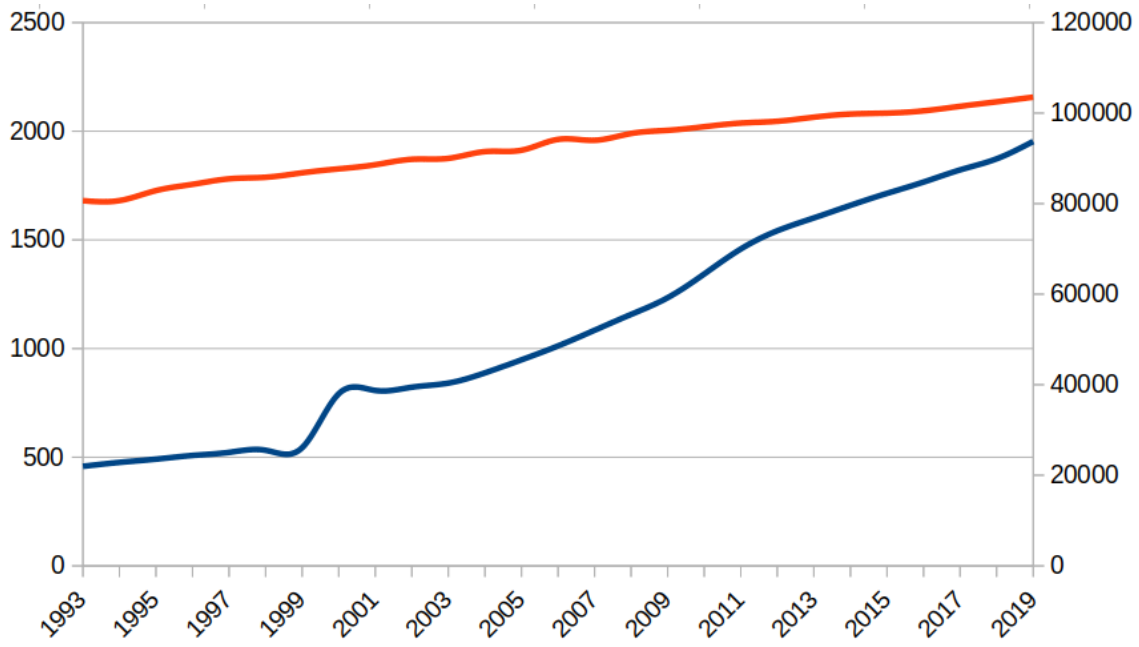

FIGURE II.1 : Évolution du nombre et du tonnage des navires sur la période 1993-2019 (source : *Lloyd's Register Foundation*,).

Si le transport transatlantique de passagers a décru avec l'essor du secteur aérien dans les années 1960, le transport maritime de passagers a connu un second souffle avec le développement des croisières. Là aussi, la course au gigantisme est de mise, avec des bâtiments pouvant accueillir jusqu'à 9 000 personnes à bord, passagers et membres d'équipage [Cen]. La figure II.2 propose un comparatif de dimensions entre un Airbus A380 et quelques navires de tailles remarquables : le porte-avions nucléaire « Charles de Gaulle », le paquebot « Queen Mary 2 » et le porte-conteneurs « Antoine de Saint Exupéry » de la CMA/CGM [1].

Les ressources halieutiques, pétrolières et gazières sont indispensables à notre vie quo-

1. respectivement mis en service en 2007, 2001, 2004 et 2018

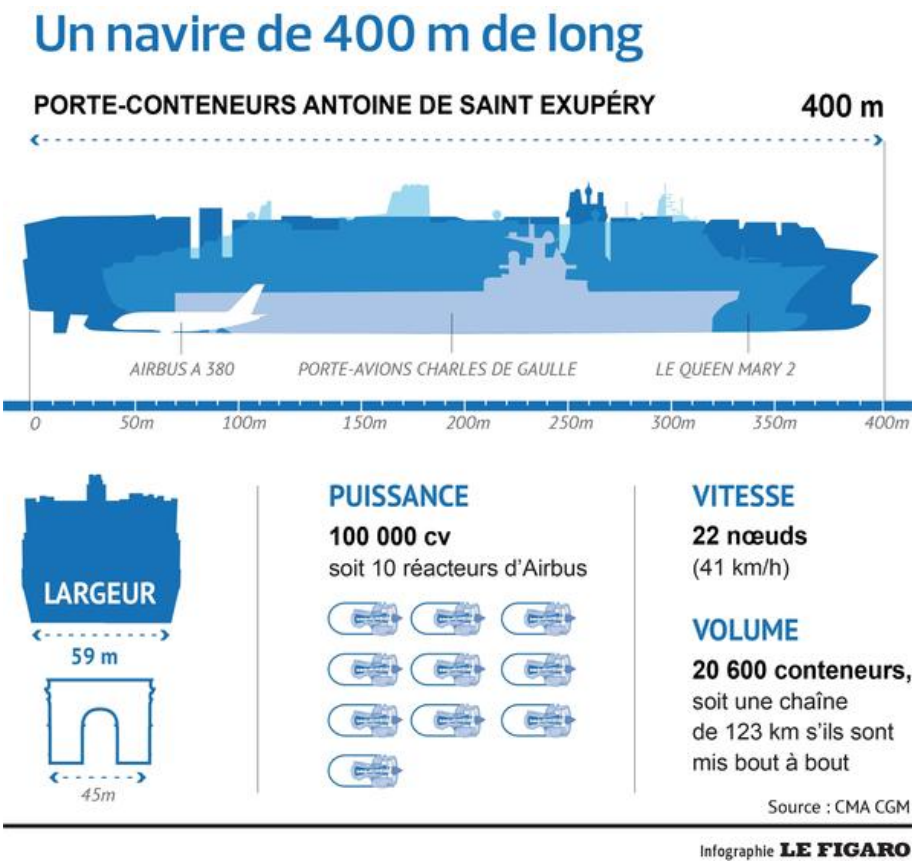

FIGURE II.2 : Dimensions relatives de navires modernes (source : CMA/CGM, infographie : Le Figaro, © Service Infographie / lefigaro.fr / 06.09.2018, reproduite avec leur aimable autorisation).

tidienne. 90 % de la quantité de pétrole brut indispensable aux besoins de la France transite par la mer et la France dépend également de la mer pour l'acheminement de nombreuses matières premières stratégiques. Dans les années et décennies à venir, l'épuisement progressif de certaines ressources et la concurrence dans l'accès aux matières premières vont entraîner des tensions géopolitiques toujours plus importantes, y compris aux frontières maritimes de l'Europe. Le transport maritime pourrait donc représenter une cible de choix et les actes de piraterie augmenter, qu'ils soient à vocation politique, économique ou terroriste.

Enfin, le secteur maritime contribue directement à l'emploi du numérique au quotidien : 95 % des communications Internet internationales transitent par les câbles sous-marins. Avec l'explosion du nombre de terminaux, notamment mobiles, et le développement de l'Internet des objets et du *cloud*, le volume des données transitant par Internet augmente constamment, causant une réelle dépendance des pays vis-à-vis des câbles sous-marins [Bla18]. La perte de services essentiels et l'impossibilité d'échange des données consécutives à la rupture d'un de

ces câbles auraient donc des impacts majeurs sur l'économie et le fonctionnement d'un pays et engendreraient d'importantes tensions géopolitiques [Cla16].

Le secteur maritime a pour ainsi dire toujours connu des actes de piraterie. Les romans et livres d'histoire fourmillent de récits de piraterie maritime, parfois même mandatée par l'État. Si on en parle moins aujourd'hui, la piraterie reste une réalité quotidienne pour de nombreux marins. Les routes maritimes sont connues de tous, de même que l'existence de détroits et de canaux d'importance vitale. La figure II.3 montre ainsi que le canal de Panama ou celui de Suez, les détroits d'Hormuz, de Bab el Mandab et de Malacca sont des voies d'accès essentielles pour le transport des minerais pour de nombreux pays dont la France. Le maintien du libre accès aux voies maritimes et détroits représente donc un enjeu majeur pour ces économies qui en dépendent [dS16]. Au-delà des actions politiques et diplomatiques, ce maintien est garanti par le recours à une présence maritime militaire dissuasive. Après une période toute relative de flottement, on constate aujourd'hui que de nombreuses économies émergentes renforcent singulièrement leurs capacités maritimes militaires, essentiellement dans un arc allant de la Méditerranée orientale jusqu'à l'Australie, via l'Inde et l'Asie.

Le secteur maritime mondial se transforme donc pour faire face aux nouveaux défis du transport de marchandises et de passagers. Les dimensions des navires augmentent fortement pour répondre aux demandes liées à l'économie globalisée. Les enjeux sous-jacents de libre circulation et de souveraineté sur les océans demeurent essentiels pour l'équilibre politique et la vie quotidienne de milliards de femmes et d'hommes (alimentation, biens d'équipement...).

II.1.2 Le secteur maritime civil français

La France est une grande puissance maritime [Lab20] [Bri19]. La connaissance relativement faible des enjeux maritimes par la plupart des Français peut s'expliquer notamment par la taille modeste de l'hexagone continental, par le magnétisme de la capitale au détriment des ports et par la méconnaissance des chemins d'approvisionnement dans une économie mondialisée. Pourtant, en tenant compte des territoires ultramarins, la France dispose de 7 000 kilomètres de littoral et possède le deuxième domaine maritime mondial, après les États-Unis et avant l'Australie, avec une Zone Économique Exclusive (ZEE) de 11 millions de kilomètres carrés. Le secteur maritime français, réputé pour influer sur 14 % du Produit Intérieur Brut (PIB), comprend 340 000 employés et a généré 83 milliards d'euros en valeur de production pour le pays en 2018-2019 [2]. Le secteur maritime joue également un rôle stra-

2. Lire https://www.cluster-maritime.fr/economie_maritime/

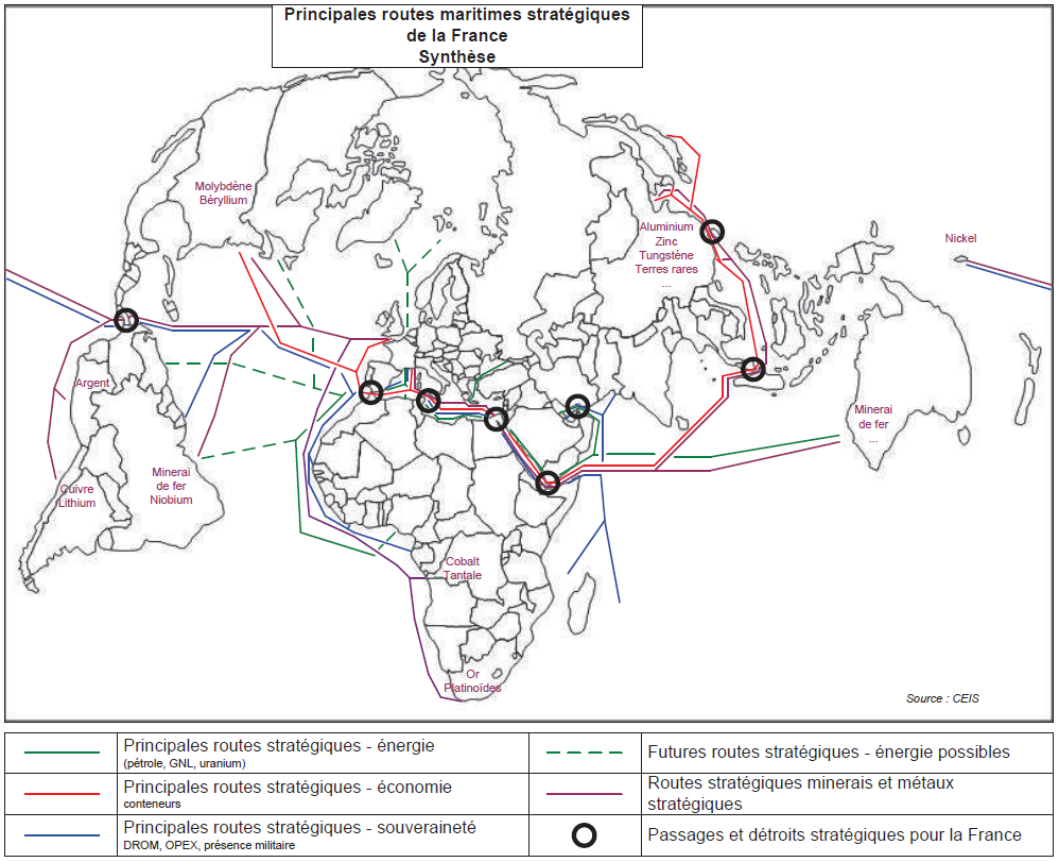

FIGURE II.3 : Routes maritimes stratégiques pour la France (source : Étude « Impacts sur l'économie française de la fermeture d'un ou plusieurs détroits maritimes majeurs » de la Compagnie européenne d'intelligence stratégique, Janvier 2016. © CEIS, tous droits réservés, reproduite avec l'aimable autorisation de CEIS).

tégique pour permettre à la France d'accéder à de nombreux minerais tels que, par exemple, le nickel, l'argent, le cuivre, le lithium, le béryllium, l'aluminium, le zinc, le tungstène, le fer ou encore le cobalt (figure II.3).

Le monde maritime français est riche d'une kyrielle de secteurs d'activité complémentaires [Vei12]. Évoquons tout d'abord les grands ports maritimes de commerce, les deux plus connus étant Marseille-Fos et Le Havre-Rouen-Paris (HAROPA). Ces deux implantations stratégiques reçoivent parfois l'appellation de *smartports*, car de grands projets de télécommunication, d'automatisation et, de manière plus générale, de numérisation y sont menés pour améliorer les flux logistiques et la sécurité. D'autres grands ports maritimes d'importance comme Dunkerque, Nantes-Saint Nazaire, La Rochelle et Bordeaux méritent d'être cités. Certains se sont spécialisés dans la construction et la réparation navale, comme Saint-Nazaire (Chantiers de l'Atlantique) et Brest. Il convient également de souligner l'implan-

tation de plusieurs sites de pétrochimie et la présence d'*hinterlands*[3] d'importance, comme à Marseille-Fos, au Havre-Rouen-Paris ou encore dans la vallée fluviale du Rhône (port Édouard Herriot). Les armateurs français sont particulièrement représentés à l'international, que ce soit dans le transport de marchandises, avec des armateurs comme CMA CGM ou Dreyfus, ou encore par le biais du cabotage et du trafic fluvial qui se redynamisent, notamment sur la Seine, le Rhin et le Rhône. L'essentiel du volume de transport de passagers est réalisé sur le trafic transmanche (Brittany Ferries) et entre la Corse et le continent . Le secteur de la croisière, en plein essor avant la pandémie de la COVID-19, est reconnu à l'international grâce des opérateurs comme Ponant pour les croisières d'exception. Dans un secteur concurrentiel, la pêche est une activité maritime d'importance en France, notamment pour les ports de Boulogne-sur-Mer, Le Guilvinec, Erquy, Port-en-Bessin, Concarneau, Roscoff ou encore Sète et Lorient. La recherche et l'exploration scientifique et océanographique sont des secteurs actifs, avec des organismes réputés comme l'Institut Français de Recherche pour l'Exploitation de la Mer (IFREMER) ou encore la Compagnie Maritime d'Expertise (COMEX), sans oublier les missions de cartographie de l'environnement réalisées par le Service Hydrographique et Océanographique de la Marine (SHOM). L'exploration et le transport pétroliers et gaziers sont représentés par plusieurs compagnies telles que Bourbon, Total ou Elengy, de même que la conception, la pose et la réparation des câbles sous-marins avec Orange Marine ou Nexans. Les secteurs de la plaisance et du *yachting* sont réputés pour la qualité de la construction des navires et le nombre de bateaux présents dans les marinas des ports français, mais aussi pour notre ambition et nos résultats reconnus dans la course au large. Enfin, plus récemment, la France se positionne dans les Énergies Marines Renouvelables (EMR), avec le développement de parcs éoliens *offshore*, d'hydroliennes, et des capacités de construction, d'entretien et d'exploitation à terre, avec des entreprises comme Sabella et l'institut France Énergies Marines.

Même si la concurrence est forte en Europe pour le transport de marchandises, avec les ports de Rotterdam et d'Anvers, et malgré les impacts liés à la pandémie, le secteur maritime français peut être considéré comme riche, très varié et doté d'un réel potentiel.

II.1.3 Le secteur maritime militaire français

En premier lieu, la Marine a comme objectif la réalisation des quatre missions de défense. La première est celle de la dissuasion : il s'agit d'assurer, d'une part, la permanence de la

3. L'*hinterland* correspond à l'aire d'attraction et de desserte continentale d'un port

dissuasion nucléaire océanique [4] et, d'autre part, la capacité tactique de dissuasion aéroportée avec les Rafale marine embarqués sur le porte-avions Charles de Gaulle. Depuis plus de 40 ans, avec la construction du premier Sous-marin Nucléaire Lanceur d'Engins (SNLE) et les premières patrouilles opérationnelles, la permanence de la dissuasion océanique stratégique n'a jamais failli. Deuxième mission : la protection des populations, des territoires et de la ZEE, objectif quotidien de nombreux acteurs de la Marine dans l'Hexagone, sur les mers, dans les airs et dans les territoires ultramarins. L'attrait des ressources halieutiques de la deuxième ZEE au monde entraîne son lot de pilleurs, au large de la Guyane comme dans l'Atlantique sud, contre lesquels il faut lutter en permanence. La troisième mission est celle de la prévention des risques maritimes, en assurant par exemple des patrouilles régulières et un pré-positionnement de forces dans des zones de conflit. Enfin, l'intervention : lorsque cela est nécessaire, la Marine dispose de forces aptes à intervenir militairement, loin et longtemps, que ce soit pour la récupération de ressortissants ou pour des frappes militaires, capacité éprouvée à de nombreuses reprises lors opérations récentes.

La deuxième fonction de la Marine correspond à l'action de l'État en mer. Les Préfets maritimes, officiers généraux de la Marine nationale, jouent un rôle essentiel dans cette fonction. Au-delà d'un rôle assimilable à celui de gardes-côtes, le Préfet maritime représente aussi l'État et peut mettre en demeure un armateur dont le navire présenterait un danger immédiat pour le littoral français, par exemple en cas d'avarie majeure de propulsion [5].

La Marine comprend aujourd'hui plus de 39 000 marins, militaires et civils, 72 bâtiments hauturiers, 200 aéronefs, 10 sous-marins nucléaires, 2 000 fusiliers marins et commandos et 1 000 gendarmes maritimes œuvrant sur 30 petits bâtiments [nat]. En métropole, la plupart des navires de la Marine nationale sont construits, entretenus et amarrés dans les grands ports militaires (Brest, Cherbourg, Lorient et Toulon). Les SNLE sont amarrés et entretenus sur la base opérationnelle de l'Île Longue. Enfin, la Marine est largement présente dans les territoires ultramarins ainsi qu'à l'étranger, par le biais de partenariats signés avec des pays alliés.

Face aux enjeux maritimes stratégiques, la France dispose donc d'une Marine de premier rang, en plein renouvellement et dont l'excellence opérationnelle a été régulièrement reconnue, y compris au cours d'engagements militaires récents, notamment en Méditerranée orientale.

4. La dissuasion peut également prendre des formes non nucléaires.
5. dont la cause pourrait d'ailleurs être cyber

II.2 La transformation numérique du monde maritime

Le milieu maritime connaît, comme d'autres secteurs, une vague sans précédent de recours à l'informatique. La construction et l'exploitation des navires modernes font largement appel aux « nouvelles » technologies. En effet, piloter, manœuvrer et opérer des bâtiments toujours plus grands et performants avec des équipages optimisés [6] impose un recours aux technologies du numérique [Tam18b]. De même, lorsque le bâtiment est à quai, l'efficacité des processus logistiques s'appuie sur les technologiques informatiques et de télécommunication afin de débarquer rapidement les marchandises en toute sécurité et d'assurer les opérations de maintenance de manière efficiente. Les constructions et rénovations des navires, ainsi que les infrastructures terrestres, basculent progressivement mais définitivement vers le numérique, sans qu'aucun plan global n'ait véritablement coordonné ou formalisé cette transformation ni mesuré ses conséquences : en quelques sortes, à l'instar d'autres secteurs, le monde maritime subit en grande partie ce que dicte la loi du marché.

La relative lenteur de cette transformation numérique s'explique, notamment pour les navires, par un cycle de vie particulièrement long. Il n'est pas rare qu'un navire, après une phase de conception de 15 ans [7], ait une durée de vie supérieure à 40 ans. On trouve donc toujours sur les mers des navires construits dans les années 1980. Ces navires, s'ils se numérisent progressivement, ont encore un recours important à l'analogique. C'est surtout à partir de 2050 que le secteur maritime aura probablement achevé sa première grande migration numérique, avec la disparition des navires anciens et l'omniprésence de navires fortement numérisés et de navires autonomes.

Le numérique constitue un incontestable vecteur de progrès pour le milieu maritime, pour la sécurité des hommes, le suivi et la sécurité des cargaisons, des passagers et par conséquent pour le développement économique mondial. Cette transformation se déroule dans un contexte réglementaire particulier : si les règlements maritimes internationaux évoquent encore peu les enjeux cyber, les normes du secteur maritime imposent cependant souvent des exigences précises en termes de résilience, notamment pour les installations cyber physiques, c'est-à-dire les installations industrielles commandées par l'informatique pour réaliser des opérations physiques de production ou de manœuvre par le biais d'automates, de capteurs et d'actionneurs. Ces installations sont donc généralement redondées, mais pas nécessairement sécurisées d'un point de vue cyber.

6. Une frégate multi-missions comprend 108 membres d'équipage, contre le double pour une frégate de lutte anti-sous-marine de génération précédente.

7. Pour les navires les plus complexes, comme les bâtiments de combat.

Concernant le développement des navires autonomes (également appelés *Maritime Autonomous Surface Ship (MASS)*), l'Organisation Maritime Internationale (OMI) a aujourd'hui fixé une réglementation stricte concernant leurs essais en mer et a défini quatre degrés d'autonomie. Le premier degré correspond à un navire qui utilise des processus automatisés avec une capacité de décision autonome : des marins présents à bord opèrent et contrôlent les systèmes et fonctions du navire. Certaines fonctions peuvent être automatisées et parfois non supervisées, mais les marins à bord se tiennent prêts à reprendre la main en cas de besoin. Le deuxième degré s'étend aux navires contrôlables à distance, mais qui disposent toujours de marins à bord : le navire est contrôlé et opéré depuis une position distante, mais les marins présents à bord peuvent prendre le contrôle du navire et opérer les systèmes embarqués en cas de besoin. Le troisième degré ne prévoit aucune présence humaine à bord : le navire est totalement contrôlé à distance. Enfin, le quatrième degré concerne les navires totalement autonomes où le système d'exploitation du navire prend des décisions et détermine ses actions en toute autonomie [8]. La transition vers la semi-autonomie ou l'autonomie complète des navires nécessitera un recours fort aux algorithmes et au numérique dans les années à venir, ainsi qu'une réglementation ambitieuse de la part de l'OMI sur les enjeux liés à la résilience, à la prise de décision autonome des navires et à la cybersécurité.

La transformation numérique durable du secteur maritime est donc une réalité : le numérique est avant tout un vecteur de force, de qualité, de rentabilité et de sécurité. La résilience reste présente au cœur des préoccupations des marins, qui connaissent les risques liés à la mer et l'importance de la sauvegarde de la vie humaine. Cependant, le manque d'intégration de la cybersécurité à bord et cette nouvelle dépendance des navires au numérique et, parfois, à la terre, pourraient entraîner des conséquences majeures qui pourraient aller jusqu'à la « paralysie de la décision » [Goe15].

II.3 La marétique

Le Livre Bleu du cluster Marétique, publié en 2012, a donné la première définition (II.1) du terme « marétique » [mf].

Définition II.1. *La marétique regroupe l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'utilisation des opérations relatives aux activités maritimes, fluviales et portuaires.*

8. https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx

Nous proposons d'employer le vocable de « Systèmes d'Information Maritimes (SIM) » pour évoquer la composante informatique de la marétique. Comme nous l'avons vu au chapitre précédent, les SIM permettent de démultiplier les capacités du monde maritime et d'en améliorer la sécurité. En complément d'une séparation spatiale de la marétique (marétique embarquée à bord des bâtiments, EMR et *offshore*) et celle présente dans les infrastructures maritimes terrestres, le *National Institute of Standards and Technology (NIST)* propose une classification en *Information Technology (IT)* et *Operational Technology (OT)* [Sto11], rappelée en annexe A, qui divise les systèmes d'information en deux, en se basant sur des caractéristiques techniques généralement discriminantes. Ces systèmes convergent cependant technologiquement et cette différence tend, parfois, à s'effacer [Gar18].

II.3.1 La marétique embarquée

Les SIM sont nombreux et couvrent pratiquement l'ensemble des fonctions essentielles d'un navire. Pour la plupart des bâtiments, civils et militaires, les fonctions qui définissent les SIM sont communes.

L'IT regroupe d'abord les communications vers l'extérieur : on retrouve dans cette catégorie l'élongation des services et réseaux du bord vers la terre (téléphonie, raccordement à Internet ou au réseau d'entreprise, visioconférence...), en utilisant des réseaux *Global System for Mobile communications (GSM)*/3G/4G/5G à proximité des côtes ou des liaisons satellites ou radio en zone hauturière. Les communications internes regroupent la diffusion générale à bord du bâtiment, les systèmes de diffusion d'alarme, de téléphonie et d'interphonie, les réseaux *Internet Protocol (IP)*, *Wireless Fidelity (WiFi)* ou *Digital Enhanced Cordless Telephone (DECT)* internes, les équipements tels que les routeurs, commutateurs, *Virtual Private Network (VPN)*, *Virtual Local Area Network (VLAN)*, les diverses solutions de sécurité (passerelles, sondes, pare-feu), les outils de journalisation. Cette catégorie regroupe également les systèmes de distraction à destination de l'équipage et des passagers, avec les accès en mer à Internet via une connexion WiFi ou filaire, les éventuels relais GSM locaux, le suivi médical dématérialisé, les systèmes d'encaissement, de contrôle de l'embarquement des passagers, de gestion hôtelière (*Property Management System (PMS)*), ainsi que la télévision à la demande. L'IT concerne aussi l'informatique « commune », comme les intranets et la messagerie d'entreprise et les serveurs locaux. Enfin, les systèmes de contrôle d'accès, de vidéosurveillance (*Closed Circuit TeleVision (CCTV)*), de sécurité en passerelle (*Bridge Navigational Watch Alarm System (BNWAS)*), les systèmes d'alarme vers la terre,

comme le *Shipboard Security Alarm System (SSAS)* et les systèmes de recherche de personne et de géolocalisation peuvent aussi être regroupés sous le terme IT.

L'appellation OT concerne les systèmes de conduite du navire (*cf* figure II.4) : cartographie numérique (*Electronic Chart Display Information System (ECDIS)*, radars, sondeurs, positionnement géographique par satellite (*Global Navigation Satellite System (GNSS)*, comme le *Global Positioning System (GPS)*, Galileo, GLONASS), les serveurs de référence de temps, les systèmes de positionnement dynamique (*Dynamic Positioning (DP)*), les outils météorologiques et d'établissement de la situation nautique (*Automatic Identification System (AIS)*, *Global Maritime Distress and Safety System (GMDSS)*), les solutions d'enregistrement de « boîte noire »maritime (*Voyage Data Recorder (VDR)*) et autres outils de journalisation et d'alerte. On y intègre aussi la conduite de la plate-forme : systèmes de production d'électricité, d'eau réfrigérée, pilotage de la propulsion, gestion des apparaux (barre, stabilisation), ouverture et fermeture des portes étanches, alimentation en gazole, traitement des eaux grises et noires et de l'air, frigo-vivres, alarmes et sécurité incendie ou voie d'eau. Sont également concernés les systèmes de gestion de la cargaison : *Cargo Control Room (CCR)*, les systèmes d'information de suivi des marchandises et du plan de chargement ou encore les systèmes de gestion des ballasts et des purges.

FIGURE II.4 : Passerelle du navire de recherche *Sikuliaq* (source : Wikimedia Commons, image non modifiée, auteur : NorthBySouthBaranof, licence : CC BY-SA 4.0).

Les navires de guerre disposent de systèmes OT particuliers, comme les systèmes de

combat avec des capteurs et effecteurs comme les sonar, radar, conduites de tir, guerre électronique, de systèmes de conduite de réacteurs nucléaires (pour les bâtiments qui en sont dotés), mais aussi de systèmes militaires de navigation spécifiques comme, par exemple, les centrales de navigation inertielle.

II.3.2 Marétique des infrastructures maritimes terrestres et *off-shore*

À terre, au sein des ports, mais aussi au niveau des armateurs et des organisations de suivi de la navigation se retrouvent également des systèmes IT, comme ceux permettant la gestion de la flotte de l'armateur, les systèmes de réservation de prestations (achat de voyages, de prestations de transport de conteneur, sites Internet et intranet/extranet), les systèmes d'échange de douane maritime ou encore les systèmes de coordination du trafic maritime et d'échanges d'information maritime. Pour sa part, l'OT regroupe par exemple les systèmes de gestion de *pipeline* et d'embarquement et de débarquement de fluides, les systèmes de chargement et de déchargement de vrac et de matériel (conteneurs), les systèmes de planification et de gestion des plate-formes portuaires, les systèmes particulièrement complexes d'exploitation des plate-formes pétrolières et gazières et, enfin, les systèmes de pilotage d'équipements de production d'EMR.

II.3.3 Les particularités des SIM

Un navire qui accueille 8 000 personnes à bord est une véritable petite ville flottante qui comprend, comme nous l'avons vu, un nombre conséquent de systèmes d'information. Un porte-avions nucléaire à la mer cumule ainsi les particularités d'une centrale nucléaire, d'un aéroport militaire, d'une pyrotechnie, d'un hôpital, d'une capacité hôtelière et de restauration pour 2 000 marins, d'un centre de maintenance aéronautique etc., le tout déployé à des centaines voire milliers de kilomètres des côtes les plus proches, parfois dans un contexte hostile et avec des moyens de soutien limités et distants. La marétique hérite donc aussi d'un cumul des particularités des navires, de leur architecture, de leur concepteur, dans des domaines d'emploi particuliers, le tout dans un environnement souvent difficile.

Dans un contexte cyber, les particularités de la marétique que nous avons pu identifier, essentiellement pour les systèmes embarqués, sont tout d'abord dues à la multiplicité des

systèmes. Que ce soit en termes de quantité, de type, de constructeur ou de technologies, le niveau d'intégration relativement faible de ces systèmes entraîne une hétérogénéité aux conséquences importantes. Les contraintes qui pèsent sur les liens par satellite sont élevées : la bande passante est limitée et le coût du lien est généralement lié à la bande passante ou au volume de données alloués. Par ailleurs, la permanence du lien n'est pas garantie, ce qui peut complexifier la télémaintenance et la surveillance, sans parler des impacts liés à la latence. Ensuite, même en cas d'avarie d'un ou plusieurs de ses systèmes, le navire en mer doit rester résilient. Les interventions de maintenance ne sont généralement possibles que lors des escales du bâtiment dans un port. Dans la plupart des cas, aucun expert ou technicien informatique n'est présent à bord du bâtiment, notamment sur les bâtiments civils : les capacités de mise à jour, d'installation de correctif et de restauration de système sont donc limitées. Enfin, à terre, aucune plate-forme d'intégration représentative de la situation réelle à bord du navire n'a généralement été conçue. En effet, la plupart des systèmes ont été réalisés par des entreprises différentes, et ont parfois été intégrés à bord par une autre entreprise. Par ailleurs, l'évolution et la mise à jour d'une installation peuvent nécessiter une nouvelle certification complète avant tout déploiement : le MCS de ces systèmes devient, par conséquent, compliqué. Si, prises chacune séparément, ces caractéristiques ne sont pas déterminantes, leur cumul, synthétisé en figure II.5, fait que la marétique et sa cybersécurité sont si spécifiques. En conséquence, la plupart des solutions « sur étagère » peuvent s'avérer inadaptées à une application directe à bord d'un navire [Jac18].

Le rôle joué par le concepteur du navire est essentiel. En tant qu'intégrateur de systèmes potentiellement hétérogènes développés par plusieurs sous-traitants, il est le garant de la cyber-sécurité globale du navire et de sa cohérence face à la menace. Si le niveau d'intégration est faible, cela n'engendre pas pour autant un couplage limité entre les systèmes. Cela signifie surtout que le partage de services et de fonctions communes - notamment de cybersécurité - n'a pas été réfléchi ni optimisé : chaque système, parfois de type différent (IT, OT), fabriqué par des constructeurs variés, dispose de fonctions indépendantes en termes de sécurité (réseau, applicative, système) de celles d'un système voisin, sans qu'une homogénéité n'ait été recherchée. En parallèle, l'ensemble des systèmes à bord de navires récents sont numérisés afin de pouvoir les surveiller et les commander à distance. Par exemple, une installation de réfrigération des vivres, auparavant purement mécanique, est aujourd'hui fréquemment contrôlée par un automate, des capteurs, des actionneurs, avec un ou plusieurs déports de contrôle-commande vers le système d'exploitation du navire, voire vers la terre. La numérisation du navire entraîne donc une dépendance qui n'existait pas précédemment. À l'échelle du navire, malgré une intégration assez lacunaire en termes de cyber-sécurité, la

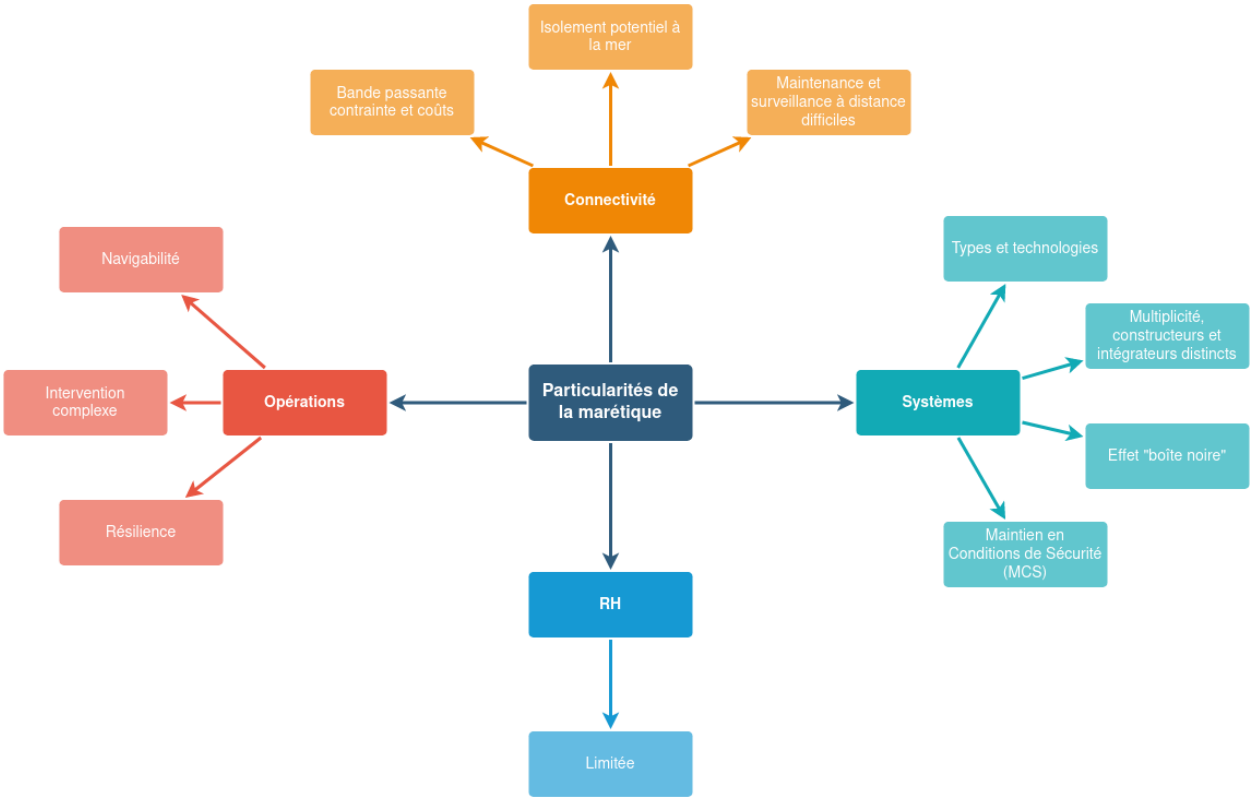

FIGURE II.5 : Particularités de la marétique (source : archives personnelles).

numérisation apporte progressivement une plus forte intégration fonctionnelle des systèmes. En multipliant les interdépendances fonctionnelles, elle augmente également la complexité de l'ensemble et les risques associés, particulièrement avec des capacités humaines limitées.

II.3.4 Le futur des SIM

La marétique continuera à accompagner les transformations du secteur maritime. Les évolutions majeures à prévoir à court et moyen termes concernent le développement des navires semi-autonomes, puis autonomes, dont les premiers essais ont eu lieu au courant de l'année 2018 et se poursuivent aujourd'hui, en France, en Europe, et dans le monde entier. Dans les décennies à venir, leur développement pourrait, dans certains cas, limiter voire supprimer le recours à l'humain dans tout ou partie de certains domaines du secteur maritime, augmentant de manière substantielle la surface d'attaque numérique de ces navires [Tam18a, Kav18, Kat17, Bol19]. La généralisation des véhicules autonomes (aéromaritimes, de surface ou subaquatiques) dans le secteur maritime s'applique aussi au monde militaire, afin de limiter l'exposition humaine aux risques et faciliter le déploiement de capteurs, notamment

à des fins de renseignement. Enfin, à plus court terme, la mise en œuvre de technologies numériques avancées comme l'apprentissage automatique et la réalité augmentée soutiendra les hommes dans les manœuvres, la conduite et la maintenance des navires et infrastructures.

II.4 Cybersécurité des SIM

Après avoir décliné les définitions de la cybersécurité au monde maritime, cette section détaille les vulnérabilités et évènements redoutés du secteur.

II.4.1 Cybersécurité et milieu maritime : définitions

Le terme « système d'information » fait l'objet de nombreuses définitions et interprétations en fonction des personnes et des organisations. Nous utiliserons donc la définition II.2 d'un système d'information pour ce manuscrit :

Définition II.2. *Système manuel ou automatisé, comme un système de traitement automatique de données, un système informatique ou un réseau informatique, s'appuyant sur des infrastructures techniques et composé de personnes, de machines et de méthodes et qui est organisé pour réaliser des fonctions de collecte, traitement, transmission et diffusion de données qui représentent de l'information.*

La figure II.6 précise les différentes vues qui peuvent être réalisées d'un système d'information, sous l'angle fonctionnel, applicatif et technique.

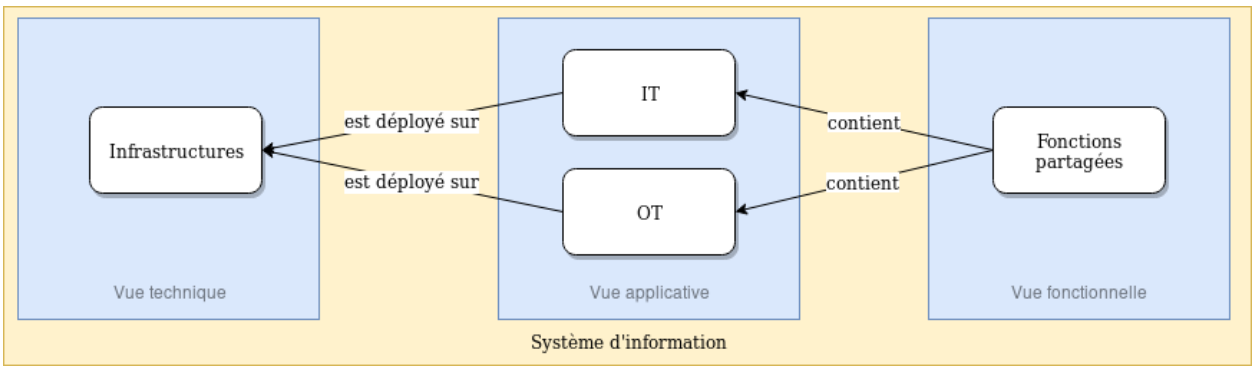

FIGURE II.6 : Vues fonctionnelle, applicative et technique d'un système d'information (source : archives personnelles).

Dans le contexte maritime, ce système d'information subit les contraintes et particularités de milieu listées en II.5 et prend l'appellation de SIM.

Défini comme un « champ de confrontation à part entière » [dllea13], le cyberespace fait partie de l'environnement informationnel, qui comprend, d'après l'Organisation du Traité de l'Atlantique Nord (OTAN), « l'information elle-même, les individus, organisations et systèmes qui la reçoivent, la traitent et la transmettent, et l'espace cognitif, virtuel et physique dans lequel cela se produit [Com12]. » La définition II.3 suivante est également proposée.

Définition II.3. *Le cyberespace est le domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunications, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés [CIC].*

Le cyberespace est interdépendant de l'air, la terre, la mer et l'espace, domaines dont il est cependant transverse, puisqu'il peut se retrouver en chacun d'entre eux [9]. S'il est parfois difficile d'en concevoir une représentation globale, la publication interarmées américaine « *Joint Publication 3.12* » propose une modélisation en trois couches ou zones [10]. Tout d'abord la couche physique : c'est la plus concrète des trois zones, bien que récemment rendue plus diffuse par les techniques d'infogérance et de *cloud computing*. Elle est composée des équipements physiques informatiques et des réseaux associés qui assurent le stockage, le transport et le traitement de l'information. Ensuite, la zone logique : elle est constituée des processus, outils et des flux d'échanges, algorithmes et protocoles qui ne s'appuient pas sur une réalité physique, mais sur un adressage purement logique. Enfin, la couche sociale ou cognitive, appelée *cyber-persona* dans la *Joint Publication 3.12* est plus difficile à appréhender. Elle abstrait les informations au format numérique présentes dans la couche logique pour créer des représentations numériques d'un acteur ou d'une entité dans le cyberespace, y compris les individus et les identités numériques associées (avatars). Dans le domaine maritime, le cyberespace comprend l'ensemble des SIM évoqués dans la section précédente.

Définition II.4. *La cybersécurité est un état recherché pour un système d'information, lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. [CIC]*

9. On rappellera également l'étymologie du préfixe *cyber*, tirée du grec *Kubernêtikê* qui signifie « gouvernail ».

10. « *Cyberspace operations* » du 8 juin 2018, consultable à l'adresse https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

La cybersécurité proposée par la définition II.4 est donc l'Effet Final Recherché (EFR) pour les SIM d'œuvrer en sécurité. Elle s'appuie sur la cyberprotection, les capacités de cyberdéfense et la cyber résilience. Il convient de souligner qu'aucune notion d'action volontaire n'est indiquée : les évènements se déroulant dans le cyberespace peuvent aussi avoir une origine involontaire ou accidentelle. Les incidents d'origine environnementale (par exemple un incendie), une panne matérielle ou une anomalie logicielle impliquant des systèmes d'information, souvent négligés dans les analyses de risques, doivent ainsi être pris en compte.

Définition II.5. *La cyberprotection est l'ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles [CIC].*

La définition II.5 de la « cyberprotection » la rend synonyme de « sécurité des systèmes d'information ». Dans le contexte maritime, c'est donc l'EFR pour les SIM d'être sûrs et performants en termes de disponibilité, d'intégrité et de disponibilité dès leur conception et tout au long de leur cycle de vie.

Définition II.6. *La cyberdéfense est l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels [CIC].*

Le suffixe « défense » a entraîné une certaine sur-utilisation du terme cyberdéfense défini en II.6 dans le contexte militaire, auquel il n'est cependant pas réservé. La définition particulière II.7 suivante est cependant donnée à la cyberdéfense militaire.

Définition II.7. *La cyberdéfense militaire est l'ensemble des actions défensives ou offensives conduites dans le cyberespace en préparation ou dans la planification et la conduite des opérations militaires, notamment pour garantir l'efficacité de l'action des forces armées et le bon fonctionnement du ministère. La cyberdéfense militaire complète les mesures de protection des réseaux, des systèmes et de l'information par une capacité d'opérations dans le cyberespace et une capacité de gestion de crise cybernétique, couplées aux capacités de résilience des systèmes d'information [CIC].*

Dans le contexte maritime, la cyberdéfense correspond donc à l'EFR pour les SIM d'être aptes techniquement à être défendus face à une agression cybernétique. La cyberdéfense

regroupe également une organisation dédiée de crise, apte à détecter, qualifier, contrer un évènement cyber, voire d'être à l'initiative d'une opération numérique.

La notion de cyber résilience est définie ci-après (II.8) :

Définition II.8. *La résilience se définit comme la capacité d'une organisation à faire face à des évènements (incidents ou agression), à leur résister et à se rétablir. Appliquée au cyberespace, elle est appelée cyber résilience et définie comme la capacité d'un système d'information à résister à une panne et à revenir à son état initial après l'incident [CIC].*

Dans le contexte maritime, l'EFR de la cyber résilience pour les SIM est d'offrir un haut niveau de disponibilité en cas d'agression, qu'elle soit humaine, environnementale, ou tout simplement suite à une panne. La résilience, ancrée « dans l'ADN » des marins, habitués à devoir se sortir seuls de situations fâcheuses, correspond à une caractéristique que les marins attendent légitimement de leurs SIM.

La cybersurveillance représente l'outil temps-réel de la cyberdéfense. Elle contribue directement à la boucle « observer, orienter, décider et agir » (OODA), car elle offre une capacité temps réel de détecter tout évènement qui pourrait s'avérer hostile ou inhabituel. Une définition de la cybersurveillance appliquée à la marétique pourrait être celle proposée en II.9 :

Définition II.9. *La cybersurveillance se définit comme la capacité d'une organisation à détecter tout évènement hostile ou inhabituel dans un système d'information et qui pourrait impacter sa disponibilité, son intégrité, sa confidentialité ou la traçabilité de ses données. Appliquée au secteur maritime, elle comprend la mise en place de capteurs sur les SIM, la collecte des métadonnées qu'ils produisent et leur analyse au sein d'une capacité générique de supervision de cyberdéfense à la recherche, en temps réel ou différé, d'indicateurs de compromission. Elle prévoit aussi la mise en place d'une organisation et d'outils qui permettent l'élaboration de la situation cyber de référence des SIM.*

II.4.2 État des lieux des vulnérabilités des SIM

Comme tout système d'information, les SIM sont concernés par de nombreuses vulnérabilités qui pourraient être exploitées par un attaquant [Jon16, Bur14, DiR15, Cim11]. Cependant, trois difficultés symptomatiques peuvent être considérées comme principaux vecteurs de vulnérabilités.

Tout d'abord, le cycle de vie et le MCS d'un navire : après une phase d'ingénierie puis de construction de plusieurs années [11], les navires sont généralement conçus pour naviguer pendant trente à quarante ans. Sur cette période, leur utilisation doit être maximale afin d'en assurer la rentabilité. Cet « emploi du temps » chargé complexifie les évolutions majeures de la marétique du navire. Si le MCS est possible sur les systèmes de bureautique présents à bord et l'IT de manière générale, il est beaucoup plus compliqué à mettre en œuvre au profit de l'OT. Par ailleurs, la durée de vie de ces systèmes est notablement plus longue que celle de l'IT : il est ainsi réaliste de penser que certains systèmes ne seront pas remplacés du tout - hors avarie majeure - pendant la durée de vie du navire. Après le neuvage du navire, la mise en place de correctifs, la sécurisation de protocoles anciens est peu vraisemblable, voire impossible à un coût acceptable et les conséquences sur le fonctionnement des autres systèmes des navires complexes à évaluer, dans un contexte croissant d'interdépendance.

Ensuite, la maturité du secteur : la cybersécurité de la marétique constitue un domaine relativement nouveau et assez peu évoqué, notamment en ce qui concerne la recherche. Ainsi, même des ouvrages de recherche très récents sur les SIM, parus au cours de cette thèse, ne font pour ainsi dire aucunement référence aux enjeux de cybersécurité maritime [LMWW21]. Si les enjeux militaires de la cybersécurité maritime ont globalement été évalués et pris en compte au cours des dix dernières années, le monde maritime civil semble également moins considéré. Les enjeux sous-jacents sont pourtant essentiels. Les multiples raisons qui peuvent expliquer la difficulté de prise en compte de la cybersécurité de la marétique sont : une faible perception des enjeux, un manque de gouvernance et de coordination, une sensibilisation insuffisante du personnel, une méconnaissance des SIM, l'absence de politique de l'armateur ou de l'opérateur, la complexité, le coût, la difficulté à identifier et fidéliser des experts.

Enfin, une absence quasi généralisée d'équipements de cybersécurité et particulièrement de détection d'évènements cyber est observée à bord des navires. En conséquence, les détections peuvent être tardives, voire perdurer pendant la durée de vie d'un système jusqu'à son retrait du service actif.

Si ces trois difficultés amènent à penser que le secteur est vulnérable, le constat doit cependant être nuancé. En effet, le numérique est un vecteur de progrès pour le milieu maritime, pour la sécurité des hommes, le suivi et la sécurité des cargaisons. Dorénavant, il n'est plus envisageable d'imaginer faire « sans » le numérique. Par ailleurs, les normes du secteur maritime imposent fréquemment des exigences précises en termes de résilience, notamment pour les installations cyber physiques. Elles prévoient ainsi généralement une

11. Parfois jusqu'à 15 ans pour les navires militaires les plus complexes

redondance de ces installations. Elles disposent même parfois de chaînes de sécurité distinctes, fonctionnant en parallèle des chaînes de commande, pour vérifier que le fonctionnement de la production est correct, conforme aux valeurs attendues et dans les limites prévues pour le système. Enfin, il convient de souligner le rôle de l'homme : le marin est résilient, entraîné, expérimenté et apte à endurer des situations difficiles et à réagir en cas d'évènement inattendu. Cette analyse systémique des vulnérabilités du milieu maritime est synthétisée dans la figure II.7.

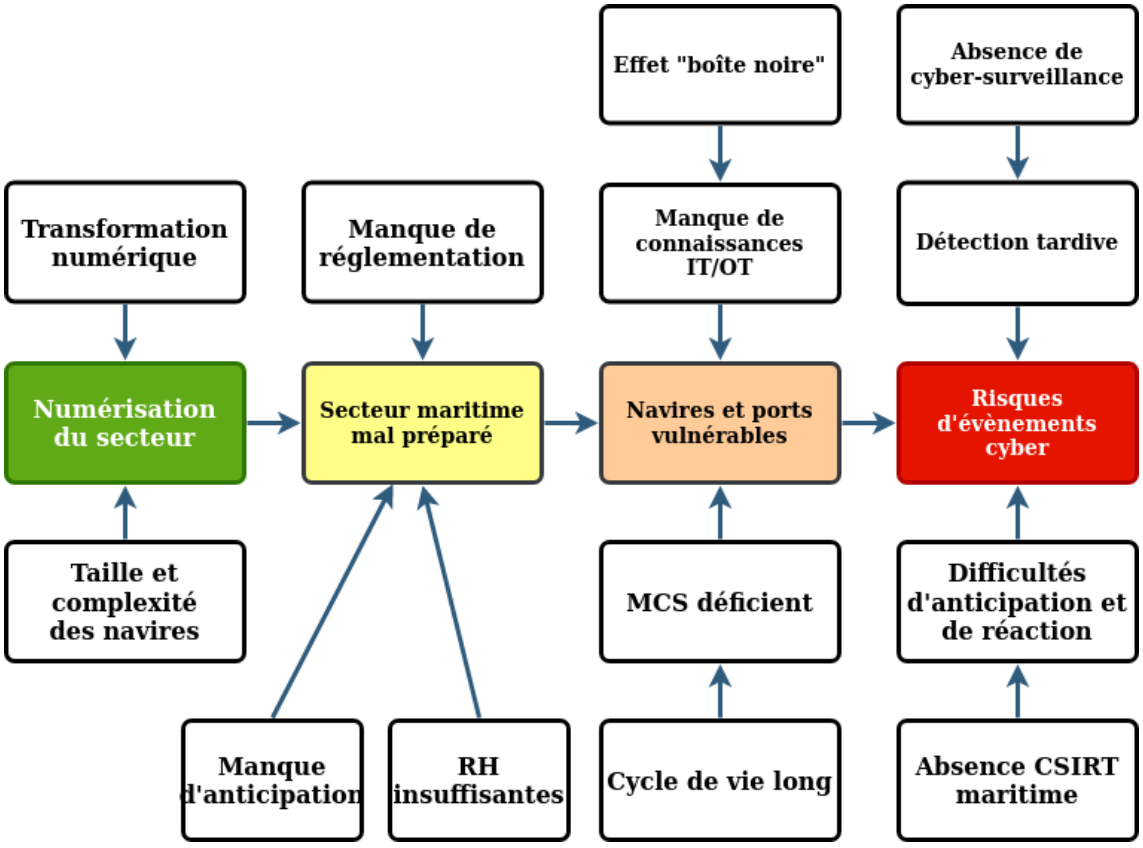

FIGURE II.7 : Analyse systémique des vulnérabilités cyber du milieu maritime induites par la transformation numérique (source : archives personnelles).

II.4.3 Exploitation des vulnérabilités des SIM à des fins offensives

L'intérêt d'emploi du vecteur cyber pour conduire une opération offensive est connu : en effet, l'attaquant sait que son action, si elle est réalisée de manière discrète, a peu de chances de faire l'objet de représailles (cyber ou cinétiques), tant la réaction est difficile à conduire dans ce champ de confrontation. Tout d'abord, le caractère anomique du cyberespace le rend

particulièrement abscons à encadrer, que ce soit pour des raisons juridiques ou politiques. Malgré des volontés récentes en matière de droit international [da19], il est incontestable que certains acteurs ont aussi tout intérêt à ce que cet état de fait reste inchangé. Ensuite, la transformation numérique rapide du secteur crée un cyberespace mouvant, en évolution permanente, difficile à maîtriser et à cartographier et dont les interdépendances fonctionnelles augmentent en permanence. Ces interdépendances pouvaient exister avant la transformation numérique : par exemple, le système d'information d'un navire nécessite souvent que les serveurs et équipements réseau disposent d'une salle climatisée. Un système cyber physique assurait cette fonction de climatisation (système de production d'eau réfrigérée, par exemple), mais n'était généralement pas numérisé. Cependant, la transformation numérique touche dorénavant les systèmes industriels : ces derniers s'appuient ainsi sur un système d'information (écran tactile, automate) pour être démarrés, arrêtés et conduits. L'étape suivante de transformation numérique consiste en l'augmentation de l'interdépendance des systèmes d'information entre eux (par exemple : diffusion des informations relatives à disponibilité de la climatisation, à la température de l'eau...). Agir sur un système en action ou en réponse à un incident peut ainsi induire des conséquences sur d'autres systèmes non impactés initialement et essentiels aux opérations (dégâts collatéraux). Enfin, la difficile imputabilité des actions dans le cyberespace facilite les opérations de manipulation et d'amplification. La manipulation consiste soit à produire, détourner ou falsifier de l'information à son profit. L'amplification vise à donner un fort retentissement à une information, vraie ou fausse, et que l'on n'aurait pas remarqué autrement. Ces deux modes d'action, fréquemment utilisés sur les réseaux sociaux, peuvent prendre part à des actions de désinformation d'un niveau plus stratégique. La réaction face à ce type d'action permet difficilement d'envisager des actions juridiques ou cinétiques, notamment en raison du caractère potentiellement mondial de l'amplification, du temps court des réseaux sociaux, de l'effort de contre-attaque nécessaire et de la difficile imputation des acteurs initiaux de ces actions de guerre informationnelle. Enfin, l'action repose souvent sur des vecteurs techniques évolutifs qui nécessitent des compétences transverses élevées : en garantir l'efficacité, l'innocuité et, dans le cas d'une attaque, l'absence d'imputabilité à long terme n'est pas une chose aisée.

Les raisons d'utiliser le cyberespace pour viser la marétique sont nombreuses [Fit15]. Les notions de preuve, d'imputabilité des actions de frontière, de distance, d'organisation ou de temps restent plus complexes à appréhender que dans les espaces physiques. Les manipulations ou amplifications demeurent en outre possibles, ce qui contribue à modifier la nature des rapports de force entre adversaires et à renforcer l'asymétrie entre attaquants et défenseurs. L'attaquant dispose souvent de plusieurs longueurs d'avance, et il sait que la

réponse face à l'attaque ne sera pas suffisamment dynamique, voire que l'attaque demeurera indétectée. Pour réaliser son forfait, il peut s'appuyer sur plusieurs vecteurs, qui peuvent être employés de manière combinée. En premier lieu, il peut utiliser la zone physique : le vol, le piégeage, la destruction physique de tout ou partie de la marétique embarquée par utilisation d'Agression Électromagnétique Intentionnelle (AGREMI), d'Impulsion Électro-Magnétique (IEM), d'agression environnementale (incendie, voie d'eau ...). Ensuite, l'attaquant peut choisir la zone logique : le vol de données (espionnage), l'emploi de vecteurs logiciels, les attaques réseau-centrées. Enfin, il peut également agir dans la zone sociale, en atteignant les personnes ou les familles de personnes qui évoluent dans le domaine maritime, par exemple en exploitant le Renseignement d'Origine Source Ouverte (ROSO).

II.4.4 Sources de menaces et évènements redoutés

Même parcellaires, les données publiques relatives aux évènements de cybersécurité dans le monde maritime que nous avons pu recenser font ressortir la prédominance de sources de menaces internes ou externes involontaires (membres d'équipages, intervenants extérieurs, concepteurs) d'une part, et d'autre part de sources de menaces externes volontaires liées à la cybercriminalité et ne visant généralement pas à proprement parler le secteur maritime, qui constitue donc plutôt dans ce cas un dégât collatéral [Jac]. Les attaques ciblant précisément le secteur maritime existent, mais restent peu documentées publiquement. Enfin, il convient de souligner que la menace étatique est renforcée pour la composante militaire avec également des cas de vols de données à des fins d'espionnage, qui peuvent également viser les académiques, industriels et sous-traitants du secteur.

Les menaces cybernétiques qui visent le secteur maritime peuvent cibler les informations. Dans ce cas, l'objectif est alors d'exploiter, d'extraire, de rendre indisponible, de détruire, de manipuler ou corrompre les informations numériques : données de cartographie, de navigation, informations sur le chargement ou le transit des marchandises [Bea17], les passagers, les caractéristiques du navire. Les systèmes d'information peuvent également représenter des cibles. Dans ce cas, les attaques peuvent avoir pour but de réaliser une cartographie des SI, l'identification de leurs vulnérabilités, la modification ou la perturbation temporaire de leur fonctionnement, voire leur destruction immédiate ou au moment opportun. Enfin, les systèmes cyber physiques peuvent constituer des cibles à haute valeur ajoutée : l'objectif est alors d'utiliser le cyberespace comme vecteur pour viser des objectifs physiques. Il peut ainsi d'agir de perturber, neutraliser, voire détruire des équipements, des infrastructures ou

des installations critiques en agissant sur les systèmes informatiques qui les pilotent ou les gèrent en exploitant les vulnérabilités informatiques de certains de leurs composants. Les menaces peuvent donc viser les trois couches du cyberespace : physique, logique et cognitive. L'annexe B synthétise les évènements redoutés du secteur.

II.5 Conclusion

Comme nous l'avons vu dans ce chapitre, le secteur maritime porte des enjeux stratégiques pour les intérêts français. Il revêt une importance capitale pour de nombreux secteurs de l'économie comme pour la vie quotidienne des Français. Dans ce secteur en pleine transformation, la marétique joue un rôle essentiel. Concourant directement au bon fonctionnement des navires, elle permet l'accomplissement en sécurité de nombreuses fonctions, physiques ou non. Les caractéristiques particulières de ces systèmes les exposent cependant à différentes sources de menaces. Intrinsèquement vulnérables, ils peuvent représenter un intérêt majeur pour l'attaquant, et les outils de sécurité aujourd'hui disponibles sont mal adaptés et ne permettent pas de percevoir ou de comprendre la situation, pas plus que de suivre l'évolution d'un évènement cyber dans le temps et encore moins d'y remédier en temps contraint. Il apparaît donc nécessaire d'identifier les outils et démarches, les plus à même de répondre aux verrous scientifiques, organisationnels, technologiques et humains de la cybersécurité maritime, de les concevoir avec une approche guidée par la modélisation de leur fonctionnement et, enfin, d'en vérifier l'apport scientifique et opérationnel.

Chapitre III

Maritime Cyber Situational Awareness : définition, modélisation et apports à la cybersécurité des SIM

Dans ce chapitre, nous abordons la QR1, à savoir l'architecture de collecte et sa modélisation nécessaires pour améliorer la détection, la compréhension et la réaction face à une menace cyber. Nous précisons les apports de la cybersurveillance des SIM à la détection des évènements redoutés du secteur et les difficultés relatives à sa mise en œuvre. Nous présentons ensuite les limitations actuelles des produits de sécurité qui contraignent leur emploi direct dans le milieu maritime. Nous détaillons enfin le principe de *Situational Awareness* et proposons son application à la cybersécurité des SIM au travers du concept original de *Maritime Cyber Situational Awareness*, dont nous proposons une architecture fonctionnelle. Le travail original du concept de MCSA a fait l'objet de plusieurs publications internationales [Jac18, Jac19a, Jac19b].

III.1 Cybersurveillance des SIM : la problématique

Dans cette section, nous évaluons dans un premier temps l'intérêt de mettre en place des capacités de cybersurveillance des SIM pour répondre aux difficultés structurelles rencontrées par le monde maritime. Ensuite, nous étudions les méthodes et outils actuels qui pourraient

permettre de répondre aux attentes du secteur en termes de cybersurveillance et en identifions les limites.

III.1.1 Apports de la cybersurveillance face aux difficultés du monde maritime

La cybersurveillance maritime, telle que nous l'avons définie en II.9, a pour objectif de détecter tout évènement hostile ou inhabituel, volontaire ou involontaire, qui pourrait impacter les SIM. Elle comprend l'organisation, les outils, les ressources humaines et les méthodes de détection, de classification d'un évènement, et de remédiation. En cela, la cybersurveillance des SIM peut s'appuyer sur l'organisation, les outils et les procédures d'un centre opérationnel de cybersurveillance (*Security Operations Center (SOC)*), comme c'est le cas pour d'autres secteurs [Zim14]. L'infrastructure technique de ces centres comporte des capteurs de terrain judicieusement placés et paramétrés et faisant l'objet d'une surveillance locale ou à distance permanente. Au travers d'une architecture applicative locale de collecte, une élongation des données est réalisée vers un centre focal, en charge de l'expertise de l'analyse, de la détection et de la qualification des évènements cyber et disposant d'une capacité de visualisation et de synthèse. Plusieurs outils informatiques concourent à cette mission, comme les *Security Information and Event Management (SIEM)* et la *Cyber Threat Intelligence (CTI)*. Si la frontière entre *SOC* et *Computer Security Incident Response Team (CSIRT)* fait l'objet de débats récurrents, notamment sur la résolution des incidents, ces centres utilisent également des *Security Incident Response Platform (SIRP)* afin d'offrir une capacité de dialogue et de partage vers d'autres acteurs de la cybersécurité, d'assurer la gestion de crise, ou encore d'informer les échelons de direction pour concourir à la prise de décision.

En-dehors de la détection, de la qualification et de la réponse aux menaces, la cybersurveillance offre aussi une première réponse aux problèmes structurels identifiés dans la figure II.7 et que nous rappelons ci-après. Tout d'abord, la veille apportée par la CTI permet d'améliorer l'anticipation des menaces, que cela concerne les vulnérabilités liées aux matériels ou logiciels, la lutte contre la menace virale ou la connaissance des *Tactics, Techniques, Procedures (TTP)* adverses [WDWI16]. Ensuite, les lacunes en ressources humaines formées et entraînées en cybersécurité maritime ont été soulignées récemment par deux études, l'une anglaise [Tam19] et l'autre réalisée auprès des armateurs et ports français [Ben18]. La concentration de ces ressources dans un centre expert répond donc en partie aux difficultés

de préparation du secteur dans ce domaine. La cybersurveillance, même sur des systèmes vulnérables et anciens, permet de détecter les tentatives d'exploitation des vulnérabilités - ainsi que leur absence. Si, dans la plupart des cas, les architectures de cybersurveillance exploitent des dispositifs « passifs » et qu'elles ne permettent donc pas de réaction physique, elles offrent cependant la possibilité technique, humaine et organisationnelle de détecter et réagir rapidement. Sans corriger les causes initiales de la problématique du MCS, la cybersurveillance apporte donc une partie de la réponse. Par ailleurs, de la capacité de la cybersurveillance à « écouter » les hôtes, serveurs et les réseaux du navire à la recherche de traces de compromission découle aussi un gain appréciable en termes de maturité et de connaissance de l'IT/OT embarqué ou dans les ports. La tendance du navire à constituer une « boîte noire » est atténuée et la réalisation de cartographies dynamiques des SIM devient possible. Enfin, la cybersurveillance engendre des effets de bord intéressants : par exemple, la finesse et le volume des informations remontées présentent un intérêt dans la maintenance prédictive, la détection de défauts de configuration, mais aussi à d'autres fins (suivi logistique, cartographie, maîtrise des capacités opérationnelles). La figure III.1 reprend la figure II.7 en y soulignant la plus-value de la cybersurveillance dans le traitement des vulnérabilités induites par la transformation numérique du monde maritime : les apports, favorables, figurent en bleu. Il convient cependant de les nuancer en rappelant que, d'une part, les moyens doivent continuer à être mobilisés pour corriger les causes systémiques déjà évoquées et, d'autre part, que la mise en œuvre de la cybersurveillance représente un coût important et ajoute de nouveaux équipements, systèmes et services qui nécessitent sécurisation, maintenance et administration sur le long terme.

III.1.2 Inadéquation des méthodes classiques de cybersurveillance

La modélisation classique d'une organisation et d'une architecture technique de cybersurveillance nécessite des compétences variées qui se heurtent au manque de maturité actuel du monde maritime. En effet, la cybersurveillance doit s'appuyer sur des moyens et procédures existants qui, dans le monde maritime civil, peuvent s'avérer absents ou immatures. Les ressources humaines qualifiées pour opérer un SOC maritime sont ainsi rares et longues à former. L'intervention et la surveillance à distance d'un navire s'avèrent complexes, en raison des contraintes évoquées de sa connectivité, qui limitent également la capacité à transmettre les volumes de données attendus par le SIEM. Enfin, la méconnaissance de certains systèmes IT et surtout OT rend difficile le déploiement de capteurs qui, par ailleurs, pourraient ne pas être adaptés. Le tableau III.1 croise les capacités nécessaires à la mise en œuvre

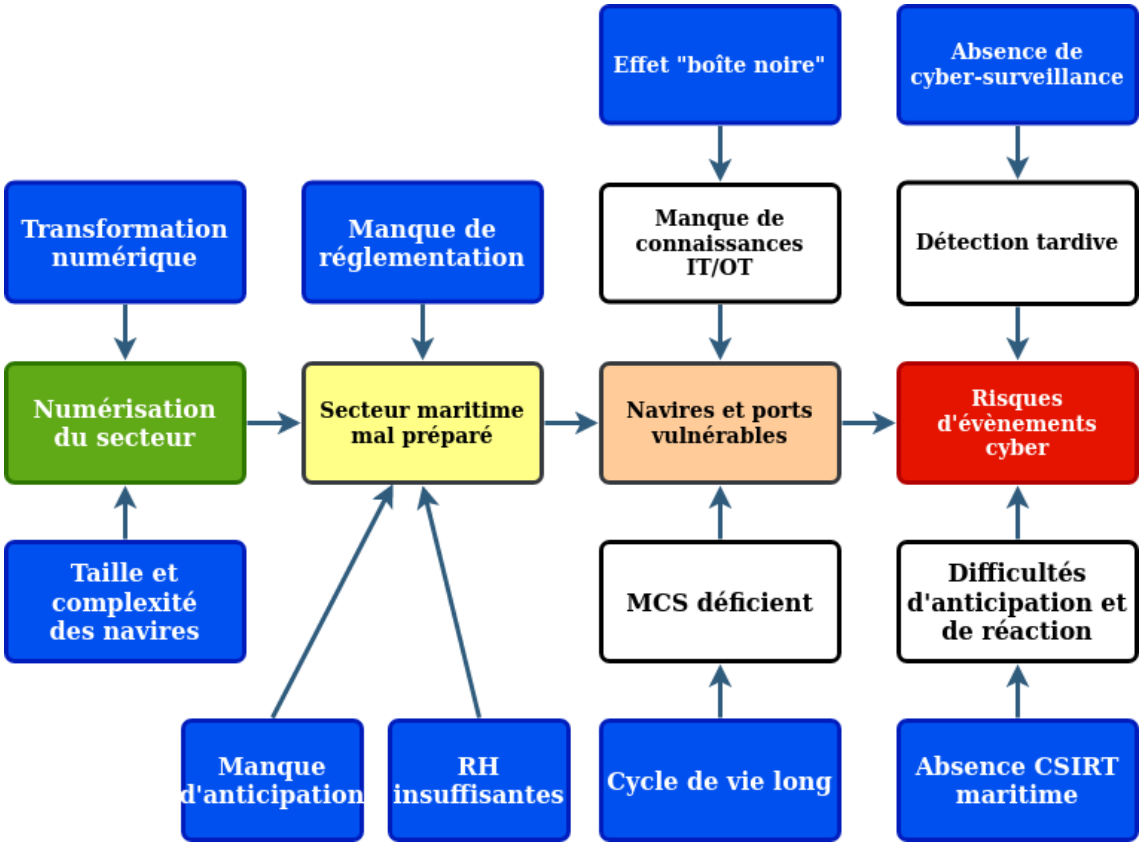

FIGURE III.1 : Apports de la cybersurveillance au milieu maritime (source : archives personnelles).

Tableau III.1 : Besoins des SOC *versus* contraintes du monde maritime

Besoins SOC	Maturité cyber	RH experte et entraînée	Intervention à distance	Volume de données	Connaissance SI	*Patch management*
Secteur maritime	Relative immaturité	RH limitée	Intervention complexe	Connectivité contrainte	Effet boîte noire	MCS
Solutions	Centre expert	RH centralisée	Logistique	Architecture dédiée	Cartographie	Capacité de détection

d'une cybersurveillance avec les difficultés attendues. Si la mise en place d'une capacité de cybersurveillance s'avère complexe, son apport est réel.

La conception d'un modèle de sécurité qui s'appuie sur la cybersurveillance expose aussi à des risques nouveaux et nécessite de s'intéresser aux techniques adverses [Bra11]. Un attaquant, pour masquer sa tactique, peut tenter de saturer les outils de cybersurveillance par de multiples détections qui, à des fins de déception, pourraient camoufler une attaque ciblée plus complexe et moins visible, le rapport signal sur bruit s'avérant alors défavorable au modèle de détection. Parmi les risques involontaires, des ressources humaines non spécialisées ou méconnaissant les architectures de détection, les systèmes surveillés, ou un mauvais positionnement ou paramétrage de capteurs peuvent conduire à une vision partielle ou faussée de la situation réelle. Enfin, le capteur constituant lui-même un système informatique, il peut également faire l'objet d'une compromission. Il apparaît donc nécessaire de concevoir des mécanismes technologiques appropriés et sécurisés, mais aussi une architecture et des indices de compromission qui permettent la contextualisation de la surveillance. Il convient également d'éprouver le fonctionnement et la finesse de ces solutions par des tests spécifiques de type audit ou test d'intrusion.

Le marché des outils de cybersurveillance s'avère plutôt mûr et prolifique. Les solutions de SIEM sont notamment nombreuses et, pour la plupart, conçues et améliorées depuis des années. Les capteurs de type *Network-based Intrusion Detection System (NIDS)* ou *Host-based Intrusion Detection System (HIDS)* et les logiciels de journalisation centralisée sont également présents de longue date, notamment sur les systèmes IT. Les fonctions d'un SIEM s'avèrent essentielles pour la détection et le traitement d'un évènement cyber. Son rôle est de collecter l'information, de l'agréger, de la normaliser, de la corréler, d'offrir des capacités de tableau de bord et d'alerte, d'archiver et de pouvoir rejouer les évènements. Cependant, ces outils multi-tâches présentent des limitations. Parmi celles-ci, Miloslavskaya [Mil19] rappelle les difficultés des SIEM à travailler sur une grande échelle de systèmes hétérogènes et répartis géographiquement, les difficultés de détection au milieu de multiples faux positifs et la masse conséquente de données. Les délais de détection et de traitement des alertes s'avèrent souvent incompatibles avec la fulgurance d'une cyberattaque. Pour combler ces lacunes, Cardena *et al* suggèrent l'emploi de technologies de traitement de données en masse [Car13].

La figure III.2 modélise les limitations actuelles des SIEM qui peuvent rendre difficile leur emploi dans des contextes comme le maritime, sous les aspects liés au volume des données (incompatible avec le milieu maritime), à l'architecture (absence de prise en compte des contraintes de milieu) et d'appréciation de la situation (l'outil en lui-même ne permet pas d'apprécier ce qui se déroule). Face à cette problématique, les solutions envisageables (représentées en bleu sur la figure) feront, majoritairement, l'objet d'études dans le cadre de

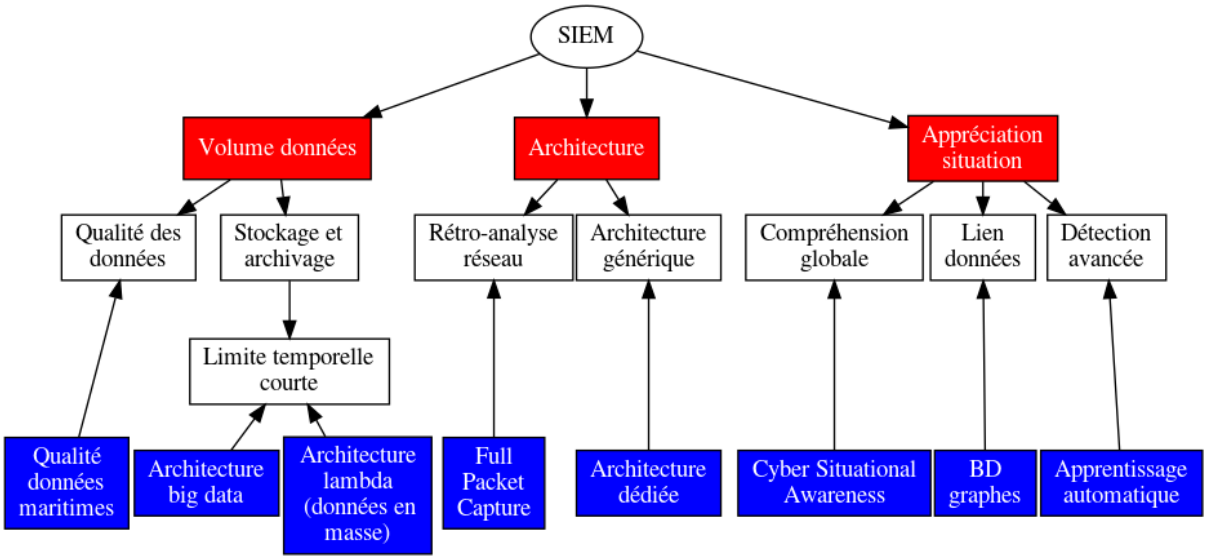

FIGURE III.2 : Limitations de l'emploi des SIEM classiques dans le contexte maritime et solutions possibles (source : archives personnelles).

cette thèse.

III.2 Appréciation de la situation

Lors d'échanges menés dans le cadre de nos travaux de recherche avec des exploitants de SOC, nous avons identifié que leur principale difficulté est liée au manque de compréhension d'ensemble des informations issues des SIEM, face à un nombre d'alertes important et à une connaissance - relative - des multiples systèmes surveillés. Ces difficultés de perception, de compréhension, de projection et de résolution rencontrées dans le contexte de la cybersurveillance nous ont permis d'établir un parallèle avec le concept de *Situational Awareness* (SA).

III.2.1 Contexte général

Une situation représente la caractéristique d'un ou plusieurs agents confrontés à des évènements, des circonstances et des relations entre objets (figure III.3) [Fer97]. Ils doivent être en capacité de se positionner et d'évaluer la situation, afin de prendre des décisions.

Les définitions, interprétations et applications de la SA sont multiples, que l'origine soit

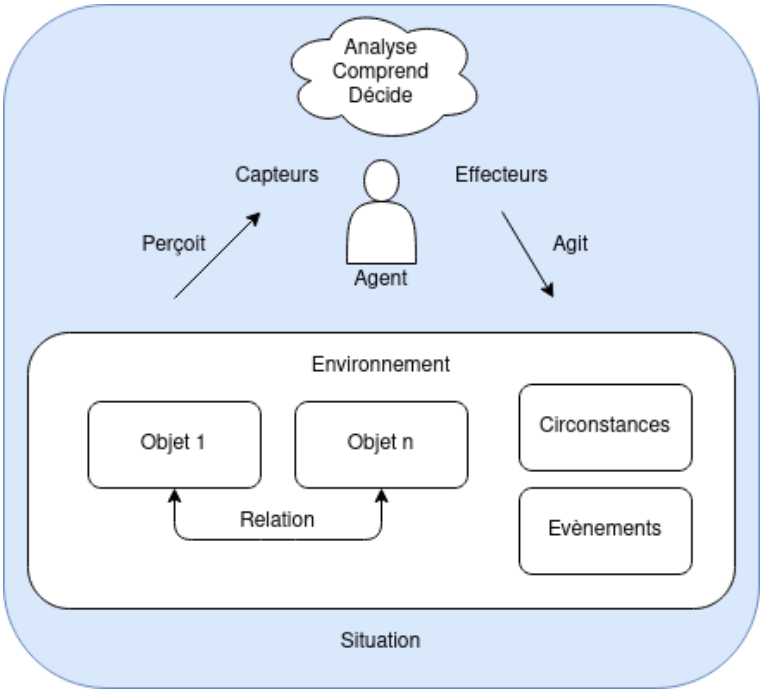

FIGURE III.3 : L'homme, en tant qu'agent, dans son environnement et faisant face à une situation (source : archives personnelles).

scientifique, militaire ou industrielle [Tad10]. Nous avons retenu la définition III.1 qui semble faire référence et qui est proposée par la chercheuse Mica Endsley, à l'origine du concept.

Définition III.1. *La Situational Awareness est la perception d'éléments d'un environnement dans un volume de temps et d'espace, la compréhension de leur signification, et la projection de leur état dans le futur proche [End95].*

La SA apporte donc, dans un volume de temps et d'espace, les notions de perception, de compréhension et de projection dans le futur proche d'une situation, dans un objectif de prise de décision par l'homme en vue d'une action par rapport à une situation.

L'OTAN recommande l'emploi du terme « connaissance de la situation » et en donne la définition III.2 suivante :

Définition III.2. *Connaissance des éléments de l'espace de bataille nécessaire pour prendre des décisions reposant sur des informations appropriées [OTA17].*

En France, le Ministère des armées parle « d'intelligence de la situation » et en donne la définition III.3 suivante :

Définition III.3. *Dans les domaines de l'anticipation stratégique comme de la conduite d'une opération, niveau de compréhension découlant de l'identification des tendances et des liens qui se développent dans le temps, dans l'espace, entre les acteurs et visant à faire leur rapprochement avec la situation observée [CIC].*

C'est donc un état de connaissance (« *state of knowledge* », selon les propres termes d'Endsley), alors que les processus organisationnels ou techniques d'acquisition, de traitement et d'analyse sont regroupés sous le vocable *Situation Assessment*. Ils contribuent directement à l'élaboration de la SA, mais constituent plus des processus à proprement parler qu'un objectif cognitif. Dans un contexte militaire, le Ministère des armées français suggère de traduire *Situation Assessment* par « appréciation de situation » et en donne la définition III.4 suivante :

Définition III.4. *Procédé de raisonnement logique qui permet au chef de prendre en considération tous les facteurs influant sur la situation militaire et d'arriver à une décision concernant la conduite à adopter en vue de l'accomplissement de sa mission*[1] *[CIC].*

Le processus d'acquisition, de traitement et d'analyse des données (*Situation Assessment*) s'appuie sur deux grandes familles de données, à savoir celle concernant notre propre

1. Dans le cadre militaire maritime, la mission pourrait être considérée comme une circonstance particulière (par exemple : projection d'un navire de combat sur une zone maritime pour accomplir une mission).

situation (*Knowledge of Us (KU)*) d'une part, permettant de disposer d'une connaissance suffisante de son propre état (position, état de fonctionnement...) et, d'autre part, celle regroupant les données relatives à autrui (position dans le temps et l'espace, savoirs, capacités, intentions...), regroupées sous le terme de *Knowledge of Them (KT)*.

On peut comprendre l'état de connaissance apporté par la SA en réponse à trois questions, d'une complexité et d'un niveau de maturité croissants : pour la *Situation Perception*, c'est la réponse à la question « Quels sont les faits actuels ? », pour la *Situation Comprehension*, c'est la réponse à la question « Que se passe-t-il ? », pour la *Situation Projection*, c'est la réponse à la question « Qu'est-ce qui est le plus probable de se produire si ? ». Endsley établit ainsi un modèle à 3 niveaux (*Layer 1 SA*, *Layer 2 SA*, *Layer 3 SA*). À l'état de connaissance apporté par ces couches, Mc Guinness & Foy suggèrent d'ajouter un quatrième niveau, appelé « *Situation Resolution* », qui ambitionne d'avoir connaissance des possibilités de résolution et donc de faciliter la prise de décision en répondant à la question « Que dois-je faire exactement ? » [McG00]. Ce quatrième niveau constitue une appréciation aujourd'hui essentiellement humaine, qui se base sur des processus - généralement techniques - de niveau inférieur, qui peuvent être normalisés et automatisés et qui s'appuient eux-mêmes sur des informations issues de capteurs. Cette aide à la décision doit aussi proposer des options pour le décideur en ayant identifié, pour chacune d'entre elles, les impacts possibles. L'effet final recherché de la SA consiste à permettre une supériorité informationnelle (*information superiority*, voire *information dominance*) et décisionnelle (*decision superiority*) face à une situation. La figure III.4 constitue une synthèse de l'ensemble.

Enfin, il apparaît opportun de noter que, sur des systèmes de systèmes complexes, l'état global de connaissance apporté par la SA peut être composé de plusieurs SA plus « thématiques ». En revanche, pour atteindre une compréhension globale, Franke et Brynielsson soulignent que l'intégration de la SA « thématique » dans la SA globale s'avère indispensable [Fra14]. La SA globale peut être vue sous la forme d'une fusion de SA intermédiaires. Cependant, au même titre qu'une SA intermédiaire est un état de connaissance, la SA globale l'est aussi. Concrètement, elle doit permettre, par exemple, de détecter une relation de cause à effet entre la connaissance d'une situation cyber dégradée et la connaissance consécutive ou simultanée d'une situation dégradée d'un système de contrôle d'accès ou d'un équipement cyber physique. Certains écueils significatifs demeurent cependant sur le sujet de la fusion des SA. En effet, sans abstraction suffisante, le risque de submersion par la quantité d'information obtenue des SA intermédiaires ne saurait être négligé car aucune tendance ou compréhension ne se dégagerait pour permettre la compréhension et donc la connaissance.

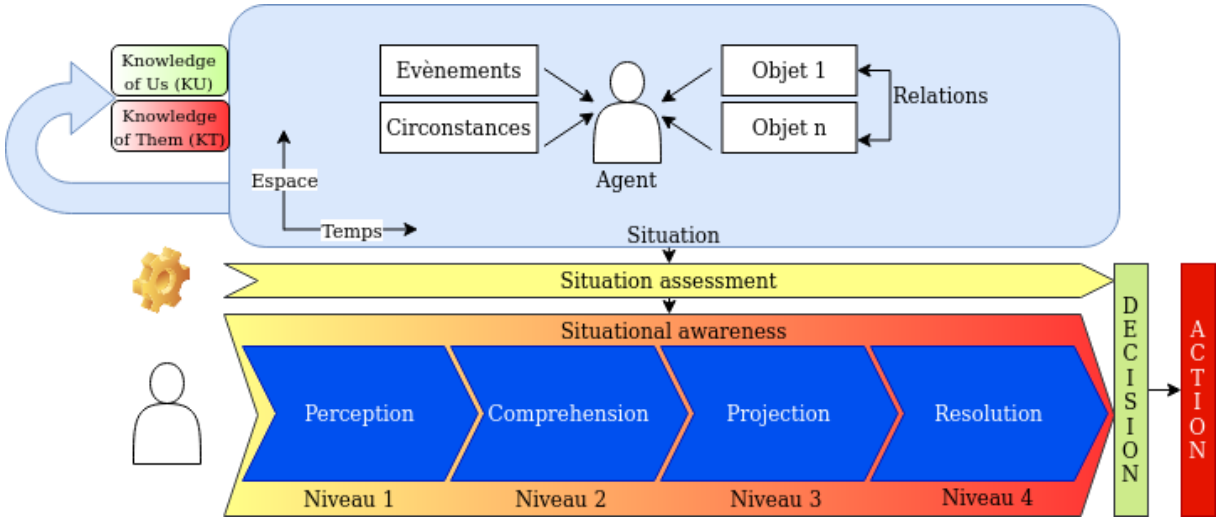

FIGURE III.4 : Modèle d'élaboration de la *Situational Awareness* d'après Endsley [End95], adapté avec la composante *Situation Resolution* suggérée par Mc Guinness & Foy [McG00] (source : archives personnelles).

Ensuite, l'intérêt d'une SA globale réside dans l'existence, la richesse et la qualité des SA intermédiaires : il apparaît donc indispensable de les mettre en perspective.

Un point difficile pour la réalisation de la fusion des SA intermédiaires repose sur le fait qu'elles n'existent pas nécessairement ou, au mieux, que leur compatibilité n'est pas assurée. En effet, aucune norme ni standard d'échange ne permet aujourd'hui d'intégrer les différentes SA et toute tentative en ce sens nécessite donc un effort particulièrement important. Pour aboutir à cette SA globale, en sortie du modèle d'Endsley pour un système, l'existence d'une étape de normalisation avant l'export de la SA intermédiaire serait nécessaire. Dans les premières étapes du processus de constitution de la SA globale (*perception* et *comprehension*), les SA intermédiaires doivent également pouvoir être corrélées entre elles, le plus probablement par le biais de scénarios hauts s'appuyant sur des évènements redoutés, ou par une approche plus géographique si les évènements se produisent, par exemple, sur un même site, voire dans un même local.

III.2.2 Première application de la SA dans un contexte aérien

Développé en premier lieu pour son utilisation dans le contexte aérien militaire par Mica Endsley, l'objectif de la SA consiste à fonctionner efficacement en temps de paix et en temps de crise. Le collimateur tête haute (*Head Up Display (HUD)*) (figure III.5), est régulièrement suggéré comme l'exemple parfait de l'information que le pilote doit avoir à

Tableau III.2 : Exemples de données KU et KT pour l'élaboration de la SA aérienne

Exemples KU
Valeurs environnementales
Défauts de fonctionnement capteurs et systèmes
Position, navigation, temps

Exemples KT
Détection radar ennemi
Détection guerre électronique ennemie
Détection missile ennemi

sa disposition pour réagir correctement et promptement face à une situation. Véritable aide pour la prise de décision en vol, l'instrument ne remplace ni le pilote ni son environnement, mais s'interface entre les deux. Par exemple, en temps de paix, le collimateur tête haute donne au pilote les informations relatives à sa position actuelle et future dans l'espace. Il dispose ainsi des informations essentielles sur une surface de quelques dizaines de centimètres carrés et éventuellement de quelques écrans supplémentaires [Foy05]. La plupart des informations affichées proviennent de capteurs physiques (cap, vitesse, altitude, angle d'attaque, puissance moteur, pression extérieure, *etc...*) et d'informations logiques (route à suivre, disponibilité des installations embarquées, *etc...*). L'ensemble des connaissances relatives à son propre environnement est évoqué sous le terme de « connaissance de soi » (« *KU* ») [Tad10]. Le collimateur tête haute affiche également des informations relatives aux autres aéronefs à proximité, « hostiles » ou non, et leur évolution par rapport à l'aéronef du pilote. Enfin, à bord des aéronefs militaires, les capteurs embarqués bénéficient de fréquentes mises à jour pour améliorer les capacités de détection de l'ennemi à l'aide d'équipements de guerre électronique. La détection d'un aéronef ou d'un radar ennemi, du lancement d'un missile et de leurs évolutions dans le temps et dans l'espace peuvent être regroupées sous le terme « connaissance de l'autre » (« *KT* »). Le tableau III.2 synthétise ainsi quelques exemples de données KU/KT pour l'élaboration de la SA aérienne.

Le succès rencontré par le collimateur tête haute a entraîné sa généralisation à l'ensemble des aéronefs de combat (où la rapidité de décision est essentielle dans un contexte cinématique rapide), puis sur les avions de ligne commerciaux récents, et même sur des véhicules à destination des particuliers. De nouvelles fonctionnalités se sont rajoutées au collimateur tête haute, comme l'affichage d'informations issues du protocole *Traffic Collision Avoidance System (TCAS)*, qui accompagnent l'aide à la résolution de situation en cas de risque de collision entre deux aéronefs [2]. La résolution est réalisée en ordonnant des manœuvres opposées aux deux aéronefs [Kuc07]. Pour autant, le rôle de l'homme n'est jamais

2. Ce protocole présente plusieurs similitudes avec l'AIS, y compris en termes de vulnérabilités face à une menace à base de radio logicielle [BSG+20].

FIGURE III.5 : Collimateur tête haute d'un avion civil Bombardier CRJ-900 en longue finale de l'aéroport de Münich (source : Wikimedia Commons, image non modifiée, auteur : Joschiki, licence : CC BY-SA 3.0).

négligé : le pilote et les centres de contrôle radar demeurent responsables de la détection des aéronefs dans leurs zones de responsabilité, mais aussi de la prise de décision finale. Des canaux de communication existent également entre les aéronefs et les centres à terre pour permettre le partage de l'information, et par conséquent l'élaboration de la SA aérienne finale à une échelle plus large (*Automatic Dependent Surveillance-Broadcast (ADS-B), Aircraft Communications and Reporting System (ACARS)*).

III.2.3 Application de la SA au contexte maritime

Un objectif majeur des acteurs du monde maritime consiste également à aboutir à l'état de connaissance fourni par la SA, parfois sans en avoir pleinement conscience. Les données issues des capteurs d'un navire sont généralement centralisées avant d'être fusionnées et présentées à l'officier de quart en passerelle. Sur les navires récents, un grand nombre d'écrans y sont ainsi disposés pour afficher des informations de type KU, comme la position et la

Tableau III.3 : Exemples de données KU et KT pour l'élaboration de la SA maritime civile ou militaire

Exemples KU
Valeurs environnementales
Défauts de fonctionnement capteurs et systèmes
Position, navigation, temps
Valeurs capteurs et actionneurs
Données radar et sonar

Exemples KT
Détection radar ennemi
Détection guerre électronique ennemie
Détection missile ennemi
Automatic Identification System
Flux de renseignement

cinématique actuelle et projetée (calculée à partir de la vitesse fond, du cap, de la vitesse angulaire, de la dérive...), les ordres d'allure ou les alarmes incendie/voie d'eau. Ces écrans multifonctions permettent également d'afficher des informations de type KT. On y retrouve la position des navires à proximité, par exemple par l'utilisation de l'AIS. Certains écrans affichent également la fusion d'informations KU et KT. C'est le cas pour la « SA surface », où la propre position du navire est fusionnée, sur le même écran, avec les positions AIS des autres navires et autres échos. De manière similaire avec le contexte aérien du protocole TCAS, les informations issues de l'AIS et du radar de navigation présentent un intérêt majeur dans la détection des risques de collision avec d'autres navires (*Closest Point of Approach (CPA)*). Des solutions identiques permettront l'élaboration de la SA pour les navires autonomes de surface à partir de centres distants [Por14]. Le tableau III.3 synthétise quelques exemples de données KU et KT pour l'élaboration de la SA maritime (civile ou militaire).

Comme pour le contexte aérien, sur les navires militaires, les capteurs et systèmes de calcul associés à bord sont mis à jour pour améliorer les capacités de détection et d'identification des menaces ennemies. Les navires peuvent également échanger des informations entre eux et vers des centres à terre, pour permettre le partage d'information et l'élaboration d'une SA maritime étendue ou globale. Contrairement au contexte aérien, les contraintes d'intégration à bord d'un navire sont généralement moindres, le volume disponible pour l'installation de capteurs ou de serveurs étant plus important et les aspects certification moins contraignants dans la plupart des cas. Ceci explique, en partie, la présence de nombreux écrans et le moindre besoin de fusion des SA en passerelle ou encore, pour le moment, l'absence de recours aux HUD ou à la réalité augmentée. En-dehors des standards proposés par l'association *National Marine Electronics Association (NMEA)* [A$^+$02, All], aucun protocole ni norme n'existe pour le partage d'information entre les équipements. En conséquence, la SA ne s'obtient pas par le biais d'un ou deux écrans et d'un collimateur tête-haute, mais souvent au travers d'une quantité importante d'écrans. Sur les navires récents, des écrans multifonc-

tions (*Multi-Functions Display (MFD)*) apportent une transition possible entre plusieurs visualisations qui permettent d'obtenir alternativement différentes SA, chaque visualisation pouvant aussi offrir la possibilité d'afficher et de réaliser des options de commande (ordres vers la machine, ouverture et fermeture de mécanismes, acquittement d'alarmes, *etc.*).

À bord d'un navire et au sein des ports et des organisations de surveillance, des outils de type *Vessel Traffic Service (VTS)* à terre, ou *Electronic Chart System (ECS)* et ECDIS à bord permettent la perception et la compréhension de la situation maritime dans une optique de prise de décision [KHL+21]. Les VTS (*cf* figure III.6) et les ECDIS (*cf* figure III.7) modernes permettent d'élaborer une situation tactique maritime en fusionnant les informations obtenues de différents capteurs et bases de données et leur affichage. C'est également le cas des systèmes de combat (*Combat Management System (CMS)*). Dans le cas des systèmes présents en passerelle ils remplacent, d'une part, l'utilisation d'une carte papier pour le suivi de sa propre position et sa projection et, d'autre part et en partie, l'écran radar pour le suivi de la situation de surface. Ils permettent aussi une certaine forme de projection : estimation de la position future, (calcul de l'*Estimated Time of Arrival (ETA)*, par exemple) et éventuellement le calcul d'alarmes de prévention des collisions (CPA). L'aide à la décision humaine (*situation resolution*) reste encore assez peu présente dans les versions actuelles, mais fait l'objet de nombreuses annonces pour les années à venir de la part des constructeurs d'électronique maritime.

Comme évoqué précédemment, sur un navire, plusieurs SA « thématiques » peuvent coexister, comme la SA physique (protection du navire), la SA incendie, la SA maritime de surface, la SA aérienne ou la SA cyber, sans qu'aucune fusion de ces différentes SA ne soit aujourd'hui effective, essentiellement par manque de protocole et de normes d'interconnexion, mais aussi parce que la fusion pourrait rendre complexes la compréhension et la visualisation. Un projet européen, SAURON, mène des recherches sur la fusion de différentes SA dans un but d'hypervision [3]. En synthèse, si le capitaine d'un navire se doit d'avoir une bonne vision de son environnement maritime immédiat et de la cohérence de la cinématique de son navire, du fonctionnement de ses installations, il ne dispose aujourd'hui d'aucune fusion des SA ni d'intégration de la cyberdéfense dans sa SA.

3. https://sauronproject.eu/publication.php?id=28

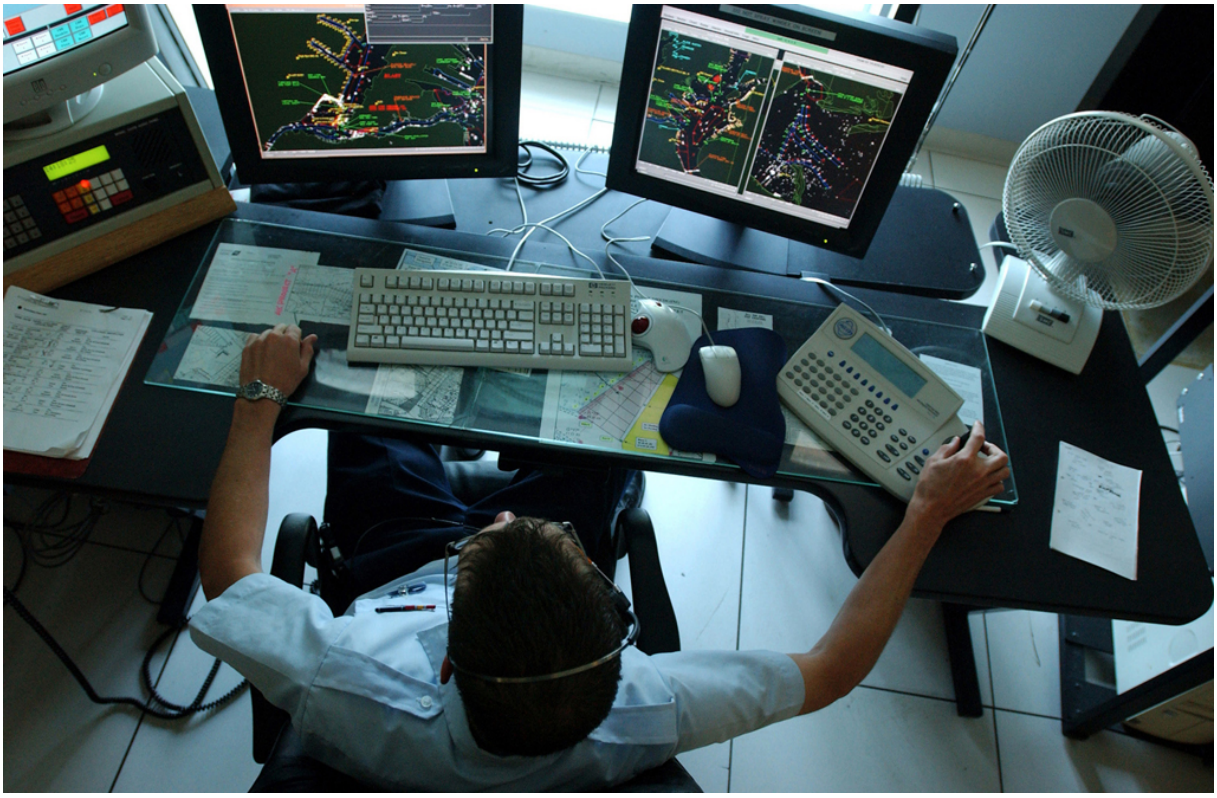

FIGURE III.6 : Opérateur VTS des *US Coast Guards* (source : Wikimedia Commons, image non modifiée, auteur : *US Coast Guard*, licence : domaine public).

III.2.4 Processus métiers pour la *Cyber Situational Awareness*

La *Cyber Situational Awareness (CSA)* constitue l'application du modèle d'Endsley aux enjeux et au contexte particuliers du cyberespace. Cette déclinaison a permis à plusieurs chercheurs de proposer des améliorations ou des précisions par rapport au modèle initial, mais qui restent en grande partie valables aussi pour d'autres domaines d'emploi. Ainsi, Barford *et al* [Bar10] établissent que la CSA est reconnue comme efficace lorsque sept processus sont élaborés pour aboutir à l'état de SA.

Le premier processus consiste à établir la connaissance de la situation actuelle (*situation perception*, P1), essentiellement à partir des données collectées par les capteurs cyber. Le deuxième processus doit permettre d'évaluer l'impact de l'attaque sur les systèmes d'information et les processus métiers et l'évolution de cet impact si aucune action n'est décidée (*impact assessment*, P2). Pour cela, le processus s'appuie sur la connaissance de ses propres vulnérabilités (*vulnerability assessment*) et l'évaluation de la menace (*threat assessment*). Souvent réalisée en parallèle des autres processus, la connaissance de l'évolution de la situation dans le temps constitue une fonction essentielle de pilotage (*situation tracking*, P3).

FIGURE III.7 : Exemple d'interface homme/machine d'un ECDIS (source : Wikimedia Commons, image non modifiée, auteur : Hervé Cozanet, licence : CC BY-SA 3.0).

La compréhension du comportement de l'attaquant (*attacker's perception*, P4) a pour objectif de déterminer l'évolution probable de l'attaque (*situation projection*, P7), en croisant la connaissance de l'attaquant (KT) avec les vulnérabilités des systèmes à défendre (KU) et en déterminant plusieurs scénarios plausibles en fonction des intentions probables de l'attaquant, des opportunités et de ses capacités. Afin d'éviter la reproduction de l'évènement et de rechercher une imputation, il apparaît aussi essentiel d'avoir la connaissance de l'origine de l'attaque (pourquoi, comment) (*causality assessment*, P5). Enfin, le niveau de qualité des éléments qui constituent la CSA (*quality assessment*, P6) doit être évalué en continu, pour garantir la pertinence du modèle d'Endsley et des conclusions résultantes du déroulement des différents processus. Ce point peut être considéré comme faisant partie du processus de *situation perception*.

Les sept processus apparaissent complémentaires : l'élaboration d'une CSA exhaustive et de qualité nécessite qu'ils soient tous réalisés et évalués. Une CSA dont l'un des éléments

manquerait deviendrait incomplète. Les processus sont également interdépendants : un processus à la qualité approximative aurait un impact sur la qualité des autres et de l'ensemble. Ainsi, la qualité globale de la CSA dépend du processus P6 qui fixe des critères de qualité pour les entrées et sorties de chaque processus : le niveau de qualité global de la CSA résulte donc de la qualité individuelle de chaque processus. Les processus sont essentiellement élaborés à partir de paramètres ou d'informations obtenus sur les systèmes d'information surveillés ou dépendant de critères de qualité du capteur. Ils peuvent également être fonction la qualité de facteurs exogènes. Ainsi, l'élaboration de certains processus nécessite d'avoir recours à des informations de sources externes (par exemple, du Renseignement d'Intérêt Cyber (RIC)). L'appréciation de ces critères repose essentiellement sur l'homme : si les éléments peuvent et doivent être acquis, transmis, traités et affichés par la machine, leur appréciation finale (cohérence, incohérence, qualité) faire encore souvent appel à l'homme. Enfin, tel que représenté à la figure III.8, la maturité et la complexité croissent de la gauche vers la droite et du bas vers le haut du modèle : ainsi, il est plus complexe et plus abouti de déterminer l'évolution future de la situation que de détecter une menace actuelle. La prise de décision constitue également un processus complexe, car elle fait appel à l'homme et à la machine. Il n'apparaît pas non plus envisageable de vouloir tenter d'établir une projection de la situation sans en avoir au préalable la perception. Enfin, il convient de noter que l'élaboration de la CSA s'effectue en analysant des éléments KU et KT connus *a priori* (cartographie, indices de compromission, scénarios) en relation avec des éléments KU et KT *in vivo* (*observables*).

La figure III.8 propose une visualisation du modèle de Barford des processus constitutifs de la CSA. Dans le cadre de nos travaux, nous avons adapté ce modèle par rapport à [Bar10], afin que le processus de projection ne soit pas rattaché au niveau *situation comprehension*, mais aussi dans la perspective de rajouter deux processus. En effet, le modèle de Barford n'intègre pas la proposition de [McG00] de rajouter le processus de *situation resolution*. Nous proposons donc l'ajout de deux processus associés à ce niveau. Le premier, *resolution anticipation*, a pour objectif d'anticiper la résolution d'une situation cyber en écrivant des scénarios basés sur les meilleures pratiques, mais également en capitalisant sur des incidents s'étant déjà produits (*playbook*). Le second processus, *resolution assessment*, a pour objectif d'évaluer le meilleur scénario de résolution et de mesurer ses impacts éventuels sur le système d'information et les processus métiers. Enfin, les SOC et CSIRT sont parfois inter-connectés et peuvent échanger des informations en temps réel sur la détection et le traitement des incidents en utilisant des standards comme *Structured Threat Information eXpression (STIX)* et *Trusted Automated eXchange of Indicator Information (TAXII)* : le partage et la fusion vers les niveaux supérieurs ou inter-SOC et inter-CSIRT constituent donc des fonctions es-

sentielles. Les SOC et CSIRT doivent également rendre compte de la SA à des échelons de direction et de commandement, avec un niveau d'abstraction cohérent.

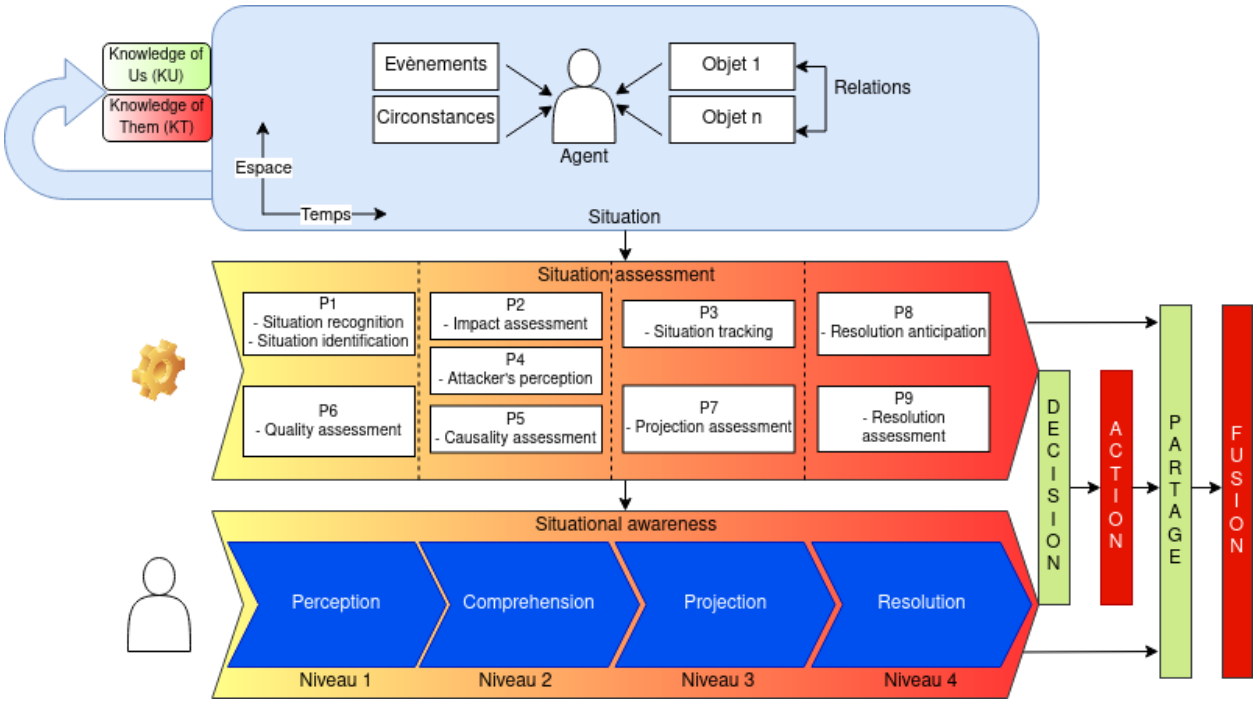

FIGURE III.8 : Processus constitutifs de la CSA, travail adapté de Barford et Mc Guinness & Foy [McG00] et prenant en compte les remarques de Franke et Brynielsson [Fra14] (source : archives personnelles).

Le concept de CSA reste un sujet de recherche actif. Peng Liu a ainsi analysé les principales questions de recherche associées à la CSA (figure III.9), auxquelles on pourrait également rajouter celles relatives à la résolution de la situation présentées dans le même article [Bar10]. Nos travaux ont permis de contribuer à ces sujets, à l'exception de la réduction des risques et du doute, à la gestion des hypothèses et à l'apprentissage automatique.

En s'appuyant sur les données issues des capteurs, les processus d'appréciation de la situation (*situation assessment*) en vue de l'obtention de la CSA doivent fournir des outils automatisés ou des interactions humaines permettant la prise de décision, afin de réagir à une menace cyber volontaire ou involontaire [Onw12]. Dans le contexte cyber, les informations KU sont essentiellement composées de flux temps réel dirigés vers un SIEM et parfois associées à des bases de données (gestion d'actifs ou base de vulnérabilités des systèmes d'information). Les informations KT sont principalement constituées de données issues du RIC, soit par l'emploi d'indicateurs de compromission (*Indicator of Compromise (IoC)*), soit directement par l'utilisation de signatures de détection grand public ou privées. Les

FIGURE III.9 : Principales questions de recherche de la CSA, d'après Peng Liu [Bar10] (source : archives personnelles).

Tableau III.4 : Exemples de données KU et KT pour l'élaboration de la CSA

Exemples KU
Connaissance du patrimoine numérique
Connaissance des flux réseaux
Métadonnées issues des capteurs

Exemples KT
IoC obtenus à partir de la CTI : adresses IP, de courriel, noms de fichiers, condensats de fichiers ou JA3, noms de domaine...
Signatures des capteurs (publiques ou privées)
TTPs, détections temps-réel

IoCs peuvent ainsi être constitués par des noms de fichiers ou des condensats, des noms de domaines, des adresses IP ou de courriel. Mais le RIC apporte également d'autres informations précieuses pour la SA, comme les TTP, qui détaillent les habitudes et techniques de groupes d'attaquants. Le tableau III.4 synthétise quelques éléments de KU/KT pour le contexte cyber.

Après avoir analysé les trois contextes (air, mer, cyber) et les KU/KT correspondants, nous proposons d'en réaliser une synthèse (tableau III.5). Si les capteurs à l'origine des KU/KT diffèrent, la variété des capteurs et l'hétérogénéité des données sont similaires. L'échange de l'information et l'abstraction vers des niveaux supérieurs représentent également des capacités essentielles.

Tableau III.5 : Exemples de similitudes de données KU et KT pour l'élaboration des SA air, mer, cyber

	Air	**Mer**	**Cyber**
KU temps réel	Capteurs, calculateurs, HUD et écrans	Capteurs, calculateurs et écrans	Flux de métadonnées des capteurs cyber (NIDS, HIDS...)
KT temps réel	Radars, IFF, guerre électronique	Radars, guerre électronique, sonars	Alertes des capteurs cyber et IoC
Mise à jour des capteurs par rapport à la menace	Principalement capteurs militaires (mise à jour des cibles, signatures)	Principalement capteurs militaires (mise à jour des signatures des radars ennemis)	Mise à jour des capteurs cyber embarqués NIDS/HIDS avec des signatures privées, publiques ou des IoCs
Partage de SA	TCAS, ADS-B, ACARS, radio	AIS, radio et autres	STIX/TAXII

Comme évoqué précédemment, un débat de recherche persiste sur la méthode de partage de la CSA. Franke et Brynielsson rappellent que la CSA ne constitue pas une SA à part entière, mais qu'elle doit s'intégrer dans une SA globale [Fra14]. Cependant, l'organisation actuelle des SOC consiste aujourd'hui en une organisation séparée des autres centres de décision où les SA « sectorielles » sont fusionnées [Zim14]. La SA globale intègre donc difficilement la SA cyber.

III.3 Modélisation de la *Maritime Cyber Situational Awareness*

Dans cette section, nous évoquons la modélisation des processus métiers et fonctionnels qui permettent l'élaboration de la MCSA. À l'instar de la figure III.8, cette modélisation des processus métiers doit permettre d'identifier les capteurs nécessaires à l'élaboration de la MCSA qui figureront dans l'architecture technique. La modélisation de l'architecture fonctionnelle doit, quant à elle, permettre d'identifier les différents flux d'information, de fusion et de traitement nécessaires à l'élaboration de la MCSA. À chaque étape, les spécificités du monde maritime identifiées en figure II.5 devront être correctement prises en compte.

III.3.1 Exemple d'état de connaissance de la MCSA

En tant qu'état de connaissance, la MCSA peut être vue comme la somme de connaissances élémentaires projetées dans le temps et l'espace (réel et virtuel) propres au monde maritime. La définition III.5 propose un exemple de l'état de connaissance qui pourrait être acquis à la suite de l'élaboration de la MCSA :

Définition III.5. *Le système d'information maritime [appellation du SIM] fait l'objet d'une cyberattaque depuis [heure]. L'attaque a pour origine [origine] et pour objectif [objectif]. Les impacts sont [impact_confidentialité, impact_intégrité, impact_disponibilité]. La cause de l'attaque est [cause_identifiée]. L'attaquant dispose de [visibilité_attaquant, moyens_attaquant]. La chronologie de l'attaque est [chronologie]. La cyberattaque pourrait se poursuivre par [projection_attaque]. Pour assurer la continuité et la reprise de l'activité et revenir à une situation nominale sûre, il conviendrait de prendre les mesures de court terme et de long terme [solutions_résolution] et d'informer [SA_globale].*

III.3.2 Modélisation d'une cyberattaque : l'exemple du modèle ATT&CK du MITRE

Si plusieurs possibilités existent pour définir les modes d'attaque, elles ne présentent cependant pas toutes les mêmes objectifs ni la même portée [Mav17, Al-16]. Partant de ce constat et de la nécessité de mieux détailler les modes opératoires de l'attaquant, l'organisation MITRE a développé le *framework* « MITRE ATT&CK™ » (*Adversarial Tactics, Techniques, and Common Knowledge*), qui formalise et modélise les différentes attaques qui peuvent viser un système d'information, ainsi qu'un répertoire d'analyse cyber [4] [Str17]. Ce *framework* émet les hypothèses que, d'une part, le défenseur dispose de connaissances importantes sur les TTP de l'attaquant et que, d'autre part, la détection des menaces par un antivirus manque de fiabilité face à des menaces de type *Advanced Persistent Threat (APT)*. En effet, l'attaquant, par recours à l'obfuscation, peut vérifier l'insensibilité des antivirus du marché à la charge qu'il conçoit. Le concept part donc du principe que les défenses classiques seront contournées et il se focalise sur l'analyse comportementale, en utilisant un modèle basé sur la menace et régulièrement mis à jour.

Plusieurs critiques peuvent être posées sur ce *framework*. Nous pouvons en formuler cinq principales. Premièrement, par rapport au cycle de vie d'une cyberattaque, le modèle

4. Voir https://car.mitre.org/

MITRE se positionne logiquement après la phase d'exploitation. Il ne cherche pas à assurer une détection des phases de reconnaissance, de préparation de l'armement, de délivrance de la charge ou de l'*exploit* à proprement parler : le modèle de détection se veut donc avancé, mais tardif dans la « *cyber kill chain* » [Yad15] [5]. Deuxièmement, pour s'avérer efficace, il doit être appliqué sur l'ensemble du système d'information de l'entreprise et disposer des capteurs et de la centralisation associés et paramétrés, afin par exemple de détecter un déplacement latéral. Par conséquent, le système d'information doit disposer d'un haut niveau de maturité en termes de cybersécurité [6]. Troisièmement, du fait de son positionnement post-exploitation, il se concentre essentiellement sur l'analyse de valeurs système par des capteurs pour assurer la détection, au détriment de l'analyse du réseau, par exemple ([Str17], §1.2). Quatrièmement, s'il apparaît approprié aux systèmes d'exploitation présents sur les systèmes d'information d'une entreprise, il s'applique difficilement à une partie des *Industrial Control System (ICS)*, notamment en ce qui concerne les automates, car le modèle se concentre sur les systèmes d'exploitation grand public comme Microsoft™ Windows™ ou GNU/Linux. Cinquièmement, le *framework* ATT&CK™ se focalise aujourd'hui sur l'identification de fonctions légitimes (par exemple, des fonctions système comme *schtasks.exe* sous Microsoft Windows) qui pourraient être exploitées à des fins de cyberattaque, mais ne s'appuie pas sur des IoC existants qui pourraient être diffusés par le biais du RIC. Ces limitations freinent donc son application sur les SIM, ou en tous cas établissent que le modèle seul s'avère insuffisant : l'étape de reconnaissance préalable à une cyberattaque demeure susceptible de générer beaucoup de bruit et de faux positifs au niveau des capteurs NIDS et rendre difficile la détection d'une menace avancée telle que recherchée par le *framework* ATT&CK™. En revanche, la détection précoce d'une menace s'avère plus efficace si l'étape de reconnaissance est incluse dans le processus de détection. L'emploi du *framework* seul permettra de détecter des menaces plus avancées, mais à une phase de réalisation plus tardive, freinant ainsi les capacités d'action. Il doit donc être considéré comme une étape parmi un ensemble de mesures de détection qui s'appuient sur des modèles génériques, mais avancés, d'attaques. Les figures C.1 et C.2 en annexe C modélisent un exemple d'attaque sur un système maritime de type ECDIS dans les phases pré et post-exploitation, ainsi que les contre-mesures qui pourraient permettre une détection.

L'identification de ces moyens techniques de contre-mesures doit être considérée comme une démarche indispensable à réaliser en parallèle de l'identification des phases d'exploita-

5. Depuis, MITRE a également développé un modèle de *framework* sur les phases préalables à l'exploitation, appelé MITRE PRE-ATT&CK Matrix™ : https://attack.mitre.org/matrices/pre/.

6. Cela sous-entend par exemple, de disposer d'un système totalement cartographié, de capteurs cyber ou encore d'un SOC. Voir également l'ISO/IEC 21827 :2008 et le guide relatif à la maturité SSI de l'ANSSI.

tion. À ce titre, les capteurs de détection d'intrusion de type HIDS apportent des capacités de cyberdéfense essentielles. Ils offrent la possibilité de réaliser des contrôles d'intégrité cryptographiques de fichiers de configuration ou de binaires, la collecte d'évènements systèmes et de journaux d'évènements, l'analyse de conformité ou encore l'inventaire des logiciels des postes clients et serveurs. S'ils présentent l'avantage de permettre une analyse fine de la configuration et de l'intégrité d'un hôte, ils doivent en revanche être précisément adaptés à la configuration et aux logiciels installés. Par exemple, le HIDS devra être configuré pour analyser les répertoires d'installation et de configuration d'un ECDIS, faute de quoi il ne sera pas en mesure d'y détecter une modification. Quant aux capteurs de type NIDS, ils constituent des outils « historiques » de la cybersécurité qui restent assez largement déployés. Ils peuvent être exploités à de nombreuses fins, comme la détection d'anomalie basée sur des signatures ou comportementale. Ils permettent également la détection d'anomalie sur des variations temporelles ou contextuelles dans les flux réseaux (augmentation brutale de la bande passante habituelle, etc.). Ils demeurent cependant particulièrement sensibles aux faux positifs [Das14] et peu adaptés aux réseaux où l'emploi de la cryptographie serait important. Leur intérêt est cependant réel à certaines phases de la préparation ou de l'exécution de l'attaque, de même que pour la dissection protocolaire aux fins de remontée de métadonnées.
Le positionnement idéal de ces capteurs dépend intimement des architectures à surveiller : dans le contexte des navires et des infrastructures portuaires, les SIM peuvent s'avérer très variés et complexes. De manière générale, les agents HIDS doivent être déployés sur chaque poste client et serveur. Concernant les NIDS, il conviendra de considérer leur positionnement comme indispensable entre deux systèmes d'information interconnectés, entre le navire et la terre et, si possible, à l'écoute de chaque boucle réseau, notamment sur les OT (ECS/ECDIS, systèmes ICS, etc.). La fusion, la corrélation et l'analyse des données issues des deux types de capteurs revêtent donc un caractère essentiel.

III.3.3 Niveaux d'abstraction de la MCSA

Le monde militaire organise généralement les opérations selon trois strates, qui permettent de définir des niveaux d'abstraction [CIC]. Le niveau stratégique est le plus haut : c'est le « niveau de direction politique et de commandement auquel un État ou un groupe d'États fixe des objectifs nationaux ou multinationaux de sécurité et fournit des ressources nationales, interministérielles, notamment militaires, en vue de leur déploiement sur différents théâtres. » Le niveau opératif est le « niveau supérieur du commandement militaire

projeté sur un théâtre ou responsable d'une zone géographique, auquel les opérations sont planifiées, conduites et soutenues par une ou plusieurs forces en vue d'atteindre les objectifs militaires fixés par le commandement stratégique et de contribuer ainsi à la réalisation de l'effet final recherché. » Enfin, le niveau tactique est le « niveau subordonné de commandement militaire projeté sur un théâtre ou une zone d'opération, auquel des actions sont planifiées et exécutées pour atteindre des objectifs militaires de théâtre et contribuer à la réalisation de l'effet final recherché avec des moyens affectés au sein de chaque composante. » De manière simplifiée, on peut considérer que, au niveau du Ministère des armées, l'État-major des armées constitue le niveau stratégique militaire, le Commandant de Zone Maritime (CZM) le niveau opératif et le commandant du navire ou de la force constituée (groupe aéronaval, groupe amphibie) le niveau tactique. Ce type d'abstraction en trois strates peut également s'appliquer au secteur civil, où un découpage similaire pourrait être réalisé : la direction de l'armateur constituerait le niveau stratégique, le responsable d'opération par zone maritime ou type de navire le niveau opératif et le capitaine du navire le niveau tactique.

Cependant, d'autres niveaux d'abstraction doivent également faire l'objet d'une analyse dans le double contexte cyber et maritime. Le niveau de compétences en cybersécurité constitue le premier niveau. À bord du navire, le niveau tactique ne bénéficie généralement pas d'expert cyber : il doit donc disposer d'un niveau d'abstraction de l'information qui lui permette de comprendre la situation sans rentrer outre mesure dans les détails techniques. Le capitaine d'un navire civil doit ainsi savoir s'il peut continuer sa mission (*impact assessment*), si un mode dégradé s'avère disponible et les actions qu'il peut mener à son niveau (*resolution assessment*). Au niveau opératif, des experts cyber sont généralement présents (par exemple, au sein d'un SOC). Ce sont eux qui vont déterminer de nombreux éléments de la *situation assessment* et déterminer les modes d'action. Au niveau stratégique, la direction ne dispose pas toujours d'expertise haute en cyber, mais a besoin, à l'instar du capitaine du navire, de mesurer l'impact sur ses opérations et d'identifier si l'incident survenu peut également impacter d'autres SIM. Une troisième possibilité d'abstraction repose sur un aspect orienté géographie ou mission : le niveau opératif peut être lié à la zone de déploiement d'un navire : ainsi, un responsable opérationnel peut être désigné pour une zone maritime donnée (par exemple : Atlantique, Méditerranée, Pacifique). Une quatrième possibilité consiste à ne considérer qu'un type de navire en particulier. Enfin, un cinquième niveau d'abstraction doit pouvoir être réalisé pour chaque type fonctionnel de SIM (évaluation par domaine). Par exemple, il peut s'avérer pertinent de disposer d'un état de connaissance sur la situation cyber de tous les systèmes ECS/ECDIS d'une flotte (domaine navigation) ou de toutes les installations de propulsion des navires (domaine propulsion). Chaque MCSA élémentaire doit

Tableau III.6 : Besoins en termes de données techniques, d'abstraction et d'intégration dans la SA globale pour les trois différents niveaux de la MCSA

	Besoin technique	**Besoin d'abstraction**	**Besoin d'intégration dans SA globale**
Niveau stratégique	Faible à modéré	Élevé	Élevé
Niveau opératif	Élevé	Faible à modéré	Faible
Niveau tactique	Faible à modéré	Modéré	Élevé

par ailleurs pouvoir transmettre ses éléments aux SA globales (par navire ou par domaine).

Le tableau III.6 synthétise l'ensemble de ces éléments.

La modélisation retenue doit donc permettre d'intégrer ces cinq dimensions (par niveau organisationnel d'abstraction, par niveau de compétences, par zone géographique ou mission, par type de navire, par domaine fonctionnel de SIM), mais aussi de pouvoir réaliser la fusion de la MCSA dans la SA globale. L'analyse à grande échelle de réseaux multi-dimensionnels à couches hétérogènes, parfois appelés réseaux relationnels, nécessite d'identifier des modèles à la fois simples, intuitifs, représentatifs et permettant la transformation des relations inter-réseaux en graphes efficaces pour réaliser des calculs. Plusieurs modèles existent, notamment les modèles à base d'hypergraphes non orientés [Yen10], tels que représentés à la figure III.10, où l'hypergraphe non orienté (H) est composé d'un ensemble de sommets (V) et d'un ensemble d'hyper-arêtes (E). L'hypergraphe permet de représenter un ensemble de sous-graphes interconnectés.

La modélisation à base de super-réseaux (*super networks*), qui permet de représenter les interdépendances entre différents graphes [Jgu16, Zha19], constitue une alternative intéressante. L'intérêt par rapport aux hypergraphes réside notamment dans la connexion inter-couche, qui peut être réalisée au travers de nœuds particuliers, dans un mode de fonctionnement par couches plutôt que hiérarchique. Les super-réseaux permettent également une meilleure représentation et visualisation des différentes couches fonctionnelles ce qui, dans notre cas, doit nous permettre de faciliter la prise en compte des niveaux d'abstraction mentionnés. La figure III.11, utilisant une modélisation à base de super-réseaux, permet ainsi de représenter les cinq différents niveaux d'abstraction identifiés, ainsi que les interdépendances éventuelles entre les systèmes d'information. Cette modélisation pourrait également permettre d'intégrer les notions de propagation horizontale et verticale de la confiance

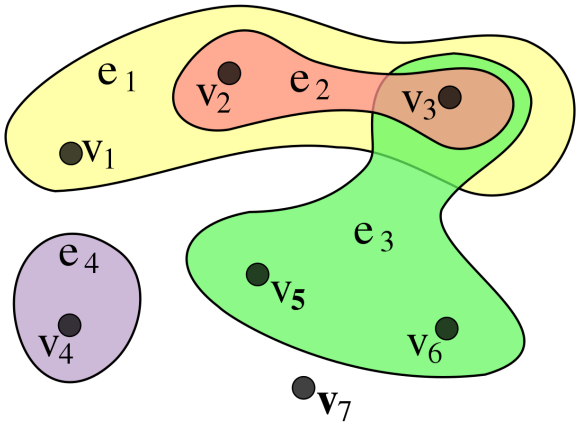

FIGURE III.10 : Exemple d'hypergraphe (source : Wikimedia Commons, image non modifiée, auteur : Kilom691, licence : CC BY-SA 3.0).

[Cos18], indispensable à l'établissement d'une MCSA de qualité.

III.3.4 Flux de données du système de cybersurveillance des SIM alignés sur les processus métiers de la SA

L'objectif de cette sous-section est de détailler les processus nécessaires à l'élaboration de la *situation assessment* dans le contexte cyber, en s'appuyant sur les processus identifiés à la figure III.8. Ces travaux sont la première étape indispensable à l'élaboration de la SA. À notre connaissance, aucun travail scientifique disponible ne s'est intéressé à l'identification et à la caractérisation de ces flux de données dans le contexte maritime. La numérotation des processus reprend celle proposée à la figure III.8. Ces processus se veulent génériques à l'établissement d'une CSA et non spécifiques, en l'état actuel, à la prise en compte des contraintes de milieu pour l'établissement de la MCSA.

III.3.4.1 P1 - *Situation recognition and identification*

Ce processus doit permettre de détecter et d'identifier l'existence et le type de cyberattaque (catégorie, libellé précis), la source (qui, quoi) et la cible (qui, quoi) [Dut13]. Ce processus constitue le premier processus de détection. En temps quasi réel (cas principal de nos travaux) ou se basant sur des investigations préventives ou réactives pour des systèmes isolés ou non surveillés, une des principales difficultés de ce processus est liée au niveau de détection : que le système soit basé sur des signatures ou des comportements, les risques

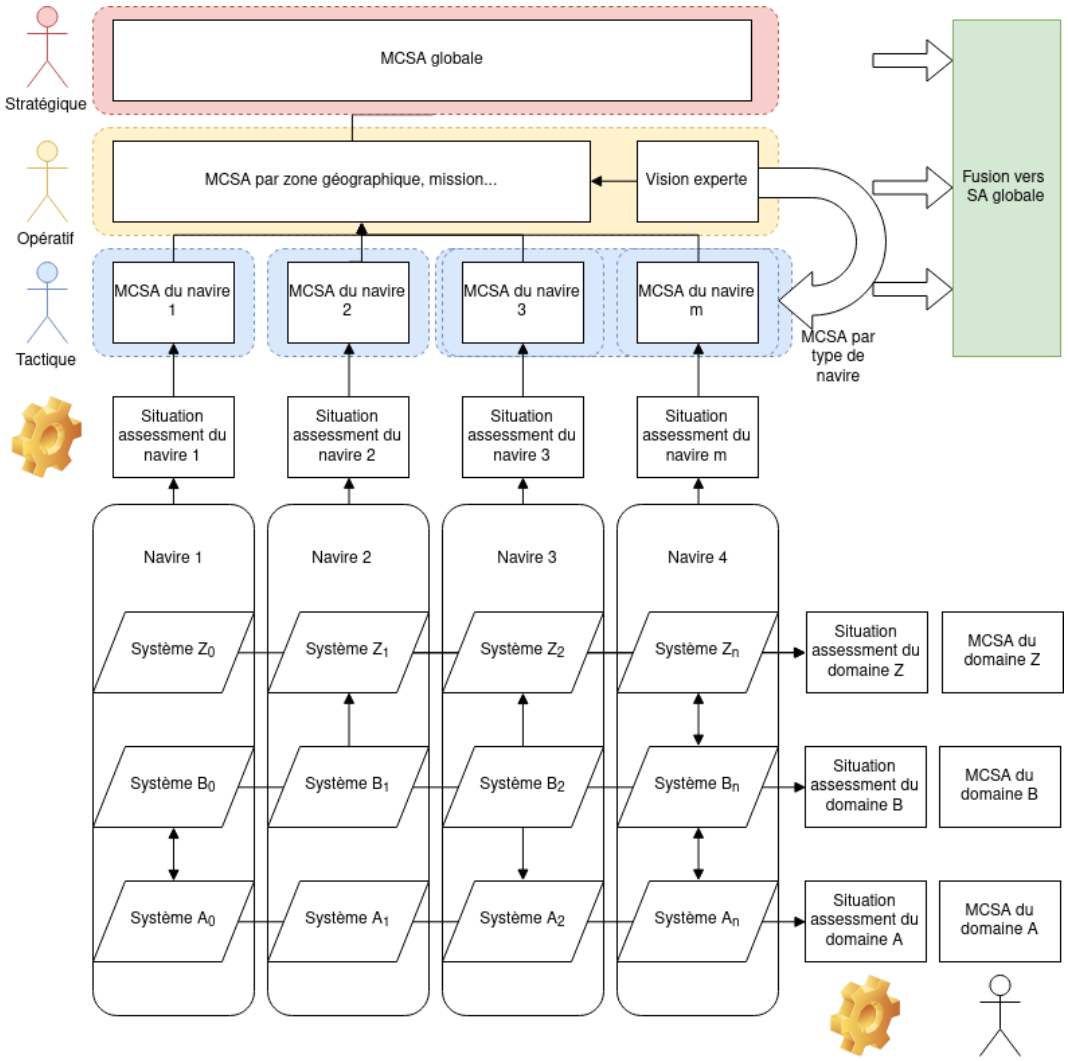

FIGURE III.11 : Modélisation de la MCSA sous forme de super-réseaux (source : archives personnelles).

de fausse alerte face à une quantité de données collectées très importante constituent un réel enjeu. Tout d'abord, le bruit de fond (constitué par les faux positifs (FP)), lié à des signatures mal adaptées, peut être si conséquent que les analystes peuvent être rapidement débordés. Cette technique peut aussi s'avérer efficace pour un adversaire pour noyer le SOC sous un déluge de détections, afin de saturer l'analyse dans l'optique de masquer une attaque plus avancée. Dans ce contexte, l'attaquant bénéficie aussi d'un avantage par rapport au défenseur, car de nombreux jeux de signatures NIDS sont constitués de données publiques (par exemple : *Emerging Threats*). Ensuite, le type de capteur, ses capacités intrinsèques (capacité d'analyse de protocole spécifique et d'extraction des métadonnées), sa configuration et les signatures qu'il utilise peuvent engendrer des faux négatifs (FN). Ce taux d'erreur (on

parle aussi de précision en calculant $\frac{VP}{VP+FP}$) est à comparer avec le taux de vrais positifs (VP) et de vrais négatifs (VN) pour déterminer la qualité de l'ensemble (on peut également calculer le rappel $\frac{VP}{VP+FN}$). Ce premier processus, le seul lié à la capture directe de données sur les SIM, est essentiel : sans une bonne qualité de détection, c'est l'ensemble des processus de *situation assessment* et de la *situational awareness* qui seront altérés, pouvant engendrer de réelles difficultés dans la compréhension de la situation et la prise de décision (myopie du décideur).

Après capture et normalisation, la comparaison entre KU et KT (métadonnée générée sur un SIM *versus* IoC d'une attaque) ou KU et KU (par exemple, valeur ou métadonnée générée à un temps t_1 *versus* sa valeur ou sa cardinalité de référence à un temps t_0) permettent de réaliser la détection d'anomalies. Le tableau III.7 synthétise le type de comparaison possible.

Pour s'avérer efficace, ce processus nécessite donc la présence de capteurs (NIDS, HIDS, producteurs de journaux de sécurité : antivirus, pare-feu, *syslog*...), de pré-processeurs adaptés aux protocoles utilisés et d'une bonne connaissance des systèmes surveillés. Le choix et le positionnement de ces capteurs dans l'architecture du SIM s'avèrent essentiels et peuvent être fonction du type de système surveillé et de son architecture réseau. Ainsi, les HIDS seront positionnés, dans la mesure du possible, sur l'ensemble des postes informatiques et serveurs des SIM du navire. Le positionnement des NIDS peut s'avérer plus compliqué sur un navire en présence de nombreux sous-réseaux. De manière idéale, un NIDS doit être positionné sur chaque boucle de réseau industriel, sur chaque réseau spécifique (navigation, communication...) ainsi qu'à chaque interconnexion entre deux réseaux (par exemple entre les systèmes d'information de passerelle et ceux liés à la propulsion, en cas de présence d'un *Integrated Bridge System (IBS)*).

Il convient également de souligner qu'une des difficultés de détection des NIDS provient du fait qu'ils ne peuvent pas toujours analyser les protocoles réseau parfois spécifiques utilisés à bord des navires (absence de dissecteur pour les protocoles industriels ou maritimes spécifiques), et ainsi ne pas disposer de signatures avancées qui apporteraient un haut niveau de précision.

III.3.4.2 P2 - *Impact assessment*

La mesure de l'impact repose généralement sur l'existence d'une cartographie physique, logique et fonctionnelle (partie connaissance) et d'un Plan de Continuité Informatique

Tableau III.7 : Comparaisons à des fins de détection

Objectif	**Exemple**
Comparaison de condensats cryptographiques	Comparaison de l'intégrité entre des éléments KU captés par un HIDS avec la base NSRL [7]. La captation peut également être réalisée par un NIDS en cas de transfert de données non chiffrées.
Comparaison d'IoC	Comparaison des données KU captées par un HIDS ou un NIDS avec les données KT issues de la CTI (adresse IP, nom de domaine, adresse de courriel, etc...) et reconnues comme employées dans des attaques récentes.
Comparaison trafic et signatures	Comparaison entre du trafic réseau (clair ou chiffré, en fonction de la couche protocolaire sur laquelle s'applique la détection) entre des données KU (transferts réseaux) et KT (signatures privées ou publiques).
Comparaison journaux et bases type Sigma [8]	Comparaison entre des données KU remontées par des HIDS ou des processus de journalisation et des expressions de type KT réputées comme régulièrement exploitées en cas d'attaque (signatures privées ou publiques).
Comparaison de métriques	Comparaison de tendances de métriques par rapport à des données KU. L'objectif est d'identifier si des métriques diffèrent d'un comportement normal habituel (KU). Par exemple : volume de données échangées sur une période de temps ou en fonction du temps, protocoles utilisés, ports TCP/UDP utilisés, *etc.* Afin de limiter la détection de faux positifs, il peut être pertinent d'utiliser l'effet cardinal de certaines valeurs afin de détecter toute nouvelle entrée.
Apprentissage automatique	Comparaison de données par apprentissage automatique supervisé ou non supervisé.

(PCI)/Plan de Reprise Informatique (PRI) ou d'une organisation de gestion de crise pour réagir face à une attaque. La mesure de l'impact est aussi intimement liée aux processus P4 (*attacker's perception*) et P7 (*projection assessment*) et à la connaissance des éventuelles vulnérabilités du SIM. En effet, la mesure de l'impact réalisée à un temps t ne peut se baser que sur les éléments dont on dispose à l'issue du processus P1. Les analyses cyber peuvent prendre du temps et la compréhension du mode d'attaque et de l'objectif final peuvent être différées. Ainsi, la partie du SIM touchée à cette date-là peut différer de l'objectif final de l'attaquant et ne représenter qu'une phase intermédiaire. Ce processus, également appelé *Impact Assessment* ou *Battle Damage Assessment* [OTA17], voire *Cyber Battle Damage Assessment* [BUTN18], pour reprendre un terme militaire, comprend l'analyse de l'impact actuel (analyse des dégâts), mais également la projection de l'impact futur de l'attaque si elle se poursuit ou si l'attaquant a la capacité d'exploiter de nouvelles vulnérabilités.

III.3.4.3 P3 - *Situation tracking*

Le processus de suivi de situation s'appuie généralement sur un outil logiciel de type SIRP. Le SIRP peut s'alimenter directement des données issues du processus P1 (après corrélation, afin d'éviter la création de multiples incidents) et jouer un rôle d'ordonnanceur vers des outils d'analyse. La principale difficulté réside dans le traitement et l'analyse d'incidents multiples, qui peuvent paraître isolés, mais en fait dépendre du même incident, ou de la même action d'ensemble. Ce processus permet d'assurer le suivi, pas-à-pas, de la situation, avec ses évolutions, les prises de décision, les mouvements de l'attaquant et l'ensemble des évènements. Ce processus s'avère essentiel à la prise de décision. En effet, il permet de regrouper sous un « cas » unique une multitude d'évènements liés, mais diffus, dans le temps ou dans le cyberespace. Il convient cependant de rappeler que l'attaquant, s'il se sait surveillé, peut également avoir recours à des techniques de leurrage (*deception*) et de déni de service. Concernant le leurrage, il va créer de multiples fausses alertes afin de créer la confusion dans les équipes d'analyse et de ralentir ou détourner la prise de décision et l'attention de la cible réelle. Concernant le déni de service, l'attaquant peut décider de saturer les systèmes de détection et de suivi avec de multiples alertes très verbeuses, afin de cacher sa véritable attaque au milieu de centaines d'alertes qui, mal ou non priorisées, détourneront les défenseurs de la cible réelle.

III.3.4.4 P4 - *Attacker's perception*

La connaissance de l'attaquant repose sur la connaissance du type d'attaque (outil, faille) et des TTP. Un attaquant peut en effet utiliser de manière récurrente les mêmes vecteurs d'infection ou les mêmes procédures dans l'exploitation de la *Cyber Kill Chain*. Connaître sa méthode permet d'anticiper la prochaine étape de l'attaque, même si les attaques peuvent aussi bénéficier d'un caractère opportuniste ou du hasard (dégâts collatéraux). Ce processus permet de connaître le comportement de l'attaquant, en partant de l'évolution de ses attaques connues et de la projection de ses intentions. Pour cela, il apparaît indispensable de connaître les TTP, généralement obtenues par le biais du RIC. Il se poursuit par le processus *Projection assessment* (P7).

III.3.4.5 P5 - *Causality Assessment*

Le processus d'évaluation de la cause s'appuie sur l'analyse des journaux et des codes malveillants (investigation numérique), mais aussi par l'enquête de terrain avec la projection éventuelle d'experts sur le lieu de l'évènement. Ce processus permet de chercher et d'identifier l'origine de l'attaque (comment), la raison de l'attaque (pourquoi) et, parfois, le qui (ou au moins un intermédiaire dans la chaîne de responsabilités). Ce critère comprend l'analyse de causalité (retour en arrière dans le temps pour identifier les différents *artefacts* précurseurs de l'incident) et d'investigation numérique (inforensique). L'analyse d'une cyberattaque et l'origine de sa cause peuvent se mesurer en jours, voire plus, ce qui rend difficile l'évaluation temps réel de ce processus. En conséquence, il est généralement traité en marge de l'établissement de la SA. Si le vecteur d'attaque peut parfois être identifié rapidement (par exemple : support USB), la cause précise, l'identité de l'attaquant ou ses motivations peuvent ainsi demeurer plus longs à établir, voire rester indéterminés.

III.3.4.6 P6 - *Quality Assessment*

Dans un contexte multi capteurs, la qualité de l'information revêt un caractère essentiel. De sa qualité contextuelle (mesure), intrinsèque (capteur) et extrinsèque (réseau) dépendra directement, par propagation, la qualité globale obtenue lors de la fusion de l'information [ML17, Bar10, Tad10]. Nos travaux s'appuient sur des capteurs existants (NIDS, HIDS, etc.) qui permettent une analyse du réseau ou du système. Nous avons donc décidé de concentrer l'essentiel de nos travaux sur les mesures de qualité de dimension intrinsèque. Ce processus

qualitatif, mené tout au long du processus de *situation assessment*, doit permettre de vérifier la qualité des éléments d'entrée (capteurs, KU, KT), avant qu'ils ne soient fusionnés puis retenus pour la prise de décision. Dans le cadre de nos travaux, nous proposons la sélection et le suivi de quatre critères de la dimension intrinsèque pour les capteurs de type NIDS. Nous avons choisi de les détailler, tout d'abord car ce sont des indicateurs quantifiables qui permettraient de valider notre modèle, mais aussi parce qu'ils restent aujourd'hui insuffisamment décrits.

Le premier critère de qualité, Q1, a pour objectif de vérifier la fiabilité du capteur (*trustworthiness*). En effet, les capteurs doivent demeurer disponibles, être intègres, disposer de signatures à jour et le lien avec le SOC doit être assuré.

Le second critère de qualité, Q2, a pour objectif de vérifier la véracité et la solidité des éléments d'entrée (véracité *truthfulness* ou solidité *soundness*). Dans certains cas, notamment dans le cas de la détection, les mécanismes utilisés reposent sur des signatures. Ces signatures, si elles sont mal écrites, peuvent entraîner des faux positifs et, si elles s'avèrent incomplètes, des faux négatifs. Comme c'est souvent le cas dans la détection d'anomalies, la vérification de ce critère s'appuie sur des jeux de données, parfois anciens, représentatifs de certaines attaques. La détection d'attaques de type *zero day* n'est donc pas envisageable par ces critères. Par ailleurs, il est souvent question de données issues de capteurs réseau uniquement (par exemple, des données enregistrées au format .pcap), et non de données multi capteurs (réseaux, journaux d'évènements...).

Le troisième critère de qualité, Q3, doit vérifier l'exhaustivité des éléments d'entrée (complétude, *completeness*). En effet, les capteurs, notamment réseau, peuvent ignorer certains paquets en entrée, ce qui peut obérer leur capacité à, par exemple, reconstruire par la suite des fichiers complets. Le lien d'élongation et les contraintes de bande passante satellite représentent autant de facteurs de pertes potentielles de données. L'objectif est donc de mesurer Q3.1, correspondant au taux de perte des capteurs NIDS, Q3.2, le taux de perte dû au lien satellite et Q3.3, la variation du nombre de paquets capturés dans le temps.

Le quatrième critère de qualité, Q4, vérifie la fraîcheur des données en entrée (*freshness*). Il correspond à la différence entre l'horodatage de la capture et l'horodatage de l'indexation dans le SIEM. On y associe également la mesure de la *timeliness* (ordonnancement horaire des métadonnées à l'arrivée à terre).

Ces quatre critères doivent nous permettre d'évaluer la qualité de l'information issue des capteurs NIDS dans le cadre de l'élaboration de la MCSA. Ils feront l'objet d'une définition

plus formelle lors de l'expérimentation sur plate-forme maritime.

III.3.4.7 P7 - *Projection assessment*

Ce processus s'avère nécessaire pour la projection dans le futur d'un évènement en cours, afin de déterminer les prochains chemins que pourrait prendre l'adversaire, en se basant sur sa perception et sur les TTP. Ce processus s'acquiert donc, d'une part, par l'analyse des intentions de l'attaquant, de ses capacités et d'un facteur d'opportunisme et, d'autre part, par la connaissance fine des chemins d'attaques éventuels établis par une cartographie précise des vulnérabilités.

III.3.4.8 P8 - *Resolution anticipation*

Ce processus a pour objectif de faciliter la prise de décision en anticipant les différents scénarios de réponse à incident possibles, aussi appelés *Course of Action (CoA)*. Face à chaque type de menace et cible potentielle sur le système d'information, ce processus permet d'établir des scénarios qui, planifiés et formalisés, facilitent et accélèrent la réponse à incident en proposant une ou plusieurs options d'action. Cette formalisation peut faire l'objet de plans de défense génériques, et de plans de continuité et de reprise par système. Il convient de noter que, en raison des niveaux d'abstraction identifiés dans le tableau III.6, cette réalisation s'avère nécessaire à différents niveaux (stratégique, opératif, tactique), les actions, priorités et modes d'exécution pouvant en effet varier d'un niveau à l'autre. L'amélioration et la consolidation permanente de ce processus et des CoA associés s'avèrent indispensables pour faire face à une menace protéiforme. Nous proposons donc de l'enrichir à partir du retour d'expérience, en fonction d'incidents internes, de l'évolution des TTP ou encore de retours d'expérience issus d'incidents externes.

III.3.4.9 P9 - *Resolution assessment*

Ce processus s'appuie, d'une part, sur la nature de l'attaque, la source, la cible et, d'autre part, sur les scénarios de *resolution anticipation* du processus P8. L'environnement (circonstances, évènements) peut cependant influer sur ce processus de décision. En effet, la position du navire, sa situation (au port, en mer, en zones d'opérations), sa cinématique, les missions ou actions qu'il doit mener dans le temps proche ou long peuvent peser sur la

prise de décision. D'autres éléments de contexte vont également intervenir, comme l'existence d'autres moyens sur zone (par exemple, si un navire peut assurer la mission de celui touché par l'attaque), de personnels déployables pour venir en aide ou encore la possibilité d'investigation ou d'action à distance. Enfin, toute décision a des conséquences : ainsi, l'isolement du lien satellite d'un navire, l'arrêt de systèmes d'information ou encore l'utilisation de sauvegardes présentent des effets directs ou indirects qui doivent être mesurés, évalués, discutés et pris en compte lors du processus de prise de décision.

C'est donc en s'appuyant sur les scénarios d'actions proposés par le processus P8, sur les éléments de contexte indiqués et sur les conséquences potentielles sur la mission du navire et de l'armateur que la décision sera finalement prise (et non sur des bases exclusivement techniques ou cyber).

Il convient également d'indiquer qu'il apparaît indispensable de vérifier que cette prise de décision est suivie d'effets et que sa réalisation, à tous les niveaux d'abstraction évoqués, s'avère effective et efficace en cela qu'elle doit interrompre l'attaque et permettre la restauration de l'intégrité, de la disponibilité et de la confidentialité des systèmes : cette partie de P9 peut également être rapprochée du processus P2 (*impact assessment*).

III.4 Apports de la visualisation pour la KU des SIM et la MCSA

La visualisation des évènements de sécurité est un enjeu majeur de la cybersécurité. De nombreux travaux de recherche, ouvrages et conférences scientifiques [9] existent sur le sujet. En France, récemment, plusieurs thèses et travaux de recherche ont été publiés en lien avec le sujet [Hum15, KDC+18]. Les enjeux de recherche demeurent importants et les difficultés liées à la visualisation restent complexes [Tad10]. En effet, dans le cas du cyberespace, même si l'on s'appuie sur des équipements physiques, la représentation que l'on peut en faire reste souvent conceptuelle et abstraite : elle ne peut en effet généralement pas être produite sur un théâtre ou un système d'information géographique, la prise en compte de mobiles en mouvement y ajoutant une complexité supplémentaire. L'intégration de la dimension temporelle dans la visualisation de la situation est également essentielle, afin de permettre un retour vers des données passées si nécessaire : les volumes d'information sont donc particu-

9. Notamment la conférence *IEEE Symposium on Visualization for Cyber Security* https://vizsec.org

lièrement conséquents et leur visualisation sur ces laps de temps importants s'avère difficile. La visualisation de la projection des données vers le futur est également un réel enjeu, qui reste envisageable pour des données continues, mais plus difficile à conceptualiser pour des données abstraites, comme la mobilité et les intentions d'un attaquant dans un système d'information. La prise en compte des spécificités des systèmes cyber physiques reste également un enjeu de recherche et la visualisation de leur fonctionnement présente un intérêt indéniable [Sic18]. Enfin, la fusion des informations et leur présentation optimale aux différents niveaux d'abstraction sont impératives pour l'obtention d'une MCSA pertinente et efficace.

Par ailleurs, une des causes systémiques des difficultés de mise en place d'une cybersécurité efficace dans le monde maritime s'explique par le manque de connaissance de ces systèmes (*cf* figure II.7). Le volume des données collectées, qui est notamment dépendant du type de capteur et de son paramétrage, doit donc permettre d'apporter une richesse et une finesse aptes à réduire cette cause systémique et permettre de disposer d'une meilleure connaissance des SIM. Ainsi, il apparaît indispensable que les travaux menés dans le cadre de cette thèse portent sur deux biens essentiels pour cartographier un SIM : l'analyse du réseau, afin de comprendre les échanges au sein du SIM et entre SIMs, et l'analyse des composants de ce SIM pour en identifier les constituants. Ces deux analyses sont étroitement liées aux capacités des capteurs en ce qui concerne l'interprétation des multiples protocoles, parfois propriétaires, présents sur un réseau. Ces analyses peuvent être menées de manière totalement passive (ce qui est généralement le cas pour la cybersurveillance où il n'y a, par conception, aucune interaction entre le capteur et le réseau analysé), ou active, dans le cas par exemple d'un ordinateur, où un agent doit généralement être installé (ou des requêtes à distance réalisées) pour collecter les informations nécessaires.

III.5 Conclusion

Dans ce chapitre, nous avons essentiellement abordé la QR1 et le sujet de l'appréciation de la situation, ainsi que la difficulté de mettre en œuvre une cybersurveillance efficace sans moyens adaptés au contexte particulier des SIM. Nous avons détaillé les limitations des outils actuels de cybersécurité. Nous avons ensuite modélisé le concept original de *Maritime Cyber Situational Awareness* et détaillé les attendus en termes fonctionnels de cet état de connaissance. Nous avons adapté les travaux originaux d'Endsley [End95] en les enrichissant des travaux de Barford, Mc Guinness & Foy [McG00] et en prenant en compte les remarques de Franke et Brynielsson [Fra14]. Nous avons proposé l'ajout de deux nouveaux processus

(*resolution anticipation* et *resolution assessment*) qui permettent de faciliter la prise de décision. Nous avons modélisé une cyberattaque visant un SIM à l'aide des *frameworks* proposés par MITRE, en précisant les capteurs à utiliser pour détecter les menaces. Par la suite, nous avons défini des niveaux d'abstraction réalistes et efficaces dans un contexte cyber et maritime en s'appuyant sur la théorie des super-réseaux. Enfin, nous avons détaillé chaque processus de la *situation assessment*, niveau de détail absent dans l'état de l'art de la CSA et avons abordé les QR2 et QR3 au travers des enjeux liés à la visualisation dans un contexte maritime. Ces travaux ont permis de montrer l'attente importante du monde scientifique et maritime sur le sujet, mais aussi de dégager un certain nombre de nouveaux axes de recherche, comme l'automatisation de l'aide à la décision et la mesure des impacts [Jac18, Jac19a, Jac19b].

Chapitre IV

Maritime Cyber Situational Awareness : architecture, expérimentation et résultats

Dans ce chapitre sont traitées les QR1 (architecture de collecte et modélisation), QR2 (analyse et représentation des données) et QR3 (détection d'anomalies dans un contexte maritime), en appliquant sur plate-forme expérimentale prototype la modélisation et les mesures de qualité présentées au chapitre précédent. Après avoir défini, implémenté et évalué l'architecture de cybersurveillance nécessaire pour permettre l'élaboration de la *Maritime Cyber Situational Awareness*, nous détaillons les résultats obtenus en termes de qualité, mais aussi d'analyse et de représentation des données. Enfin, nous contribuons directement à une architecture avancée de détection dans le contexte des SIM, et plus spécifiquement sur le standard NMEA 0183.

IV.1 Réalisation d'un prototype sur plate-forme et expérimentation

Cette section a pour objectif de détailler l'expérimentation sur plate-forme réalisée dans le cadre de nos travaux, tant sur la composante embarquée que sur l'élongation vers la terre. La réalisation de ce prototype permettra de vérifier la faisabilité technique de notre modèle

d'élaboration de la MCSA.

Dans un premier temps, nous détaillons l'architecture fonctionnelle d'un navire moderne, et notamment de la couche permettant la capture d'information à des fins cyber. Dans un second temps, nous précisons la composante terrestre mise en place sur notre prototype.

IV.1.1 Composante embarquée

L'École navale dispose de matériel représentatif de systèmes d'information maritimes, financé dans le cadre du dernier Contrat Plan État-Région (CPER). Par ailleurs, elle a récemment acquis des équipements complémentaires dans le cadre du projet européen H2020 *Foresight*, afin d'étendre ses capacités à la représentation du fonctionnement d'une passerelle de navire. Pour modéliser le prototype de plate-forme afin que l'ensemble s'approche au mieux, en termes de réalisme, d'un navire, nous nous sommes appuyés sur trois articles scientifiques qui abordent le sujet [Kri13, Rø14, TO21], ainsi que sur des articles concernant plus particulièrement les systèmes industriels [Nic19]. Le prototype de ce navire générique, conçu sous forme d'une plate-forme appelée *Naval Cyber Range*, doit nous permettre de valider la faisabilité technique de l'élaboration de la MCSA (figure IV.1).

L'architecture complète de la plate-forme peut être représentée suivant plusieurs approches. D'un point synthétique, cependant, si l'on s'intéresse exclusivement aux systèmes de type OT, le navire simulé peut être considéré comme constitué essentiellement de trois sous-systèmes.

Le sous-système « passerelle », visible en figures IV.2 et IV.3, est représentatif d'une passerelle de navire de taille moyenne, avec essentiellement des capteurs (GNSS, AIS) et les antennes associées, un bus et des connecteurs aux standards NMEA 0183 et 2000, des écrans de visualisation de l'ECS et un simulateur de navigation 3D. Ce sous-système est représenté en bas à gauche de la figure IV.5.

À bord d'un navire, de nombreuses productions industrielles sont réalisées : électricité, motricité, réfrigération, filtration. À ces fins, les chantiers navals et leurs sous-traitants créent des installations industrielles finalement assez proches de ce que l'on peut trouver dans des ports ou dans d'autres installations à terre, sous la forme de systèmes de contrôle industriels (*Industrial Control Systems*, ICS), au sens de la définition proposée par le NIST [1]. Le sous-

1. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

FIGURE IV.1 : Aperçu de trois boucles de la plate-forme d'expérimentation (partie systèmes industriels) (source : archives personnelles).

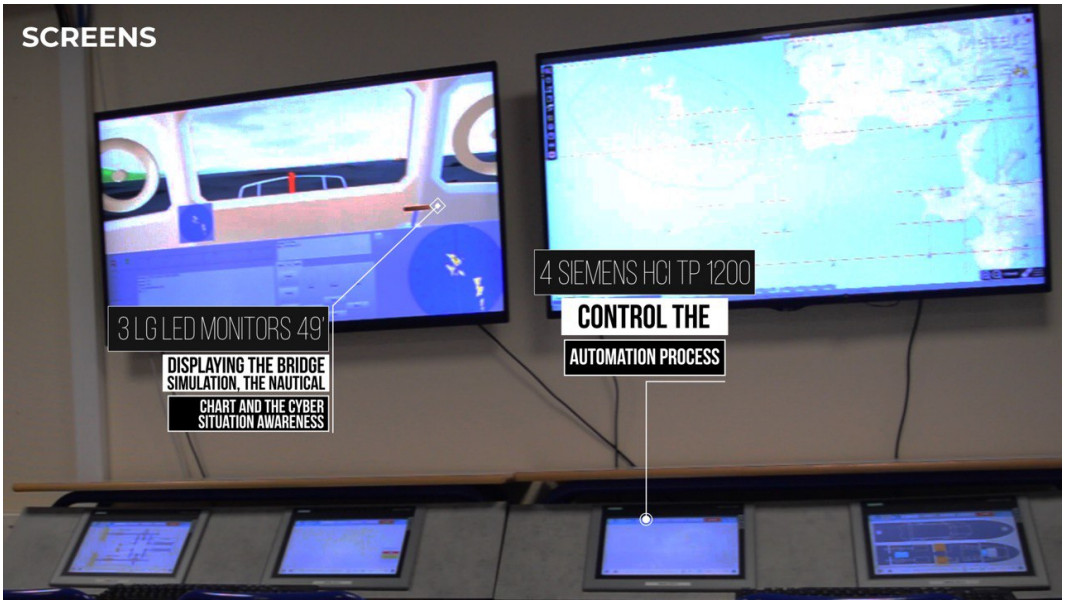

FIGURE IV.2 : Environnement de simulation de la passerelle de navigation (source : Chaire de cyberdéfense des systèmes navals, reproduite avec l'aimable autorisation de l'auteur).

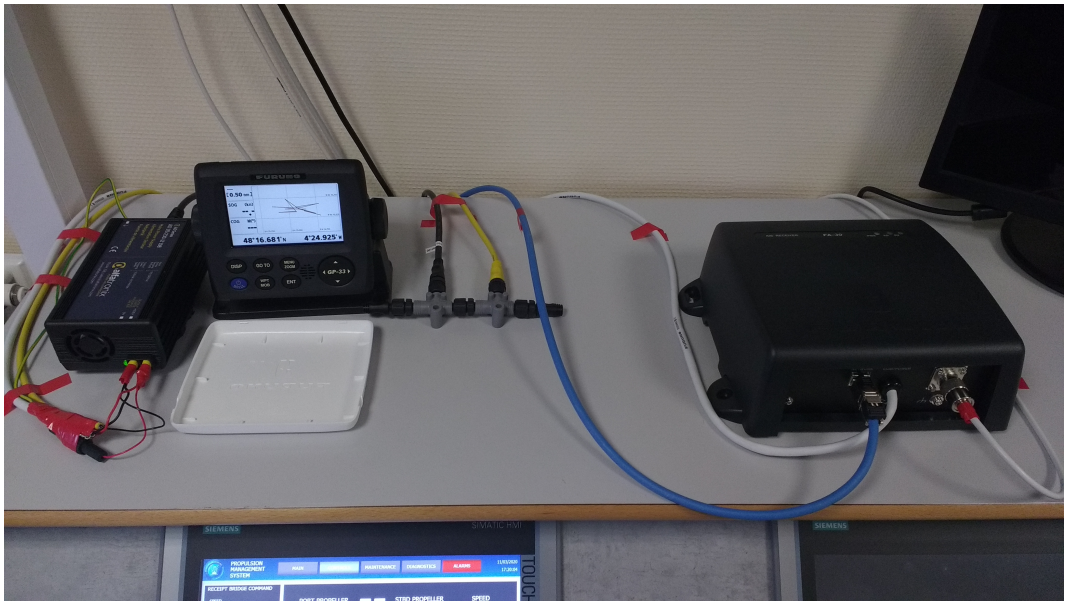

FIGURE IV.3 : Récepteur GPS (à gauche), connecteur NMEA 0183 et bus NMEA 2000 (au centre) et récepteur AIS (à droite) (source : archives personnelles).

système « industriel » comprend quatre sous-réseaux, utilisant des technologies de boucles réseau : la boucle « mobilité », la boucle « sécurité », la boucle « électricité » et la boucle « auxiliaires ». La boucle « mobilité » (figure IV.4) gère la propulsion principale et auxiliaire, ainsi que les apparaux à gouverner : stabilisation, gouvernail, propulseur azimutal et ligne d'arbre. La boucle « sécurité » gère la détection et la lutte contre les sinistres (voie d'eau, incendie), l'ouverture et la fermeture des vannes, portes et panneaux, la ventilation et la production d'eau froide. La boucle « électricité » pilote la production d'énergie haute tension à bord du navire, en fonction des besoins en tension et en intensité. À partir de sources telles que les turbines, les groupes électrogènes ou encore les batteries, l'électricité est ensuite convertie puis distribuée à bord. Enfin, la boucle « auxiliaires » commande les servitudes, la gestion de l'alimentation en combustible, en air, en huile, la production d'eau douce, le traitement des eaux grises et noires et la réfrigération des vivres. Au sein de chaque boucle, ces fonctions sont assurées par un ou plusieurs Automates Programmables Industriels (API), auxquels sont raccordés des capteurs et des actionneurs qui peuvent être réels ou simulés. Ce sous-système est représenté en bas à droite de la figure IV.5.

Le sous-système « communication » représente d'une communication par satellite entre le navire et la terre, avec ses contraintes (bande passante, délai, perte temporaire de lien). Ce sous-système est schématisé en haut à gauche de la figure IV.5.

La plate-forme expérimentale prototype présentée en figure IV.5 s'avère assez proche

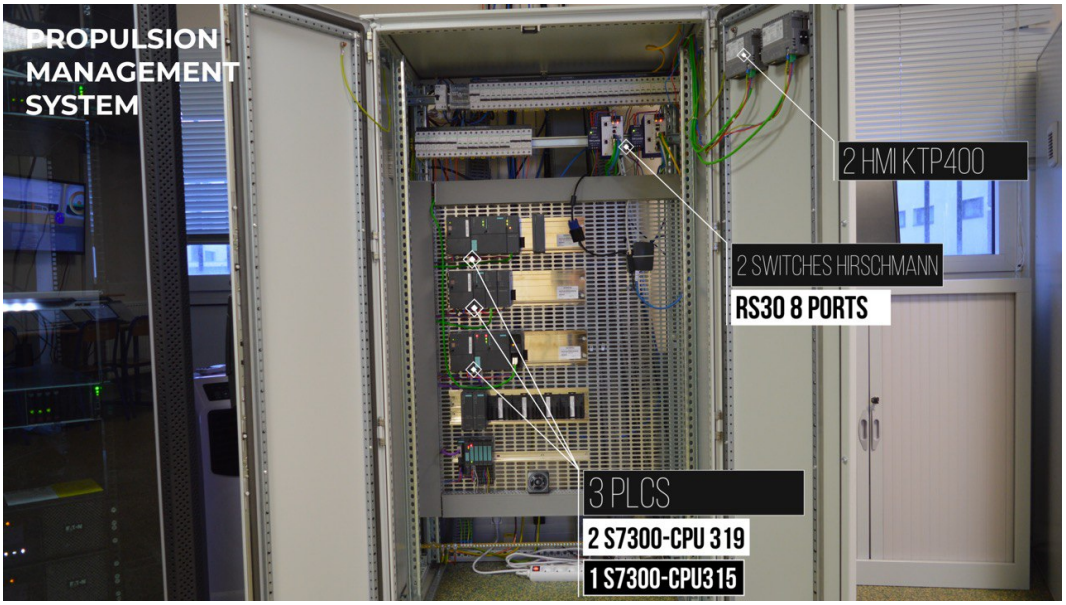

FIGURE IV.4 : Aperçu de la boucle mobilité (le capteur NIDS se situe en haut à droite de la baie) (source : Chaire de cyberdéfense des systèmes navals, reproduite avec l'aimable autorisation de l'auteur).

d'autres modélisations, comme celle de Purdue pour les systèmes industriels et *cyber test beds* [TXLJ19]. Elle se veut la plus générique possible, car chaque type de navire dispose de particularités dans ses capteurs, actionneurs, systèmes, qui peuvent donc être ajoutés dans les couches processus et instrumentation. Par ailleurs, l'architecture réseau peut également s'avérer plus complexe, en matière de redondance ou de séparation physique ou logique.

Afin de réaliser l'expérimentation et la validation de nos modèles et concepts de recherche, nous créons et intégrons à ce prototype de navire générique un sous-système « cyber » (figure IV.6). Ce sous-système comprend les différents éléments nécessaires au processus de *situation assessment* et à l'élaboration de la MCSA, par l'ajout de capteurs NIDS et HIDS, mais aussi par la récupération des journaux émanant des producteurs éventuels et l'ajout d'une couche de cybersurveillance séparée. Ces travaux s'appuient notamment sur les articles scientifiques publiés par l'ANSSI ([Chi14] et [Dia14]), ainsi que d'autres architectures d'analyse de données dans un contexte de détection d'anomalies cyber [Pan18]. L'architecture technique a notamment été détaillée dans [Jac18].

Pour chaque sous-réseau, un premier bloc constitué par un dispositif de prélèvement de type *Test Access Port (TAP)* ou *port mirroring* est mis en place. Il est appelé *Network Connexion Safety (NCS)* dans l'article [Jac18]. Ce dispositif permet d'éviter toute interaction en « écriture » avec le réseau surveillé.

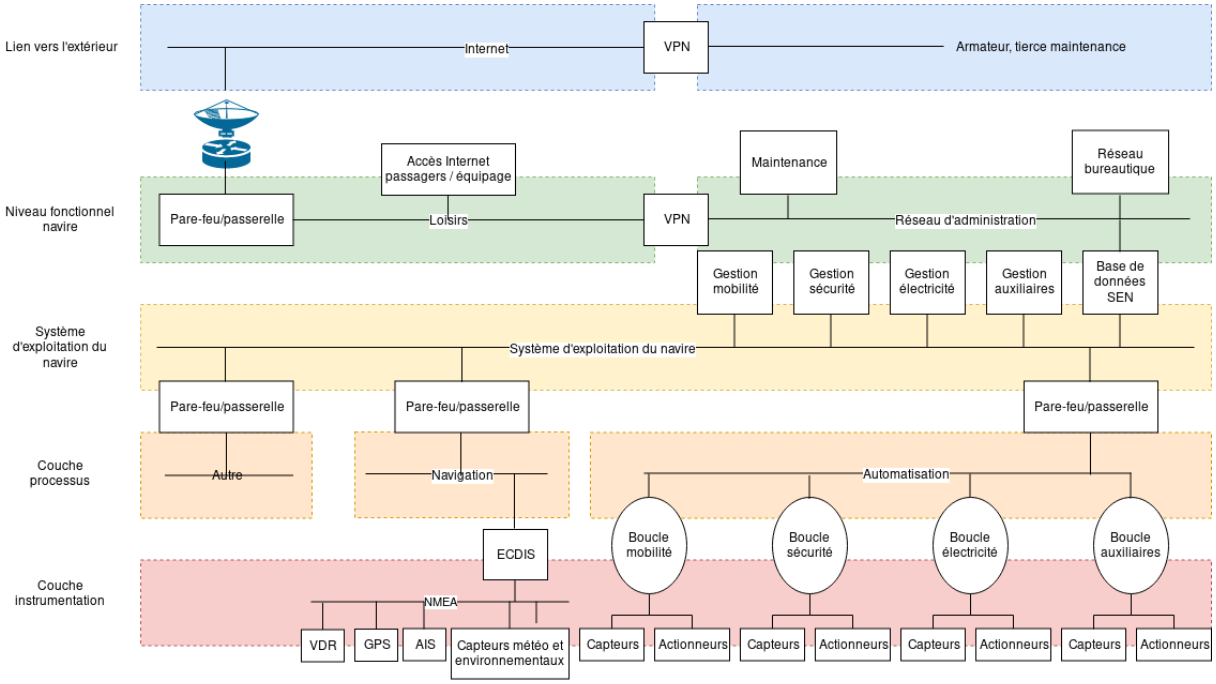

FIGURE IV.5 : Modélisation technique du prototype avec les sous-systèmes « passerelle », « communication » et « industriel » (source : archives personnelles).

Un deuxième dispositif, appelé *Network Probe Isolation (NPI)*, permet d'héberger plusieurs NIDS sur un seul serveur physique en s'appuyant sur l'architecture et les technologies proposées dans [Chi14]. Chaque capteur est isolé des autres par l'emploi de conteneurs sécurisés, ce qui permet d'y faire fonctionner de manière séparée des capteurs utilisant des moteurs de détection, des pré-processeurs et des règles distinctes. Cela offre également la possibilité de configurer le capteur pour récupérer des métadonnées et des métriques spécifiques au système surveillé. Au sein de ce dispositif peut être mis en place un outil de *Full Packet Capture (FPC)* permettant une analyse très fine directement au niveau des paquets, ce qui peut s'avérer utile en cas d'investigation poussée sur des protocoles particuliers, le trafic étant stocké et indexé dans l'outil de *big data* constitué par le *Local Engine (LE)*.
Le troisième bloc, *Local Preprocessor (LP)*, assure la normalisation des entrées, le filtrage et la suppression de données inutiles, ainsi que la transformation des données si nécessaire (par exemple, sous forme d'enrichissement des données avec la résolution de l'adresse IP). Il permet aussi une corrélation des évènements et des alarmes afin de limiter l'impact sur le lien satellite.
Le quatrième bloc, LE, permet un stockage court et long terme des informations à bord du navire, offrant ainsi une capacité d'indexation et de recherche en temps immédiat d'une part, et une rétention longue pour des raisons légales d'autre part. Le stockage de ces données et

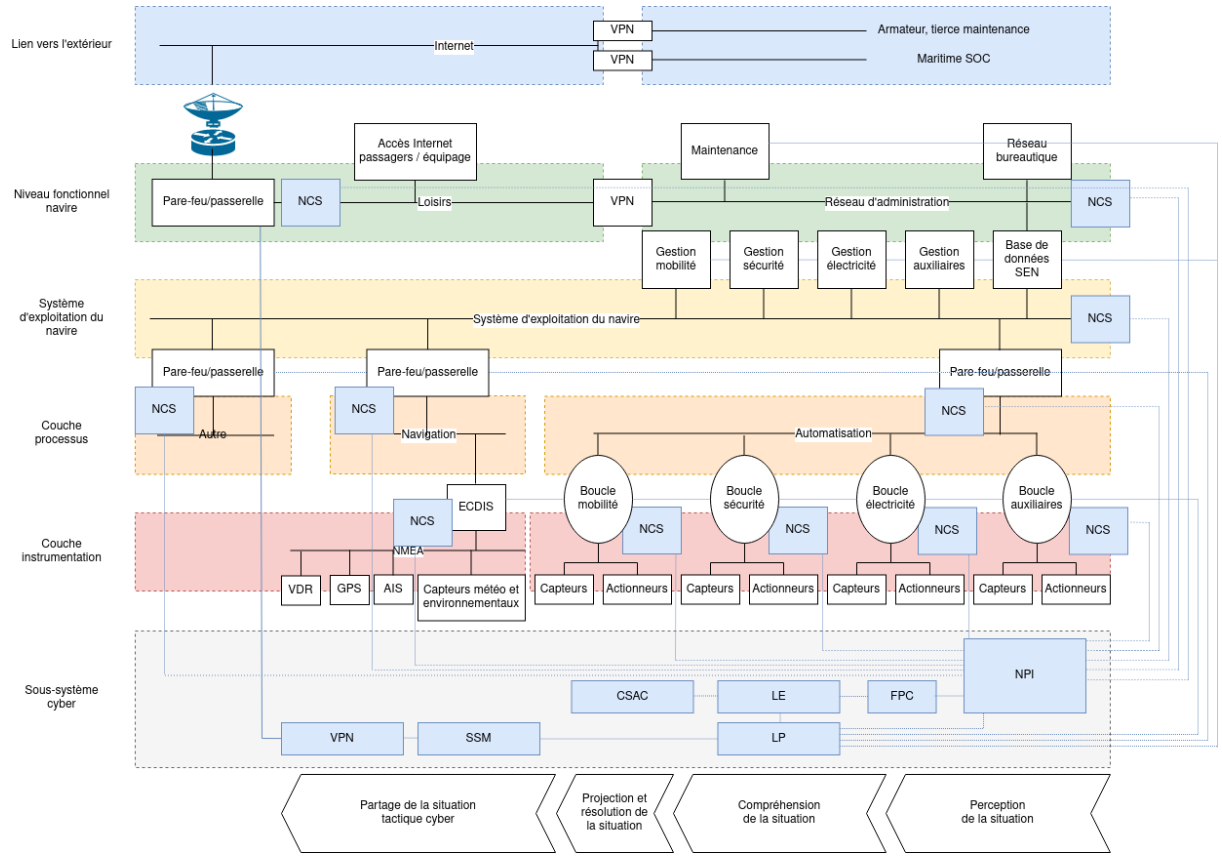

FIGURE IV.6 : Modélisation technique simplifiée des interconnexions de la plate-forme d'expérimentation avec le prototype de sous-système cyber (source : archives personnelles).

leur indexation permettent également d'y réaliser des opérations d'apprentissage automatique.

Le cinquième bloc est constitué par le *Ship Shore Manager (SSM)* : cet outil fonctionne comme un cache pour garantir que les données sont correctement envoyées vers la terre même en cas de coupure satellite ou de débit insuffisant. Il limite la bande passante attribuée au sous-système cyber pour éviter qu'il n'occupe un pourcentage trop important de la bande passante totale. Il permet également de prioriser les données émises en fonction d'un marquage donné (émission prioritaire des alertes par rapport aux métadonnées, par exemple). En cas de coupure du lien satellite, les données sont stockées en cache, en mémoire ou sur un support magnétique ou *flash*, puis retransmises vers la terre dans le bon ordre lors du rétablissement du lien.

Le sixième bloc est constitué de la *Cyber Situational Awareness Console (CSAC)*. En utilisant cette console, l'équipage du navire dispose d'une vue simplifiée, mais complète, de la situation cyber à bord qui est partagée avec le SOC à terre. Même en cas d'interruption

du lien satellite, il dispose de remontées permettant de réaliser les premiers diagnostics si nécessaires. Enfin, le lien entre le navire et le SOC doit être sécurisé, car il transmet des informations critiques et ne doit être ni corrompu, ni capturé. C'est la raison pour laquelle un VPN dédié permet de transmettre l'information vers la terre et isole le flux de surveillance cyber des autres flux de données.

IV.1.2 Composante « terre »

Comme le présente la figure IV.7, côté « terre », le SOC maritime s'organise autour de quatre blocs. Le premier bloc, en charge de la gestion du lien avec le navire et de l'ingestion des données, réalise la terminaison de la liaison mer/terre avec le SSM « terre ». Il garantit que les données collectées à bord sont reçues à terre, de manière ordonnée, dans le respect des contraintes de bande passante fixées, et ce, même en cas de coupure du lien satellite au travers du *Bandwidth Manager (BM)* et d'une partie du *Central Processor (CP)*.
Le second bloc est constitué du traitement des données. Il comprend le *CP*, qui centralise l'ensemble des données sous forme de flux qui peuvent être triés, filtrés, transformés, enrichis ou normalisés afin de traiter le cas de données issues de capteurs hétérogènes, et le *Central Engine (CE)*, qui stocke et indexe les données en vue de leur analyse. Le traitement des données issues du RIC appartient également à ce bloc (sources d'IoC), ainsi que les sources d'enrichissement (cartographie : adresses IP, enregistrements *Domain Name Service (DNS)*, etc. . .).
Le troisième bloc concerne à la rétention long terme et à la visualisation, avec des outils permettant la génération de tableaux de bord dynamiques et l'analyse fine des données.
Enfin, le quatrième et dernier bloc couvre les fonctions cyber à proprement parler, par l'emploi des outils de réponse à incident, d'analyse cyber (*Digital Forensics and Incident Response (DFIR)*, SIRP) et de partage d'information.

Cette architecture applicative nécessite la mise en place de flux de données et de matériels et logiciels de capture, d'analyse et de présentation, détaillés dans la section suivante.

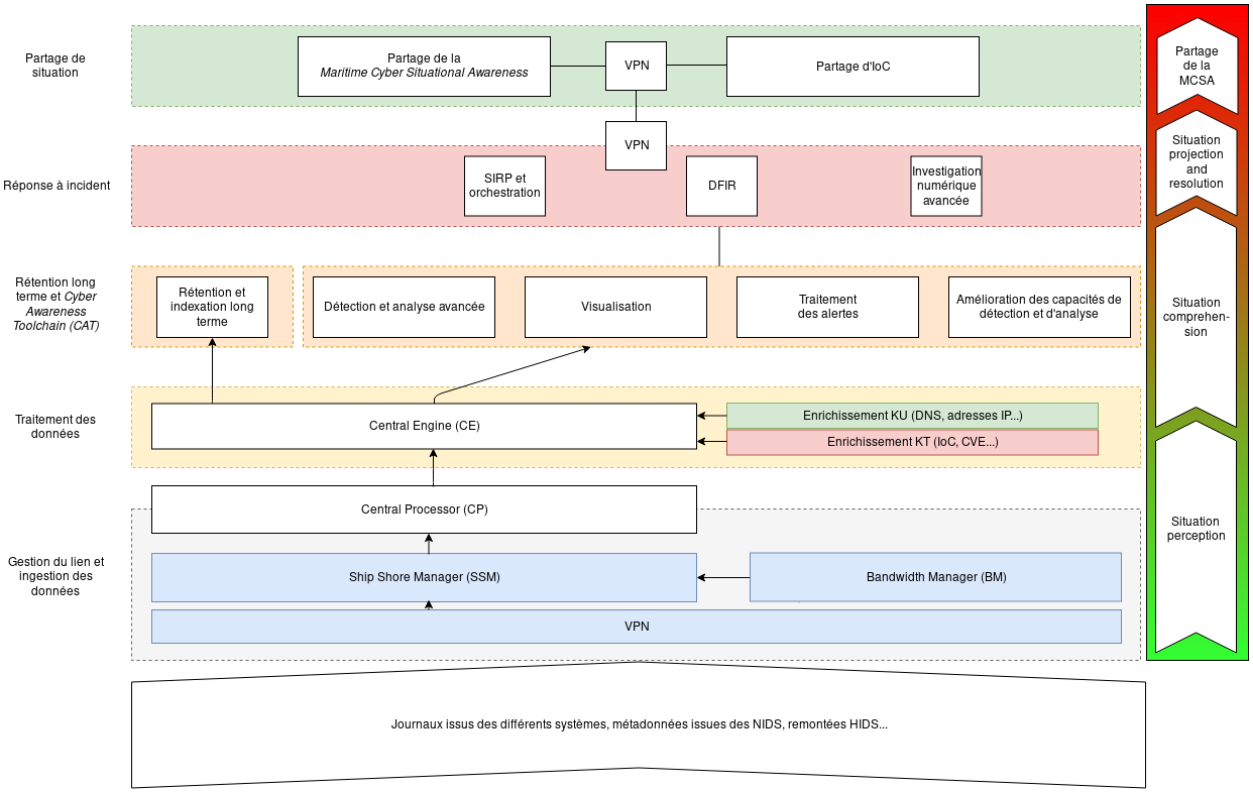

FIGURE IV.7 : Architecture applicative de la composante « terre » de cybersurveillance maritime (source : archives personnelles).

IV.1.3 *Architecture applicative* pour l'établissement de la MCSA sur le *Naval Cyber Range*

Cette sous-section détaille l'architecture applicative mise en place pour la récupération des données « réseau » et « système » des SIM, leur centralisation et leur analyse en vue de l'élaboration de la MCSA.

IV.1.3.1 Architecture applicative pour les données « réseau »

La figure IV.8 modélise le bout en bout de l'analyse d'un flux réseau, comprenant la partie extraction des métadonnées et des alertes, la mise à jour et l'amélioration des signatures et une boucle de rétro-information vers la CSAC et le SIM.

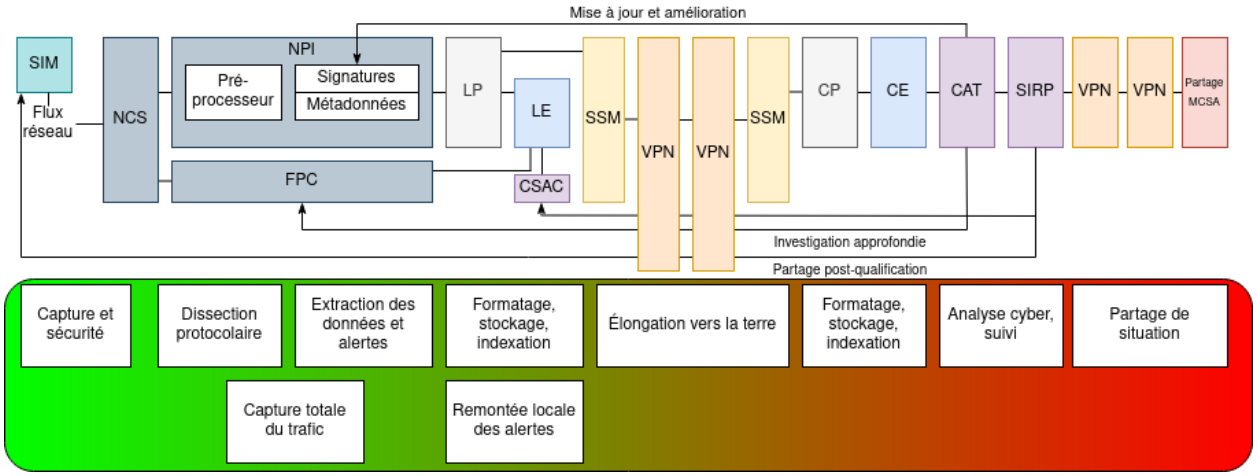

FIGURE IV.8 : Bout en bout de l'analyse d'un flux réseau (source : archives personnelles).

IV.1.3.2 Architecture applicative pour les données « système » (journaux)

La figure IV.9 modélise l'ensemble de l'analyse d'un flux issu de journaux (HIDS ou autre producteur), comprenant la partie extraction des métadonnées et des alertes, la mise à jour et l'amélioration des signatures et une boucle de rétro-information vers la CSAC et le SIM.

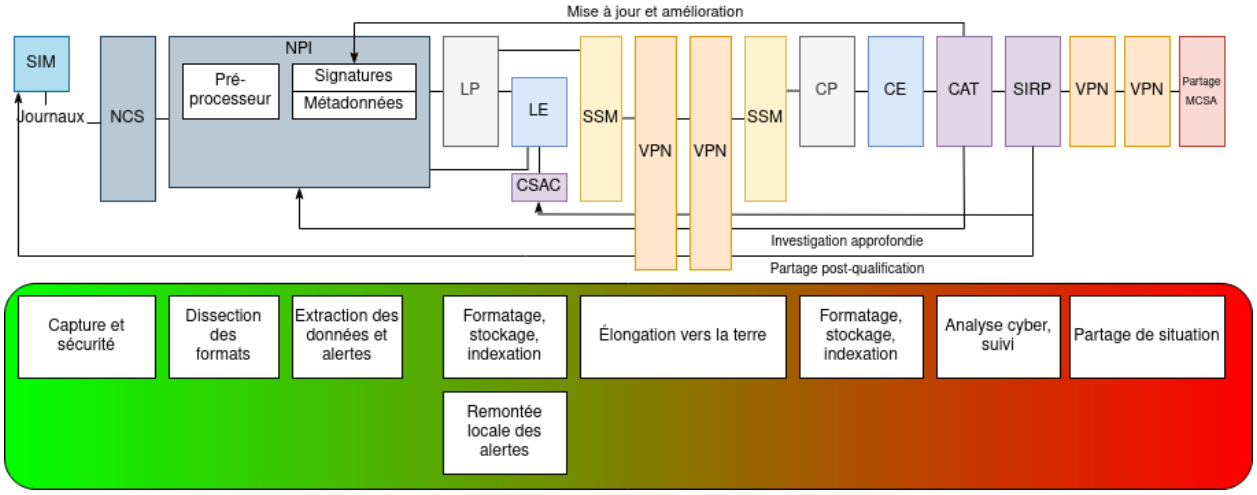

FIGURE IV.9 : Bout en bout de l'analyse du flux des journaux (source : archives personnelles).

Les deux flux sont réalisés en temps réel et peuvent se compléter et se corréler dans le cadre de l'analyse globale d'une cyberattaque telle que modélisée en Annexes C.1 et C.2.

IV.2 Analyse de la qualité - résultats

La qualité est l'un des processus de la *situation assessment* (*Quality Assessment*) devant être évalué dans le cadre de l'élaboration de la SA (voir paragraphe III.3.4.6). En effet, les données analysées par les systèmes afin de leur donner du sens et une connaissance à une fin de prise de décision (intelligence) (figure IV.10), peuvent présenter des défauts de qualité (données erronées, incomplètes, imprécises et incertaines). Ces défauts, d'origine contextuelle, intrinsèque ou extrinsèque [ML17], involontaires ou faisant suite à une manœuvre tactique de l'adversaire (*adversarial*), peuvent déformer la connaissance obtenue de la situation et donc impacter la prise de décision. La mesure de la qualité de la donnée s'avère ainsi indispensable à la prise de décision. Afin de vérifier le niveau de qualité atteint sur la plate-forme prototype, des critères et mesures de qualité ont été définis puis évalués.

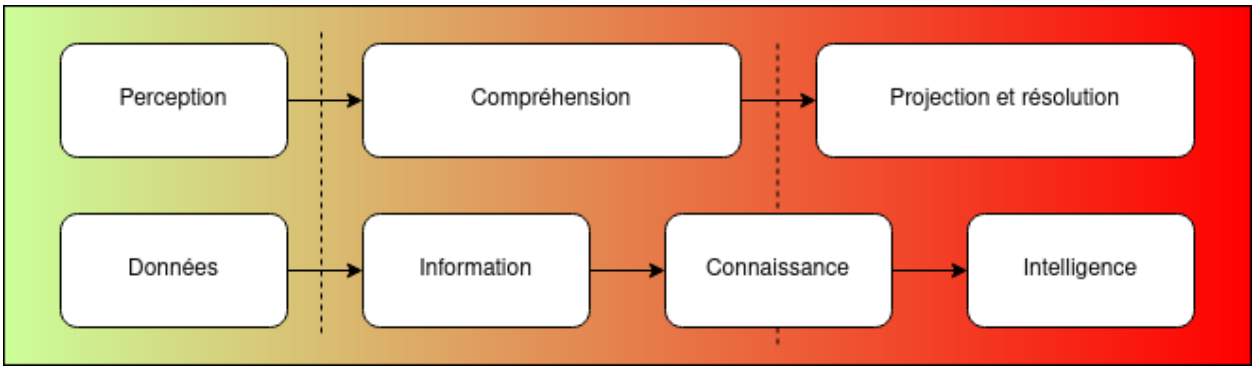

FIGURE IV.10 : Parallèle envisageable entre données, information, connaissance, intelligence et *situational awareness* (source : archives personnelles).

Comme synthétisé dans la figure IV.11, dans notre contexte multi-capteurs dans un système de systèmes, l'objectif de l'analyse de la qualité est donc d'identifier des critères (*trustworthiness*, *truthfulness*, *completeness*, *freshness*, *timeliness*), qui permettent de garantir que la prise de décision se basera sur des données et des informations sûres et de qualité.

Cette section détaille les modalités, mesures et résultats de qualité obtenus sur cette plate-forme expérimentale développée dans un contexte le plus proche possible de la réalité du navire (le lien satellite est simulé de manière réaliste : latence, coupures). L'ensemble des critères de qualité remonte, en temps réel, comme les métadonnées cyber, vers les serveurs CP, CE et CSAC pour information et accompagnent donc la donnée tout au long de l'établissement de la SA. Concernant les mesures de qualité, l'analyse détaillée concerne les capteurs de type réseau. Cependant, il demeure possible d'identifier des généralités dans

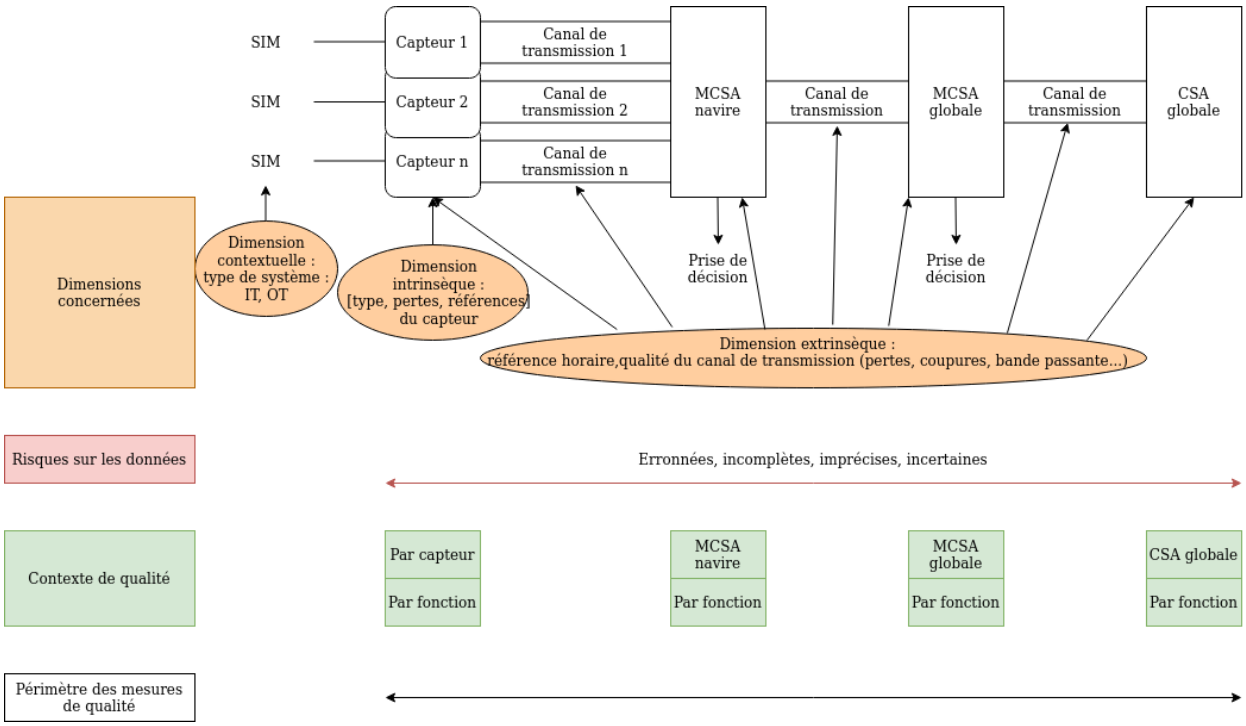

FIGURE IV.11 : Mesure de la qualité : vue d'ensemble des dimensions de la qualité, liens avec données et risques (source : archives personnelles).

leurs critères, les rendant applicables à d'autres types de capteurs cyber.

IV.2.1 Critère de qualité Q1 - *Trustworthiness*

La mesure de qualité liée au critère de *trustworthiness* vient mesurer la confiance que l'on peut avoir dans l'intégrité du capteur et dans son aptitude à transmettre ses données dans le flux d'analyse. Cette confiance se mesure au travers de quatre sous-critères, mesurant la disponibilité effective du capteur (Q1.1), son intégrité (Q1.2), l'actualité de ses signatures de détection (Q1.3), et le bon fonctionnement de l'élongation vers la terre (Q1.4).

IV.2.1.1 Premier sous-critère de *Trustworthiness* Q1.1 : disponibilité

Tout d'abord, les processus liés aux capteurs NIDS doivent être fonctionnels : cette capacité se mesure par le taux de disponibilité du service NIDS. Ce critère est appelé Q1.1. Avec n le nombre de NIDS et $dispo(x) \rightarrow \{0; 1\}$ la disponibilité, Q1.1 peut être exprimé en pourcentage sous la forme :

$$Q1.1 = \frac{\sum_0^n dispo(i)}{n} * 100$$

Il est à noter que cette disponibilité peut être calculée pour chaque niveau d'abstraction précisé au §III.3.3.
Sur notre plate-forme expérimentale, nous avons développé un *script* en *bash* sur le NIDS permettant d'informer le SIEM du bon fonctionnement du capteur (avec, par exemple, une ligne comme *Feb 25 09 :57 :02 root : NIDS en fonction*).

IV.2.1.2 Deuxième sous-critère de *Trustworthiness* Q1.2 : intégrité

Ensuite, les capteurs ne doivent pas avoir été altérés. Ce critère est appelé Q1.2. Avec n le nombre de NIDS et $integ(x) \rightarrow \{0; 1\}$ l'intégrité, Q1.2 peut être exprimé en pourcentage sous la forme :

$$Q1.2 = \frac{\sum_0^n integ(i)}{n} * 100$$

Sur notre plate-forme expérimentale, nous évaluons Q1.2 en vérifiant, par le biais du HIDS ou via un *script* en *bash*, l'intégrité des répertoires de configuration et de données. Ainsi, l'intégrité des signatures est assurée par la réalisation régulière d'un condensat cryptographique, qui remonte jusqu'au SIEM, pour vérification. La ligne *Sep 15 16 :01 :51 nids-mob pi : SHA256 bd819ce1cb2ddfa3ddad588971da099c2e873b4a143a3cadd61c3b685e0985c2 /etc/suricata/rules/smtp-events.rules* retourne ainsi le condensat cryptographique des signatures relatives aux évènements *Simple Mail Transfer Protocol (SMTP)* du capteur NIDS, garantissant ainsi son intégrité par comparaison avec une liste de référence des condensats cryptographiques des signatures.

IV.2.1.3 Troisième sous-critère de *Trustworthiness* Q1.3 : actualité des signatures

Ensuite, les signatures doivent être à jour. Ce critère s'appelle Q1.3. Avec n le nombre de NIDS et $actu(x) \rightarrow \{0; 1\}$ l'actualité des signatures, Q1.3 peut être exprimée en pourcentage sous la forme :

$$Q1.3 = \frac{\sum_0^n actu(i)}{n} * 100$$

Sur notre plate-forme expérimentale, Q1.3 est mesuré par deux paramètres obtenus et transmis de manière régulière : le premier est constitué de la date des fichiers de signatures (par exemple : *Feb 24 16 :01 :51 nids-mob pi : Date /etc/suricata/rules/smtp-events.rules : vendredi 21 décembre 2018, 15 :43 :33 (UTC+0100)* indique que la date de création du fichier */etc/suricata/rules/smtp-events.rules* est le 21 décembre 2018 à 15 :43 :33) et le second concerne la vérification de certains paramètres du NIDS : *stats.detect.engines.last_ reload*, qui retourne la dernière date de rechargement des règles, *stats.detect.engines.rules_ loaded*, qui précise le nombre de règles chargées, et *stats.detect.engines.rules_ failed*, qui donne le nombre de règles en erreur. Ainsi, une date de rechargement des règles antérieure à la date des fichiers de signatures informera que la dernière version n'a pas été chargée, par exemple par le biais d'une alerte.

IV.2.1.4 Quatrième sous-critère de *Trustworthiness* Q1.4 : disponibilité de l'élongation

La disponibilité de l'élongation est essentielle pour garantir que lien avec le SIEM est bien assuré. Ce critère est appelé Q1.4. De manière formelle, avec *MTBF* le *Mean Time Between Failure* et *MTTF* le *Mean Time To Failure*, la disponibilité D d'un système est généralement écrite sous la forme :

$$D = \frac{MTTF}{MTBF}$$

La mesure de disponibilité peut être obtenue en simulant une connexion complète avec le SIEM (test du service), ou par le biais d'une requête utilisant le protocole *Internet Control Message Protocol (ICMP)* (test du réseau). Le besoin émanant essentiellement de la détection d'une coupure satellite, nous avons retenu la seconde possibilité. En créant un *script* en *bash*, nous obtenons dans les journaux une nouvelle entrée *syslog* récurrente, initiée par exemple chaque minute : « *Feb 24 14 :29 :01 nids-elec root : Serveur MCSA accessible* ». En complément des autres indicateurs, cette mesure nous permet d'identifier les éventuelles coupures du lien.

IV.2.2 Critère de qualité Q2 - *Truthfulness*

Le second critère de qualité, Q2, a pour objectif de vérifier la véracité et la solidité des éléments d'entrée (véracité *truthfulness* ou solidité *soundness*). Dans certains cas, notamment dans le cas de la détection, les mécanismes utilisés reposent généralement sur des signatures. Ces signatures, si elles s'avèrent incomplètes, peuvent entraîner des faux positifs et, si elles sont incomplètes, des faux négatifs (*cf* §III.3.4.1). Le cas des faux positifs est symptomatique des difficultés quotidiennes des SOC [KSB+19]. Ces faux positifs, qui peuvent être dus à des signatures de piètre qualité, peuvent aussi être générées à dessein par un attaquant à des fins de leurrage (*deception*). En effet, face à une tempête de faux positifs destinée à détourner l'attention du défenseur de la cible réelle, la détection et la priorisation d'une vraie cyberattaque s'avèrent complexes.

La qualité de ce critère repose sur plusieurs bases. Tout d'abord, le capteur NIDS doit être à même d'analyser le protocole utilisé pour mener la cyberattaque. Ensuite, les signatures utilisées par le capteur (génériques, type *Emerging Threats*, spécifiques, par exemple par la réception d'IoC émis par un CSIRT, ou descriptives, décrivant le trafic réseau nominal présent sur le réseau), aussi précises soient-elles, ne permettent pas nécessairement la détection de l'exploitation de faille de type *zero day*. Enfin, les jeux de données réseau de cyberattaques sont encore assez peu nombreux, parfois incomplets ou obsolètes, et souvent peu adaptés à notre contexte maritime et industriel [HBB+20]. Il n'apparaît donc pas pertinent de générer un indicateur chiffré pour ce critère Q2 : les signatures mises à la disposition des capteurs doivent être considérées comme « à l'état de l'art » dans un contexte de détection par signature, et cette vérification est déjà réalisée pour le critère Q1.3.

IV.2.3 Critère de qualité Q3 - *Completeness*

Le troisième critère de qualité, Q3, doit vérifier l'exhaustivité des éléments d'entrée (complétude, *completeness*). En effet, les capteurs, notamment réseau, peuvent ignorer ou ne pas être en mesure de reconstituer certains paquets en entrée ce qui peut, par exemple, obérer leur capacité à reconstruire par la suite des fichiers complets. Le lien d'élongation et les contraintes de bande passante satellite peuvent également être des facteurs de perte de données. L'objectif est donc de mesurer Q3.1, correspondant au taux de perte des capteurs NIDS, Q3.2, le taux de perte dû au lien satellite et Q3.3, indicateur qui vérifie le bon fonctionnement de la capture.

IV.2.3.1 Premier sous-critère de *Completeness* Q3.1

Il existe plusieurs raisons pour lesquelles un NIDS pourrait ne pas réussir à analyser la totalité des paquets qui transitent sur le réseau qu'il écoute. Elles peuvent être dues au très haut débit du réseau local, engendrant des limitations en termes de mémoire ou des saturations des ressources du processeur, à des erreurs de somme de contrôle de redondance cyclique, etc. Avec nb_{pr} le nombre de paquets reçus par le NIDS et nb_{pi} le nombre de paquets invalides, nous pouvons formaliser Q3.1 en utilisant la précision sous la forme :

$$Q3.1 = \frac{nb_{pr} - nb_{pi}}{nb_{pr}} * 100$$

La perte de paquet peut se mesurer au niveau de la carte réseau elle-même, par exemple avec l'utilisation de la commande *ethtool* sur un système *GNU/Linux*. Nous partons du principe que cette mesure a été réalisée à la mise en place des capteurs pour détecter toute anomalie matérielle. Pour analyser la perte éventuelle de paquets au niveau du NIDS lui-même, nous réalisons le suivi de la valeur du paramètre *suricata.eve.stats.capture.kernel_drops* sur une durée d'une semaine, afin d'en déduire un pourcentage de perte par rapport au nombre de paquets capturés (*stats.capture.kernel_packets*). Sur la semaine de suivi de la valeur de ce paramètre sur l'ensemble des capteurs de notre plate-forme d'expérimentation, nous n'avons pas constaté d'évolution de ce chiffre durant nos mesures : il est ainsi constamment resté à 0, l'indicateur de *completeness* Q3.1 étant ainsi toujours égal à 100%. Il apparaît cependant pertinent de continuer à mesurer ce paramètre dans la durée, afin d'en détecter toute évolution défavorable.

IV.2.3.2 Deuxième sous-critère de *Completeness* Q3.2

Les débits des liens satellite peuvent varier de manière conséquente entre les navires, en fonction de leur type, de leurs besoins, de leur positionnement géographique. Dans leur grande majorité, ils sont asynchrones, les besoins en réception à bord du navire étant généralement supérieurs aux besoins en émission. Le débit maximal disponible à un temps t est essentiellement lié à des questions de coût d'abonnement, de technologie, de diamètre de l'antenne embarquée sur le navire, du nombre d'antennes et de facteurs environnementaux. La technologie ayant réalisé des progrès importants ces dernières années, les débits descendants vont de 8 Mbits/s pour un navire de croisière à 6 Mbits/s pour un ferry, 2 à 4 Mbits/s pour un navire de commerce, et 2 Mbits/s pour un navire de pêche moderne, parfois moins.

Des essais récents permettent d'espérer une augmentation forte des débits sur les prochaines années [2]. Les débits montants sont généralement liés par un facteur de 10 au débit descendant (par exemple : 256 kbits/s montants pour un débit descendant de 2 Mbits/s [3]). Quant à eux, les besoins en débit pour l'élaboration de la MCSA sont essentiellement montants, afin d'assurer la remontée des métadonnées, alors que les débits descendants sont inférieurs et essentiellement liés au téléchargement de nouvelles signatures ou au partage d'information.

Les liens satellites sont contraints, que ce soit par la bande passante, les délais d'émission et de réception, les erreurs qui sont généralement la conséquence de conditions environnementales difficiles (pluie, par exemple) ou de la congestion du lien. Sur plate-forme expérimentale, la connexion satellite simulée a, par défaut, les caractéristiques d'un lien fixe. La figure IV.12 montre un délai moyen inférieur à 1 ms qui n'est pas réaliste.

```
ping 11.0.0.2
Envoi d'une requête 'Ping' 11.0.0.2 avec 32 octets de données :
Réponse de 11.0.0.2 : octets=32 temps<1ms TTL=63
Réponse de 11.0.0.2 : octets=32 temps<1ms TTL=63
Réponse de 11.0.0.2 : octets=32 temps<1ms TTL=63
Réponse de 11.0.0.2 : octets=32 temps<1ms TTL=63

Statistiques Ping pour 11.0.0.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

FIGURE IV.12 : Délai nominal d'un *ping* ICMP sur le lien WAN de la plate-forme du *Naval Cyber Range* (source : archives personnelles).

Le *Round Trip Time (RTT)* moyen théorique d'une liaison de bout en bout pour un satellite en orbite géostationnaire (ce qui est le cas des satellites utilisés dans le monde maritime, comme les constellations de satellites *Very Small Aperture Terminal (VSAT)*) est de l'ordre de 500 ms. En effet, la distance à parcourir par les ondes radio entre la terre et un satellite géostationnaire est d'environ 36 000 km. À une vitesse de la lumière de 299 792 km/s, le temps entre l'émission à terre et la réception au niveau du satellite est donc de 0,12 s. Pour un aller terre/satellite/terre, le temps est donc de 250 ms environ et de 500 ms pour le RTT complet entre l'émetteur et le récepteur. Si l'on ajoute à cette valeur le temps nécessaire pour joindre le routeur du téléport et la distribution à bord du navire (figure

2. https://www.satellitetoday.com/mobility/2018/02/26/watch-ses-ceo-setting-new-bandwidth-capacity-record/
3. https://www.nsslglobal.com/index.php?idPage=4&p=101433

IV.13), le RTT est donc supérieur à cette valeur optimale et, d'après les mesures que nous avons pu faire, généralement plus proche des 650 ms à 800 ms dans des conditions normales.

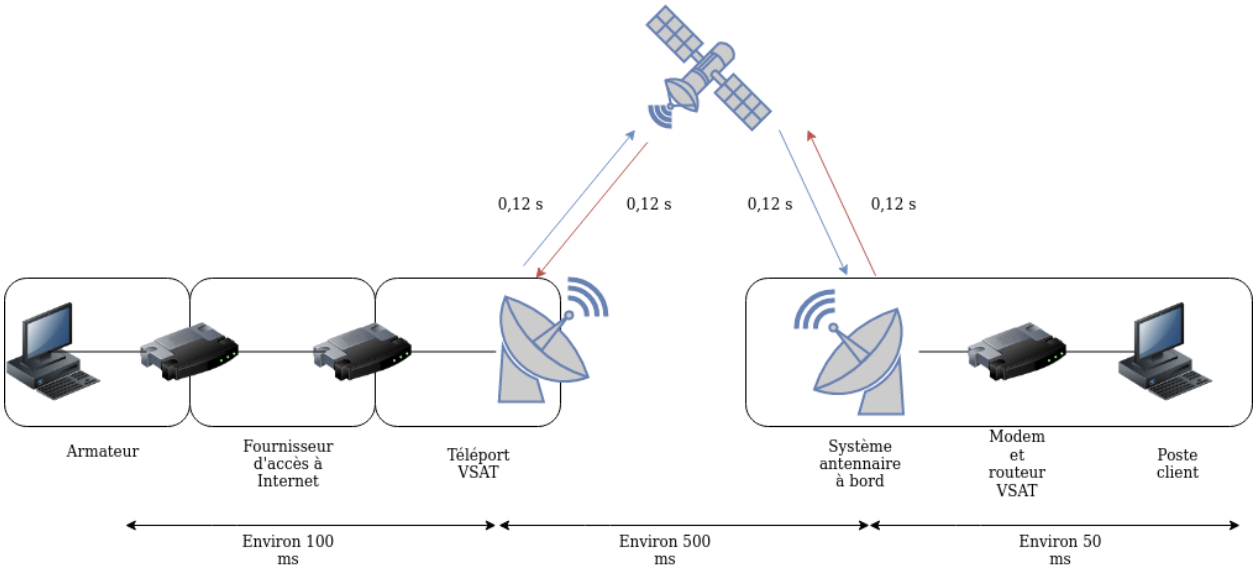

FIGURE IV.13 : Schématisation du *Round Trip Time* d'une liaison satellite vers un navire en mer (source : archives personnelles).

Nous y ajoutons donc un délai de 650 ms et une distribution normale de +/- 20 ms de ce délai. Le lien satellite n'étant pas exempt de pertes de paquets, nous injectons une condition défavorable qui correspond à une perte de 10 %. Afin de simuler ces caractéristiques sur notre plate-forme, nous utilisons le système GNU/Linux et la commande *tc*. *tc*, pour *traffic control*, est un utilitaire qui permet de paramétrer l'ordonnanceur de paquets de GNU/Linux et, dans notre cas, d'en dégrader certaines caractéristiques pour simuler un lien satellite. Ainsi, la commande *tc qdisc add dev ens19 root netem delay 650ms 20ms distribution normal loss 10% corrupt 5% duplicate 1%* nous permet de simuler des conditions défavorables sur un lien satellite simulé, comme le confirment les résultats de la figure IV.14.

La commande *tc* permet également de contraindre la bande passante en émission et en réception, ainsi que le *Maximum Transmission Unit (MTU)*, par l'emploi du paramètre *rate*[4]. Sur notre prototype, nous contraignons donc la bande passante descendante à 2 Mbits/s, la bande passante montante à 256 kbits/s. Nous ajustons également le MTU et les paramètres de dégradation du lien afin d'approcher aux mieux les caractéristiques d'une liaison satellite d'un navire de taille moyenne.

4. Par exemple, par la commande *tc qdisc add dev ens19 parent1 : handle 2 : tbdrate 256 kbit burst 256kit latency 50ms mtu 1460* pour le lien montant et *tc filter add dev ens19 protocol ip parent ffff : prio 1 u32 match ip src 0.0.0.0/0 policy rate 2Mbit burst 2Mbit drop flowid :1* pour le lien descendant.

```
Réponse de 11.0.0.2 : octets=32 temps=636ms TTL=63
Réponse de 11.0.0.2 : octets=32 temps=652ms TTL=63
Réponse de 11.0.0.2 : octets=32 temps=629ms TTL=63
Réponse de 11.0.0.2 : octets=32 temps=650ms TTL=63
Délai d'attente de la demande dépassé
Réponse de 11.0.0.2 : octets=32 temps=626ms TTL=63
Réponse de 11.0.0.2 : octets=32 temps=670ms TTL=63
Réponse de 11.0.0.2 : octets=32 temps=641ms TTL=63
Délai d'attente de la demande dépassé

Statistiques Ping pour 11.0.0.2:
    Paquets : envoyés = 37, reçus = 33, perdus = 4 (perte 10%),
Durée approximative des boucles en millisecondes :
    Minimum = 603ms, Maximum = 676ms, Moyenne = 649ms
```

FIGURE IV.14 : Délai adapté d'un *ping* ICMP sur le lien WAN de la plate-forme (source : archives personnelles).

Sur cette liaison, dorénavant dégradée par des coupures simulées qui engendrent des pertes de paquets, des délais et des corruptions, nous envoyons depuis le navire vers la terre notre flux de cybersurveillance pour vérifier la fiabilité de l'architecture et l'absence de perte d'information due au lien satellite. Pour assurer la complétude des données, nous réalisons une somme de contrôle cryptographique au départ et à l'arrivée des données. Nous constatons que les sommes de contrôle à l'arrivée et au départ sont identiques : par conception, l'architecture définie permet donc de garantir l'absence de perte de données sur le lien satellite. Nous avons également, à plusieurs reprises, interrompu volontairement la liaison de données. Malgré ces coupures, l'ensemble des données a bien été réceptionné, le SSM côté bord assurant le cache des données (dans la limite de la taille de son disque dur) tant qu'elles n'ont pas été réceptionnées par le SSM côté terre.

Il convient également de noter qu'il n'est pas concevable d'utiliser l'ensemble de la bande passante satellite aux seules fins de détection d'anomalies cyber. Il convient donc, au sein du lien satellite, de contraindre également le lien entre les SSM. La valeur précise de la bande passante nécessaire dépend du type de navire, du nombre de capteurs et de leur paramétrage, ainsi que du volume de données qui transite par le navire. Sur notre prototype, nous avons pu restreindre la bande passante jusqu'à 1/32è de la bande passante sans que cela n'engendre d'inflexion notable du critère de *freshness*.

L'architecture étant, par conception, qualitative, nous proposons donc de ne pas suivre

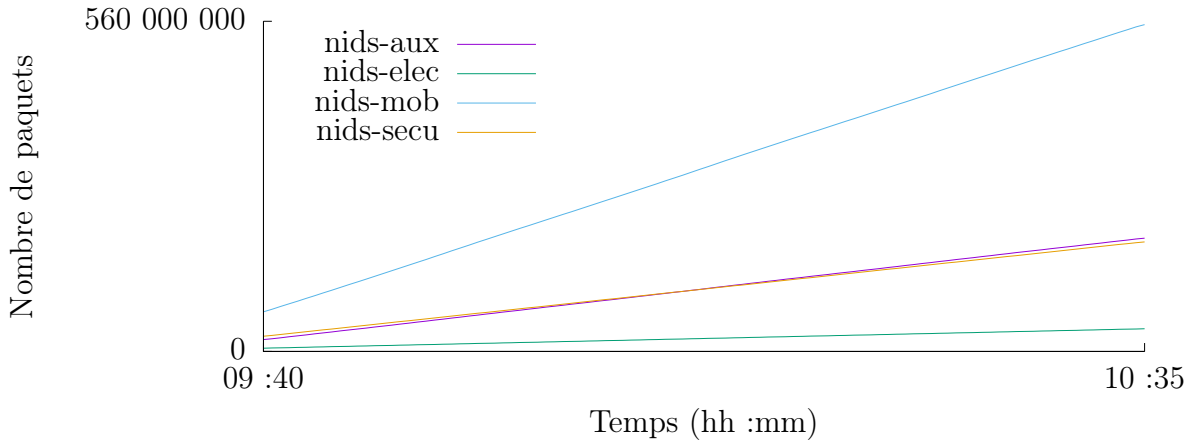

FIGURE IV.15 : Variation du paramètre *stats.capture.kernel_packets* pour les quatre boucles industrielles (source : archives personnelles).

de paramètre associé à ce critère de qualité.

IV.2.3.3 Troisième sous-critère de *Completeness* Q3.3

Sur notre plate-forme prototype nous avons étudié, pour chaque boucle, l'évolution dans le temps de la valeur *stats.capture.kernel_packets*. Cette valeur, renvoyée par le capteur NIDS, indique le nombre de paquets réseau capturés par le noyau GNU/Linux. Nous suivons cette valeur pour le capteur NIDS présent sur chaque boucle (*nids-aux*, *nids-elec*, *nids-mob*, *nids-secu*). Cette mesure a pour objectif de confirmer l'intérêt du suivi du paramètre pour l'établissement de l'indicateur Q3.3, mais aussi de vérifier le caractère déterministe des systèmes industriels de type OT.

La figure IV.15 présente les mesures de l'indicateur Q3.3. L'ordonnée indique la valeur du paramètre *stats.capture.kernel_packets* et l'abscisse le temps, l'échantillonnage étant fixé à 1 s.

Il est intéressant de constater que la relation entre le paramètre *stats.capture.kernel_packets* et le temps s'approche d'une fonction linéaire $f(x) = \alpha x$. L'explication est notamment liée au caractère relativement déterministe des réseaux dits « industriels ». En effet, l'OT est plus caractérisé par le fonctionnement du navire à proprement parler et relativement peu influencé par les activités humaines. *A contrario*, comme on peut le relever sur un système IT (*cf* figure IV.16), le même paramètre évolue de manière non déterministe, ou en tous cas d'un déterminisme fonction de l'activité de

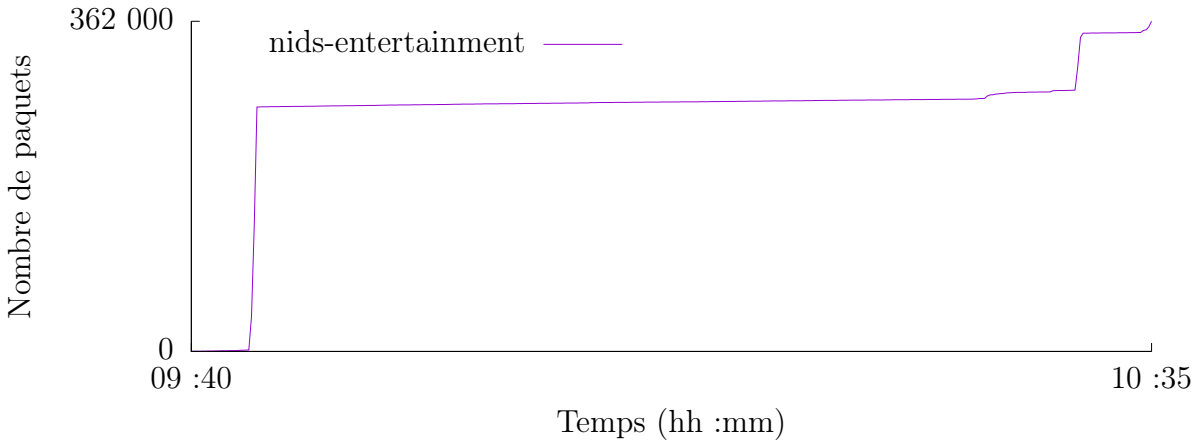

FIGURE IV.16 : Variation du paramètre *stats.capture.kernel_packets* pour un réseau IT (source : archives personnelles).

Tableau IV.1 : Coefficient directeur α de la demi-droite représentative du paramètre *stats.capture.kernel_packets* sur les quatre boucles industrielles

Capteur	**Coefficient α**	**Automates**	**Nb E/S**	**Variables**
NIDS boucle électricité	10,32	4	39	268
NIDS boucle sécurité	45,02	4	49	296
NIDS boucle auxiliaires	54,59	4	50	302
NIDS boucle mobilité	160,43	3	63	540

l'utilisateur sur le réseau (téléchargement de fichiers, vidéos, activité limitée la nuit...). Cette évolution reflète donc à la fois l'activité latente et permanente du système d'information, mais aussi, majoritairement dans le cas de l'IT, le comportement humain.

Le tableau IV.1 indique le coefficient directeur α de la fonction f représentative de la variation du paramètre *stats.capture.kernel_packets*.

Le coefficient directeur α semble lié au nombre d'entrées et de sorties analogiques et numériques par boucle, mais surtout au nombre de scrutations et d'écritures des variables par boucle.

Pour concevoir l'indicateur Q3.3, nous travaillons sur des fenêtres temporelles pour vérifier que, sur la série chronologique, la valeur est stable entre deux fenêtres. La mesure a été réalisée sur une fenêtre de temps glissante de 30 secondes : on réalise donc une mesure du coefficient directeur α à t et t_{+30s} sur les 4 boucles. En simulant une perte de la capture sur une boucle suite à une défaillance matérielle, la fonction f n'est plus linéaire mais devient constante, progressivement ou brutalement : le coefficient directeur α tend vers 0 ou devient

nul : la dégradation est alors immédiatement visible. La figure IV.17 présente les résultats de ce test. La dégradation de Q3.3 apparaît sur la droite du graphique : α tend alors vers 0. Le point de vigilance demeure la largeur de la fenêtre temporelle : trop large, elle risque de ne pas montrer de défauts de captures brefs. Trop courte, elle risque de remonter trop de faux positifs. Dans nos travaux sur plate-forme, la valeur de 30 secondes a donné les meilleurs résultats.

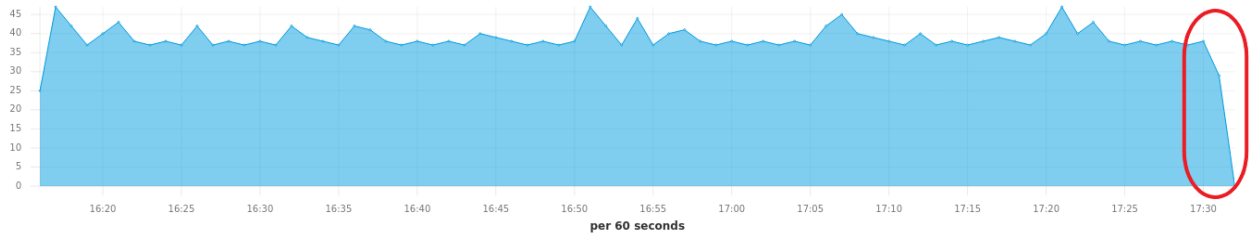

FIGURE IV.17 : Dégradation du sous-paramètre Q3.3 suite à la simulation d'une défaillance matérielle (source : archives personnelles).

IV.2.4 Critère de qualité Q4 - *Freshness* et *timeliness*

Le quatrième critère de qualité, Q4, vérifie la fraîcheur des données en entrée (*freshness*). Le bon ordonnancement des données en entrée (*timeliness*) s'avère également essentiel pour qu'elles soient présentées à l'analyse dans le bon ordre, afin de permettre la réalisation de chronologies lors des phases d'investigation numérique (aussi appelées *timelines*).

Pour le critère de *freshness*, nous établissons un indicateur correspondant à la différence entre l'horodatage à l'insertion dans le lac de données (LE) ($t_{@timestamp}$) et l'horodatage de la capture ($t_{timestamp}$) par le NIDS :

$$Q4 = t_{@timestamp} - t_{timestamp}$$

Q4 est calculé, dans le LE, par la formule *Painless* proposée à la figure IV.18.

```
if(!doc['timestamp'].empty) {
return (doc['@timestamp'].value.getMillis() -
doc['timestamp'].value.getMillis())/1000 }
```

FIGURE IV.18 : Formule de calcul du critère de *freshness* Q4 (source : archives personnelles).

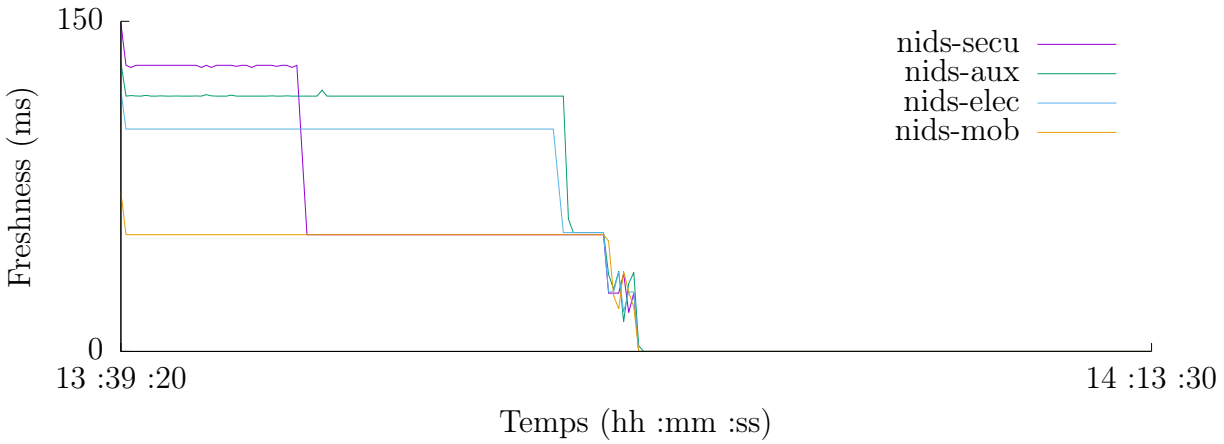

FIGURE IV.19 : Amélioration du critère de *freshness* des données pendant la phase de synchronisation NTP (source : archives personnelles).

La fraîcheur est essentiellement dépendante du bon fonctionnement du lien satellite (absence de coupure) et de la bande passante disponible. Ainsi, une métadonnée capturée à un temps t, mais qui n'aurait pas pu être transmise immédiatement verra son critère de fraîcheur moins bon que celui d'une métadonnée remontée immédiatement entre le SIM et le SIEM à terre, qui aura une meilleure fraîcheur (de l'ordre de 350 *ms*, liée au délai du lien satellite). La précision nécessite bien sûr une synchronisation parfaite des horloges du capteur et du SIEM, par exemple par le recours à une référence horaire fiable type GNSS.

Dans le cadre de notre prototype, nous avons réalisé un graphique temps-réel qui permet de suivre l'évolution du paramètre de qualité *freshness* à bord du navire simulé et au niveau du SIEM de l'armateur. La figure IV.19 présente la phase de synchronisation *Network Time Protocol (NTP)*. Au départ, les capteurs et le SIEM ne sont pas synchronisés d'un point de vue horaire (du début du graphique jusqu'à 13 h 55 min 00 s environ). La synchronisation NTP porte progressivement ses effets pour arriver, à compter de 13 h 56 min 00 s environ, à une synchronisation quasiment parfaite et à un excellent niveau de *freshness*. La mesure de la *freshness* permettrait d'établir rapidement, au-delà d'une défaillance franche et toutes choses égales par ailleurs, une moindre qualité de l'horloge d'un capteur.

La mesure de qualité liée à l'ordonnancement (*timeliness*) a pour objectif de vérifier que, même en cas de coupure satellite, les données reçues après la coupure sont bien exhaustives et qu'elles sont réindexées avec le bon horodatage. Si ce n'était pas le cas, elles pourraient se retrouver manquantes ou disséminées à des horodatages qui ne correspondent pas à leur horodatage de génération (par exemple : leur heure d'indexation dans le CE). Pour réaliser cette mesure, un fichier comprenant un million d'évènements est généré. Chaque évènement

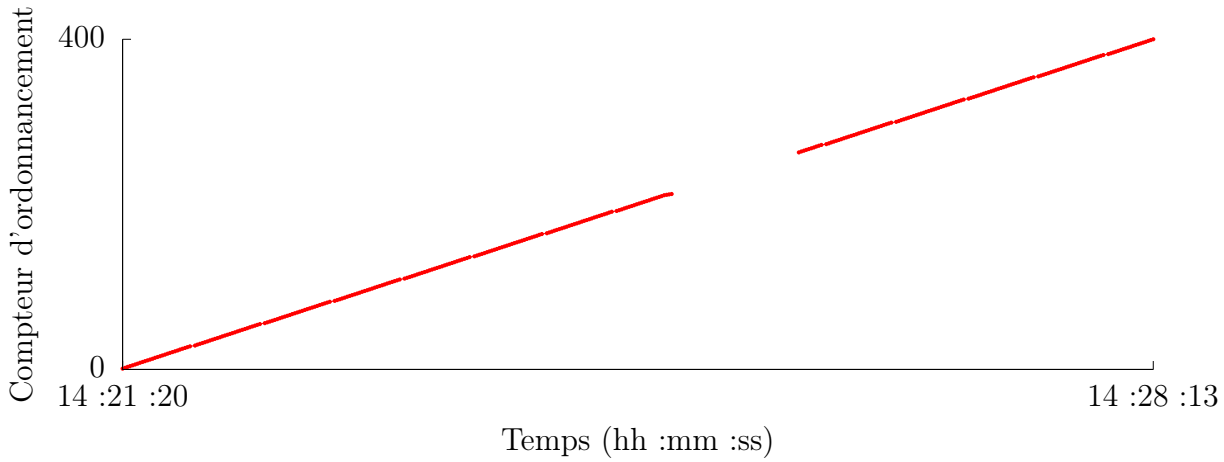

FIGURE IV.20 : *Timeliness* des données suite à une coupure satellite (source : archives personnelles).

est séparé d'une seconde, et ordonné par un index incrémenté à chaque évènement. Nous émettons ensuite ce fichier à destination du *local engine* embarqué et du *local engine* à terre, en réalisant des coupures du lien satellite. À l'arrivée, nous vérifions que le message est exhaustif, que les données sont arrivées dans l'ordre et qu'elles sont correctement réindexées. La figure IV.20 permet d'identifier la progression régulière de la réception de l'index au niveau du LE jusqu'à la coupure satellite (14 h 25 min 00 s, heure du SIEM). Le graphique semble indiquer une perte des index correspondants. Cependant, l'analyse des données reçues (tableau IV.2) montre que les données correspondantes sont bien reçues, la seule différence étant que certains index *n+1* ont été reçus en même temps que des indices *n*. La mauvaise interprétation possible est liée au fait que l'horodatage de l'outil est réalisé sur la référence horaire du SIEM et non du capteur, d'une part, et à l'outil de graphe qui ne représente pas correctement la réception exacte des données. En utilisant la référence horaire du SIEM et une fenêtre de temps plus courte, on vérifie alors que les données correspondantes ont bien été reçues (voir, à la figure IV.21, la récupération du retard, cerclée de rouge). L'utilisation de l'horodatage du capteur permet donc de pallier cette situation : les données transmises sont indexées à la valeur de l'horodatage du capteur et non à celle du SIEM, garantissant une chronologie cohérente : le critère de *timeliness* est ainsi garanti par conception.

IV.2.5 Analyse de la qualité - Conclusion

Le travail réalisé a permis, au-delà de la réalisation et de l'instrumentation d'un *cyber range* maritime réaliste à des fins de prototype, d'apporter une plus-value et des précisions

Tableau IV.2 : *Timeliness* des données suite à une simulation de coupure satellite

Horodatage	***Timeliness***
4 Mars 2020 14 :25 :14.661	231
4 Mars 2020 14 :25 :13.659	230
4 Mars 2020 14 :25 :12.656	229
4 Mars 2020 14 :25 :12.656	227
4 Mars 2020 14 :25 :12.656	228
4 Mars 2020 14 :25 :12.655	225
4 Mars 2020 14 :25 :12.655	226
4 Mars 2020 14 :25 :12.654	223
4 Mars 2020 14 :25 :12.654	224
4 Mars 2020 14 :25 :12.653	222
4 Mars 2020 14 :25 :12.641	221
4 Mars 2020 14 :25 :12.640	219
4 Mars 2020 14 :25 :12.640	220
4 Mars 2020 14 :25 :12.639	217
4 Mars 2020 14 :25 :12.639	216
4 Mars 2020 14 :25 :12.639	218
4 Mars 2020 14 :25 :12.638	215

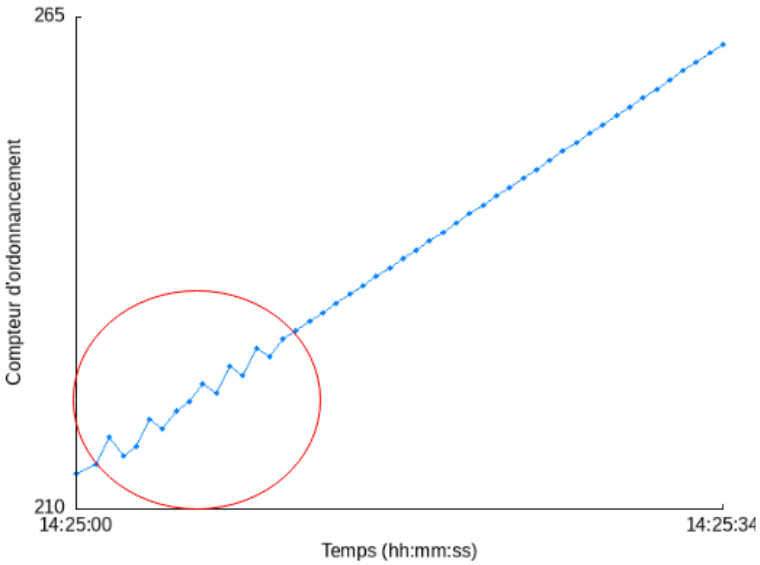

FIGURE IV.21 : Récupération du retard dans la réception du compteur (source : archives personnelles).

importantes sur les notions de qualité appliquée au contexte de la détection d'anomalie cyber sur des systèmes maritimes et cyber physiques. Derrière chaque terme générique (*trustworthiness*, *truthfulness*, *completeness*, *freshness*, *timeliness*), nous avons proposé, formalisé, généré

et mesuré ces valeurs en temps réel sur notre plate-forme, afin de disposer, à tout moment, d'une mesure de qualité essentielle à l'élaboration de la MCSA et à la prise de décision. Nous avons vu que, dans le contexte de la MCSA, la qualité des critères de *completeness*, *freshness* et *timeliness* sont essentiels par rapport à une CSA plus générique hors contexte maritime. Nous avons démontré que notre architecture permettait de garantir cette qualité ou, à défaut, d'en mesurer les écarts.

La prise en compte de cette qualité et des spécificités des systèmes surveillés (IT/OT) permet de faciliter l'emploi et l'analyse de données issues d'outils cyber de conception, d'origine et d'objectifs variables. La confiance, la précision, la fraîcheur des données qu'ils produisent peuvent être suivis pour déterminer la qualité des informations nécessaires à la prise de décision. Cette phase prototype, indispensable à la validation de notre modèle, nous permet à présent de garantir la qualité des données que nous collectons et de poursuivre nos travaux.

IV.3 Visualisation et cartographie - résultats

Dans cette section, nous répondons à la question de recherche QR2 sur ses aspects visualisation, et à une partie de la QR3 sur la détection d'anomalie sur les SIM ainsi qu'aux points évoqués dans la section III.4. Afin de valider les apports de la MCSA, l'ensemble de nos travaux sera mené sur notre plate-forme prototype.

IV.3.0.1 Cartographie passive dynamique

Les informations qui peuvent être collectées passivement sur notre *cyber range* sont particulièrement variées. Certaines peuvent être communes à tous les systèmes IT et OT (adresses physiques de couche 2, certaines métadonnées de couche 3). D'autres sont spécifiques aux systèmes industriels, mais peuvent être rencontrées sur des systèmes à terre (protocoles S7, Modbus ou autres). Enfin, certaines s'avèrent spécifiques aux SIM (standards NMEA, etc.). L'analyse temps réel du réseau, telle que réalisable avec l'architecture proposée, permet également d'obtenir des informations sur les logiciels installés, par l'interception de bannières, de négociations et ceci, de manière totalement passive. Ce type de technologie, souvent appelée *fingerprinting*, présente un intérêt majeur dans le cadre des systèmes maritimes, afin d'améliorer de manière notable la KU des SIM.

Dans ce cadre, la difficulté n'est pas tant la collecte des données (*situation perception*) que leur analyse (*situation comprehension*). Dans un premier temps, un ensemble dynamique de représentations graphiques a été conçu. Il permet de fusionner, d'enrichir au mieux et d'afficher les informations pertinentes relatives à un équipement (par exemple, une machine ou un automate), à des fins de cartographie et de détection d'anomalie, à partir d'une source de données multicapteurs. La figure IV.22 montre ainsi le type de visualisation qui peut être réalisé et qui représente un gain important en termes de temps pour l'analyste qui obtient alors une représentation efficace et immédiate des données à sa disposition. En un seul tableau temps-réel, l'ensemble des informations captées passivement est ainsi présenté. Les informations disponibles comprennent, par exemple, la répartition des protocoles réseau utilisés par la machine, le *HTTP User-Agent*, les alertes détectées par les capteurs et relatives à la machine et leur répartition dans le temps, les ports sources / destination utilisés et le volume de trafic concerné, les requêtes DNS émises par la machine et le nombre de requêtes associées, ou encore les machines avec lesquelles elle échange le plus, en émission et en réception.

IV.3.0.2 Visualisation des flux réseau

Les graphes à coordonnées parallèles sont particulièrement adaptés à la visualisation des flux de données qui transitent sur le réseau [CTSdG12]. En effet, d'une perspective cognitive, une connexion réseau entre un équipement A et un équipement B se représente facilement par un segment. Si ce type de graphique est généralement réalisé *a posteriori* sur des données collectées, notre architecture permet de le réaliser, en temps réel, sur des SIM distants, soit sur les données des couches 2, 3 et 4 du modèle *Open Systems Interconnection (OSI)*, soit sur les couches applicatives, à partir du moment où les données peuvent être collectées et interprétées par les capteurs utilisés.

Pour cela, nous utilisons l'architecture décrite à la figure IV.6 et réalisons des requêtes au niveau du CE du SOC. Étant donné le nombre de capteurs positionnés, nous sélectionnons à chaque fois un sous-réseau, afin de pouvoir représenter les échanges en temps réel. Les données obtenues au niveau flux permettent de correctement séparer le sens des connexions (client/serveur et serveur/client), de manière à réaliser correctement le graphique, comme on le voit dans la figure IV.23. Il convient cependant de noter que l'activation des données *netflow* ou *flow* dans les capteurs à bord représente un sur-débit non négligeable pour le lien satellite montant, qui impacte les autres flux du navire qui utilisent cette même liaison.

FIGURE IV.22 : Fusion de données multicapteurs (NIDS, HIDS) à des fins de détection d'anomalies sur un SIM (source : archives personnelles).

Mais c'est, à l'heure actuelle, la seule manière de disposer de l'information du sens de la connexion, information absente dans les pré-processeurs applicatifs du NIDS (comme on le voit à la figure IV.24).

La conséquence de cette absence est que le port de destination n'est pas une donnée directement exploitable pour réaliser, par exemple, un graphe à coordonnées parallèles. En effet, la répartition des ports de destination (*dest_port*) mélange ports sources et ports de destination, comme on le voit à la figure IV.25, sous forme de *scatter plot* : les ports de destination issus des réponses du serveur vers le client sont regroupés en haut (ports au

```
dest_ip: 34.95.71.207
src_ip: 192.168.1.44
@timestamp: Aug 22, 2019 @ 13:14:27.281
app_proto: tls
timestamp: Aug 22, 2019 @ 13:14:27.069
dest_port: 443
tcp.psh: true
tcp.ack: true
tcp.state: established
tcp.tcp_flags_tc: 1a
tcp.syn: true
tcp.tcp_flags_ts: 1a
tcp.tcp_flags: 1a
proto: TCP
@version: 1
tags: suricata
event_type: flow
src_port: 33,496
flow_id: 654,490,614,960,586
flow.state: established
flow.end: Aug 22, 2019 @ 13:13:28.690
flow.pkts_toserver: 24
flow.pkts_toclient: 21
flow.age: 59
flow.bytes_toclient: 2,668
flow:start: Aug 22, 2019 @13:12:29.987
flow.bytes_toserver: 3,171
flow.reason: shutdown
flow.alerted: false
```

FIGURE IV.23 : Aperçu des données avec la capacité *flow* activée sur un NIDS (source : archives personnelles)

minimum > 1024), alors qu'il s'agit en fait de ports source au sens du *three-way handshake* du protocole *Transport Control Protocol (TCP)*. De même, les ports de destination réels des serveurs sont visibles en bas du graphique ($dest\_port < 1024$, de manière générale).

Comme on le voit à la figure IV.26, ce défaut a pour conséquence d'obtenir un graphique à coordonnées parallèles avec un effet « miroir » au niveau des ports source et destination, et un mélange des adresses IP source et destination. Nous proposons une solution qui propage le sens de la connexion au niveau des datagrammes applicatifs (couches ≥ 4 du modèle OSI)

```
in_iface: wlp2s0
dest_ip: 192.168.1.44
src_ip: 192.168.1.254
@timestamp: Aug 22, 2019 @ 13:12:30.274
timestamp: Aug 22, 2019 @ 13:12:29.987
dest_port: 36,211
proto: UDP
@version: 1
tags: suricata
event_type: dns
src_port: 53
flow_id: 1,815,519,059,369,073
dns.rd: true
dns.grouped.A: 34.95.71.207
dns.grouped.CNAME: prod.webextstoragesync.prod.cloudops.mozgcp.
net
dns.version: 2
dns.id: 6,680
dns.answers: {
    "rrname": "webextensions.settings.services.mozilla.com",
    "rrtype": "CNAME",
    "ttl": 85,
    "rdata": "prod.webextstoragesync.prod.cloudops.mozgcp.net"
},
{
"rrname": 'prod.webextstoragesync.prod.cloudops.mozgcp.net",
"rrtype": "A",
"ttl": 1603,
"rdata": "34.95.71.207" }
dns.rrname: webextensions.settings.services.mozilla.com
dns.foags: 8180
dns.rrtype: A
dns.type: answer
dns.qr: true
dns.rcode: NOERROR
dns.ra: true
```


FIGURE IV.24 : Aperçu des données issues d'un NIDS au niveau applicatif (source : archives personnelles)

[Jac19a]. Son intégration dans le NIDS Suricata [5] est en cours. Elle permettra l'obtention d'un

5. https ://github.com/OISF/suricata/pull/3521

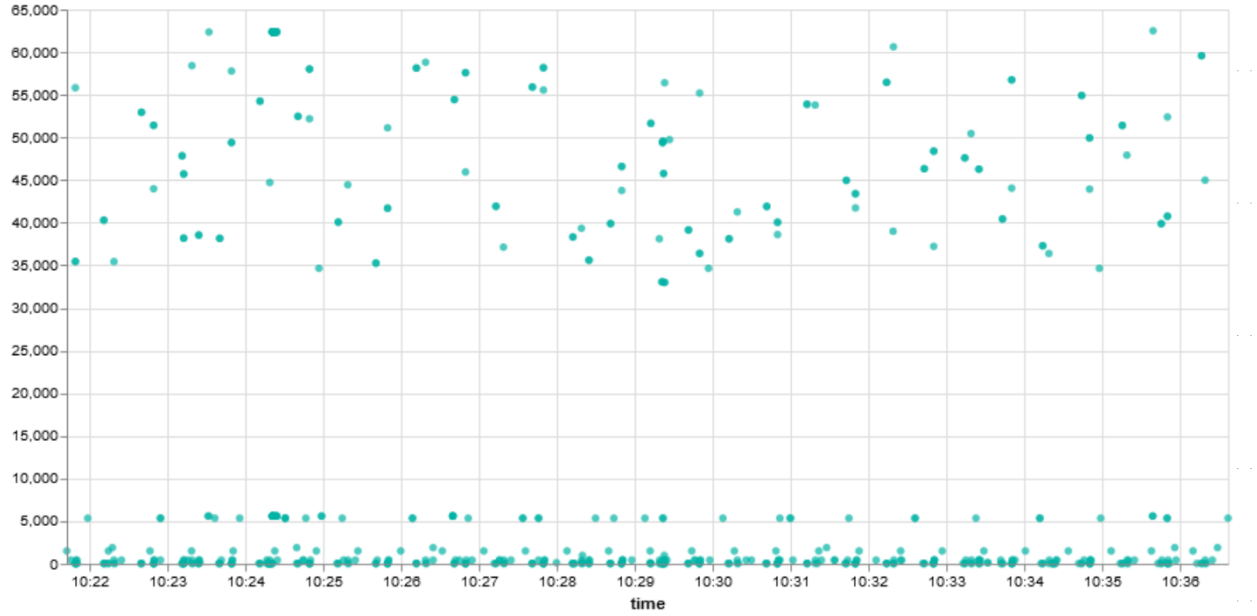

FIGURE IV.25 : Graphe de la métadonnée *dest_port* (ordonnée) dans le temps (source : archives personnelles).

graphe à coordonnées parallèles où les ports source et destination apparaissent correctement, comme le montre la figure IV.27. Ce graphe temps-réel permet alors clairement de distinguer les ports sources utilisés par une machine (ici, essentiellement dus à de nombreux onglets dans un navigateur web) et les ports de destination (53, 80, 443). Réalisé sur une période plus longue, ce graphe est représentatif des flux de données utilisés au sein d'un réseau. Dans certains cas (navire à quai, par exemple), les graphes obtenus par l'utilisation d'un outil compatible *netflow* restent cependant plus complets, car ils sont indépendants des capacités du NIDS en termes de dissecteur. Au final, ce type de graphe permet, dans un premier temps, d'améliorer la KU des SIM et, par ailleurs, facilite la détection d'anomalies de manière graphique.

IV.3.1 Évaluation dynamique des risques

L'évaluation dynamique des risques (*Dynamic Risk Assessment (DRA)*) est un enjeu important de la recherche en cybersécurité pour réaliser une analyse précise des risques et favoriser la prise de décision. Les travaux de recherche sur ce sujet se poursuivent [GGDM+18, Lag10, LPV13], y compris dans un contexte maritime [PPM18]. Sa réalisation en temps réel apporterait une réelle plus-value pour l'établissement des différents processus de *situation assessment* nécessaires à l'élaboration de la MCSA, mais aussi pour établir les liens entre

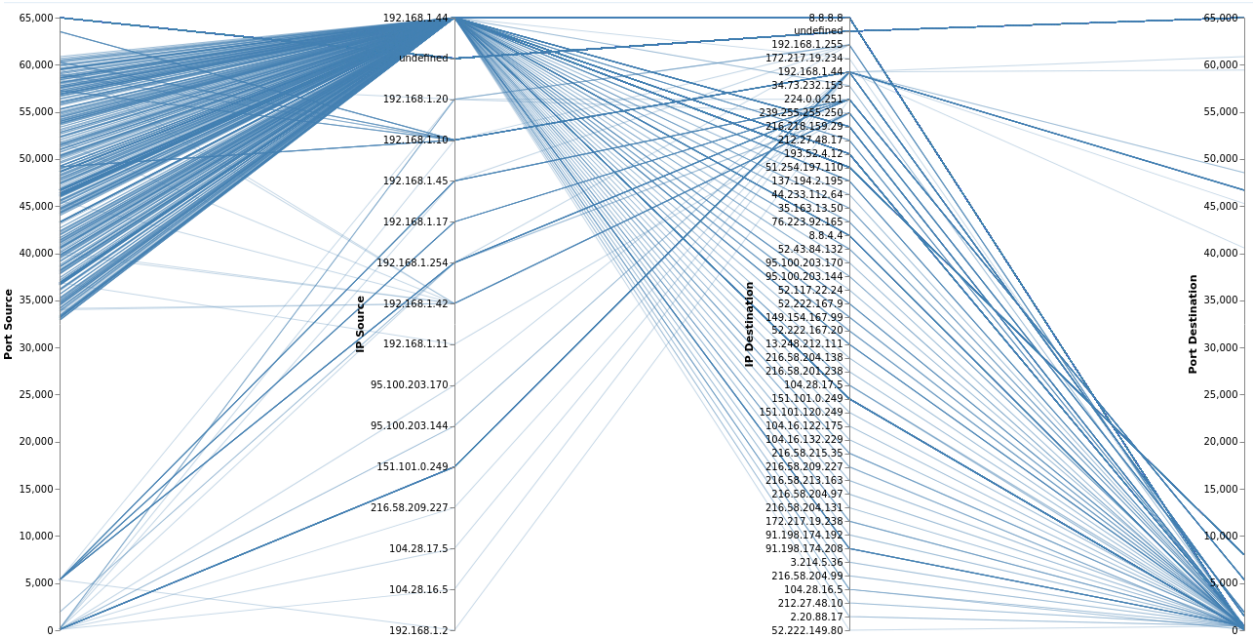

FIGURE IV.26 : Graphe à coordonnées parallèles temps réel obtenu sans le correctif proposé (source : archives personnelles).

les informations de sources et de formats différents. Au niveau *situation comprehension*, la DRA pourrait faciliter la visualisation des données, leur analyse, ainsi que les liens entre les métadonnées. En termes de *situation projection*, la cartographie dynamique des constituants d'un SIM permettrait d'identifier les systèmes qui pourraient constituer des cibles potentielles en raison de leurs vulnérabilités. Enfin, la DRA pourrait également concourir à la *situation resolution* en facilitant la prise de décision.

Nous avons souhaité apporter une contribution sur deux aspects contributifs à la DRA. D'une part, nous nous sommes intéressés à la visualisation d'informations d'intérêt cyber à base de graphes à des fins de détection d'anomalies, notamment dans l'optique de favoriser la représentation des données. D'autre part, nous avons souhaité évaluer la plus-value de la DRA pour la prise de décision et le partage de situation cyber. Dans le contexte de visualisation et de compréhension d'une masse importante de données, la prise de décision peut-être longue et difficile. En effet, en cas de détection, elle nécessite de pouvoir rapidement identifier les impacts potentiels (*impact assessment*), mais aussi la cause (*causality assessment*). Or, les données généralement présentes dans un SIEM sont peu liées entre elles (on parle aussi de pivot), et l'opérateur doit régulièrement basculer d'outils ou de base de données pour obtenir une compréhension correcte de la situation.

Pour cela, nous avons créé une base de données graphes qui assure le lien entre plusieurs

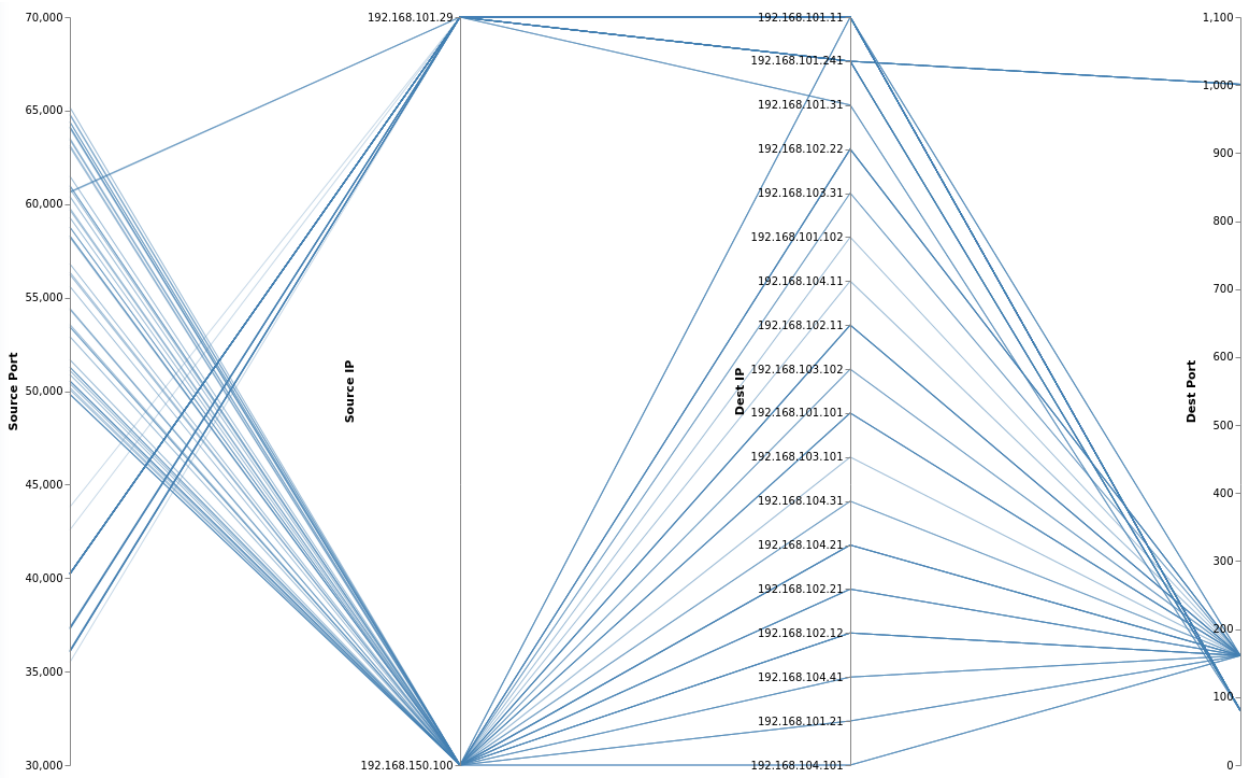

FIGURE IV.27 : Graphe à coordonnées parallèles temps réel obtenu avec le correctif proposé (source : archives personnelles).

types de données sur notre plate-forme prototype de cybersurveillance du *Naval Cyber Range*. Nous utilisons les métadonnées enrichies, collectées et indexées dans le CE et réalisons un lien entre elles pour faciliter l'analyse (figure IV.28). Nous y intégrons également le correctif proposé au paragraphe IV.3.0.2 pour faciliter le suivi de connexion. L'analyste d'un SOC peut alors rapidement identifier les connexions suspectes issues d'une machine ou d'un réseau, en s'aidant de l'ensemble des données associées présentes dans le CE (heure, libellé de l'alarme ou des journaux concernés, adresses IP résolues...). L'apport aux processus de *situation comprehension*, *causality assessment* et *situation resolution* dans le contexte maritime est donc substantiel.

Afin d'obtenir les figures IV.29 et IV.30, nous lions à présent les données issues du CE (métadonnées issues de capteurs embarqués) avec les données issues d'un CSIRT afin d'identifier et de grapher instantanément les machines vulnérables à une *Common Vulnerabilities and Exposures (CVE)* particulière, de manière passive (utilisation des métadonnées des en-têtes), ou par l'utilisation des données remontées par un HIDS. À la figure IV.29, nous identifions ainsi une machine (ip-12-34-56-7...) qui attaque le serveur « ship1_intranet » le 7

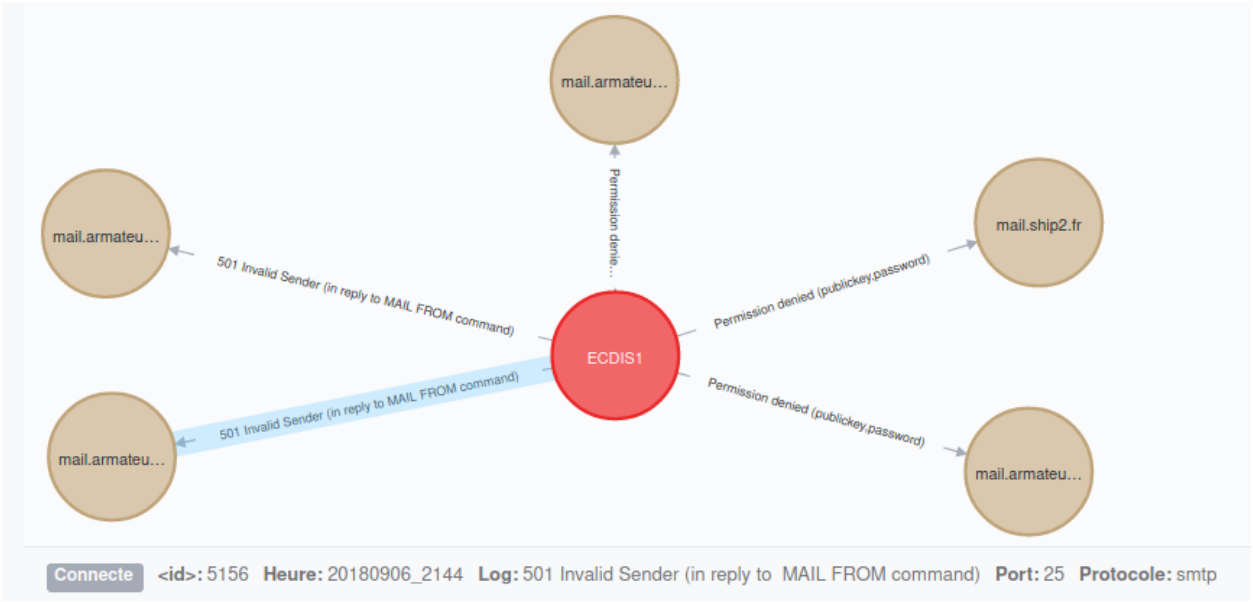

FIGURE IV.28 : Analyse d'un cas de connexions anormales en provenance d'un ECDIS (source : archives personnelles).

janvier 2020, avec une signature spécifique remontée par le capteur. Le même graphe (figure IV.30) permet aussi d'identifier que le serveur en question dispose du logiciel *Content Management System (CMS)* « Wordpress », dont la version est vulnérable à une CVE, identifiée sous le numéro CVE-2017-14723. Les métadonnées de cette CVE (*Common Vulnerability Scoring System (CVSS)*, catégorie, description) peuvent permettre de penser qu'elle a été exploitée pour mener une attaque sur le serveur. Dans un contexte maritime, ce type de graphe qui assure une fusion et un lien rapide entre les données facilite grandement l'identification des vulnérabilités, que ce soit suite à la parution de nouvelles CVE, mais aussi pour l'analyse, en liant ces informations à des violations potentielles de sécurité.

FIGURE IV.29 : Visualisation et lien quasi temps réel des métadonnées relatives à l'attaque par l'utilisation de graphes (source : archives personnelles).

Il convient également de noter que ce type de graphe peut concourir à la *situation*

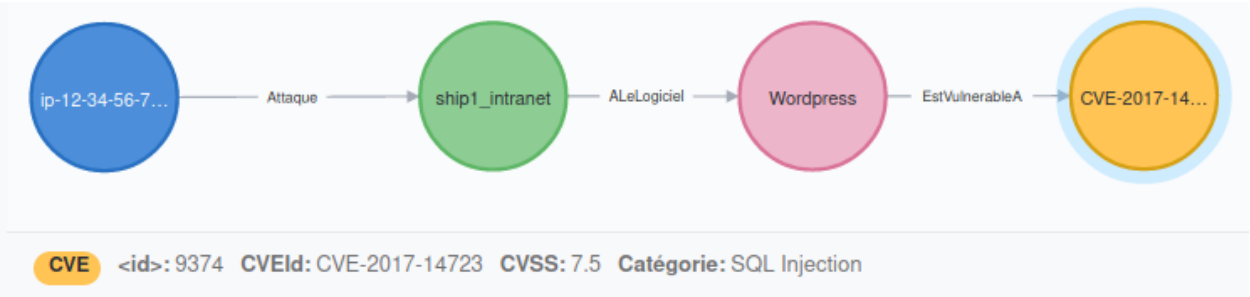

FIGURE IV.30 : Apport de la base de données graphes pour établir le lien temps-réel entre les signaux d'une attaque, les données KU et une CVE potentiellement exploitée (source : archives personnelles).

resolution. À la figure IV.31, nous importons des données complémentaires relatives aux correctifs de sécurité des éditeurs puis créons le lien entre la CVE et un éventuel correctif de l'éditeur, en précisant les vulnérabilités corrigées, le lien de téléchargement du correctif, etc. Ainsi, entre la détection d'une alerte (KT), la connaissance du système impacté (KU), des impacts éventuels, de la CVE et du correctif, l'ensemble des processus nécessaires à l'élaboration de la MCSA est établi et le gain de temps et de précision est particulièrement appréciable.

FIGURE IV.31 : Apports d'une base de données graphes en partant de la *situation perception* jusqu'à la *situation resolution* (source : archives personnelles).

IV.4 Application de la MCSA par domaine : détection et visualisation sur des données NMEA 0183, contribution à la mise en place d'une détection par apprentissage automatique

Dans ce chapitre, nous terminons nos travaux sur la QR3 en abordant les questions de détection d'anomalies sur les SIM, et précisément sur les réseaux qui utilisent NMEA 0183. NMEA 0183 est un standard propriétaire développé à partir des années 1990, qui permet

l'interopérabilité et l'interconnexion des différents équipements utilisés en passerelle (ECDIS, récepteur ou transpondeur AIS, radars, sondeurs, capteurs divers, etc.). Ce standard permet la fusion et la représentation de l'information issue des différents capteurs, généralement au niveau des ECS et ECDIS. L'analyse des données du réseau sur lequel transitent des informations NMEA peut donc permettre d'identifier des incohérences et des anomalies dans ces informations dont la qualité est indispensable à l'élaboration de la *Maritime Situational Awareness (MSA)*.

IV.4.1 Contexte

Plusieurs études et articles scientifiques ont démontré les vulnérabilités des ECDIS en tant qu'outils de fusion [Svi19], mais aussi des capteurs qui les alimentent, comme l'AIS [BPW14, BG17, Bur16] ou encore les GNSS tels que le GPS [6], sensibles au leurrage et au brouillage [ABPG20]. Ces vulnérabilités, qui deviennent critiques avec le développement des drones de surface autonomes (*Unmanned Surface Vehicle (USV)*) [Kav18], sont régulièrement exploitées par des attaquants dans les zones de conflit et sont regroupées sous le terme de *Navigation War (NAVWAR)*.

La fusion d'informations nécessaires à l'élaboration de la MSA à bord d'un navire s'appuie donc sur un standard, NMEA 0183, faillible par conception et qui collecte des données multicapteurs dont l'authenticité, la sincérité et la cohérence ne peuvent être garanties.

IV.4.2 Description du standard NMEA 0183

Au niveau physique et électrique, ce protocole s'appuie sur les normes EIA RS-232 ou EIA RS-422 pour échanger des données en utilisant l'encodage *American Standard Code for Information Interchange (ASCII)*.

```
$GPGGA,064036.289,4836.5375,N,00740.9373,E,1,04,3.2,200.2,M
,,,,0000*2E
```

FIGURE IV.32 : Exemple d'une trame GPGGA circulant sur un réseau NMEA 0183 (source : Wikipédia, licence : CC BY-SA 3.0).

6. https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5c99488beb39314c45e782da/1553549492554/Above+Us+Only+Stars.pdf

La figure IV.32 montre un exemple de trame de position transmise par un récepteur GPS sur un réseau qui utilise le standard NMEA 0183. Les deux premiers caractères situés après le signe $ permettent d'identifier l'équipement émetteur de l'information (*talker id*). Ainsi, *GP* signifie que l'on a affaire à un équipement GPS, mais d'autres identifiants existent comme *AI*, pour un équipement AIS, *RA* pour un radar de type *Automatic Radar Plotting Aid (ARPA)*. Les trois lettres suivantes précisent le type de trame : en l'occurrence, une trame *GGA* indique l'heure d'envoi de la trame en temps universel, la position en latitude et en longitude, le type de positionnement, le nombre de satellites utilisés pour calculer les coordonnées, la précision horizontale, l'altitude en mètres, de même que plusieurs champs additionnels. Les deux caractères après le caractère « * » correspondent à un contrôle de parité (par une opération $\oplus$ sur l'ensemble des caractères compris entre les signes $ et *). Il existe également d'autres trames comme *GPRMC*, qui indique la latitude, la longitude, la date, la vitesse et la route sur le fond, mais sans information d'altitude. Nous avons recensé plus d'une centaine de références de *talkers ids* et 210 références de *sentences ids*, que nous avons intégrées, pour celles ne l'étant pas déjà, dans un dissecteur NMEA utilisable par les logiciels d'analyse réseau *tshark* et *Wireshark*[7].

Dans le cadre de notre plate-forme expérimentale, nous avons mis en place un bus NMEA (versions 0183 et 2000) utilisant un récepteur GPS Furuno ® GP-33 et un récepteur AIS Furuno ® FA-30, ainsi que les antennes associées (*cf* figure IV.3). Le bus NMEA connecte chaque équipement pour permettre l'alimentation et les échanges de données (émission et/ou réception). Dans notre cas, le récepteur GPS émet ses données sur une sortie NMEA 0183 vers un multiplexeur, composé d'un Raspberry Pi équipé d'un *hat* RS-422. Les données issues du Raspberry Pi peuvent ensuite être émises avec le protocole *User Datagram Protocol (UDP)* sur un réseau Ethernet classique et utilisées pour être affichées sur l'*ECS*. Dans la réalité, sur un navire, de nombreux équipements peuvent donc être connectés ensemble, soit sur le bus NMEA à proprement parler, soit après un multiplexeur. Si l'intrusion physique sur un bus NMEA (ajout d'équipement, injection de données) apparaît envisageable, nous avons conduit nos travaux sur la connexion Ethernet et les données NMEA qui y circulent, car ce point constitue un réseau plus facile d'accès à distance et, donc, plus vulnérable. Sur un navire de fort tonnage, ce réseau s'appelle généralement *Integrated Navigation System (INS)*, et est parfois lui-même intégré dans un réseau plus large, qui comprend aussi les systèmes de contrôle/commande et de supervision des réseaux industriels embarqués et

7. https://github.com/kmpm/wireshark-nmea/commit/5064cfcbb026d08454c392818ac6b64e42689881#diff-ed9edf58cc775cca6a485eb01b4638e7 et https://github.com/kmpm/wireshark-nmea/commit/6ffd70c640961f2364b7ee966534437e144fc573#diff-ed9edf58cc775cca6a485eb01b4638e7

que l'on appelle *IBS*.

IV.4.3 Vulnérabilités du standard NMEA 0183

Le standard NMEA 0183 est soumis à de nombreuses vulnérabilités qui peuvent être classées dans deux catégories distinctes : les vulnérabilités extrinsèques et les vulnérabilités intrinsèques. Les premières sont liées aux capteurs raccordés au bus NMEA : ils peuvent eux-mêmes s'avérer vulnérables, défaillants, de mauvaise qualité, ou soumis à des perturbations externes (leurrage ou brouillage dans le cas d'un GNSS) ou encore environnementales : la qualité des données injectées sur le bus NMEA peut donc en souffrir, et peu d'informations de qualité sont transmises au sein des *sentences* NMEA. Les vulnérabilités intrinsèques au réseau NMEA sont, quant à elles, liées à ses défauts de conception (attaques physiques, absence de dispositif qui permette de garantir l'authenticité, l'intégrité, la confidentialité, la disponibilité, la traçabilité et la non-répudiation des données).

IV.4.4 Particularités du standard NMEA 0183 à des fins de détection d'anomalies

Durant nos travaux sur plate-forme prototype, nous avons pu réaliser ou obtenir de nombreuses captures de trafic NMEA 0183 avant ou après leur passage par un multiplexeur, le trafic étant alors transmis en utilisant le protocole UDP et, dans une moindre mesure, TCP. La détection d'anomalies sur un réseau NMEA peut s'effectuer à trois niveaux. Le premier, essentiellement une fois que le trafic est multiplexé et encapsulé dans le protocole UDP, consiste à détecter des anomalies dans le trafic IP circulant sur le réseau INS. Le second revient à analyser l'enveloppe de la trame NMEA et ses caractéristiques. Enfin, le troisième niveau concerne les données dynamiques transmises par le standard (par exemple : positions géographiques, pistes AIS, données environnementales, etc.), parfois appelées « charge utile ».

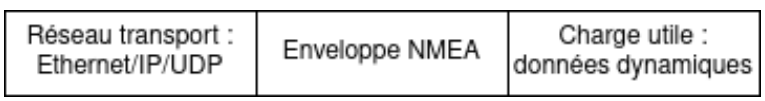

FIGURE IV.33 : Les trois niveaux possibles de détection d'anomalie sur un réseau NMEA 0183, une fois multiplexé et encapsulé (source : archives personnelles).

Tableau IV.3 : Caractéristiques des fichiers de capture du trafic NMEA

Nom	**Nombre de paquets**	**Durée de capture (s)**	**Paquets/s**	**Taille moyenne des paquets**	**Débit moyen (o/s)**
cap1.pcapng	22 707	385	58,9	86	5044
cap2.pcapng	22 574	209	122,3	87	10 651
cap3.pcapng	29 330	234	125,3	87	10 889

IV.4.4.1 Particularités de l'enveloppe NMEA 0183

Parmi ces captures, nous avons isolé trois captures significatives de trafic NMEA, appelées *cap1*, *cap2* et *cap3*. Le tableau IV.3 synthétise les caractéristiques de ces captures, qui représentent un total de 9,3 millions de paquets. Deux remarques peuvent être réalisées en première analyse : la taille moyenne des paquets reste stable et faible. En revanche, le débit moyen et le nombre de paquets varient : dans un réseau *a priori* déterministe, nous émettons l'hypothèse que cette variation est liée aux données AIS et radar, hypothèse confirmée en isolant le trafic réseau concerné. Cette différence s'explique par le fait que, suivant la position du navire (quai, mer), sa zone de navigation, voire même les conditions de propagation ionosphérique, le trafic maritime capté dans l'environnement du navire varie fortement : le volume de données retransmis sur le réseau NMEA par les capteurs AIS et radar est donc susceptible de varier de manière significative.

IV.4.4.2 Analyse de l'enveloppe du standard NMEA 0183

Dans cette sous-section, nous réalisons une analyse de l'enveloppe du standard NMEA 0183. Cette analyse a pour objectif de permettre l'identification d'attributs (*features*). Par conception, nous émettons l'hypothèse que le trafic NMEA doit présenter des caractéristiques plutôt déterministes, notamment par le fait que les capteurs émettent probablement leurs données à intervalles réguliers. Nous recherchons donc les caractéristiques d'un système déterministe sur l'enveloppe des trames NMEA. La figure IV.34 indique ainsi la répartition, en nombre, des phrases PHKS (propriétaire), AIVDM (AIS), RATTM (RADAR) et PHTRO (propriétaire), qui présentent toutes un volume caractéristique et significatif, alors que les

sentences du *talker* NW présentent une répartition égale en quantité (4,21 % des trames capturées). Enfin, les trames liées au positionnement et aux paramètres environnementaux (GCGGA, GCVTG, GCZDA, GPRMC, NAVHW, SDDBT, SDDPT, SPDPT) représentent toutes une répartition égale à 2,16 %.

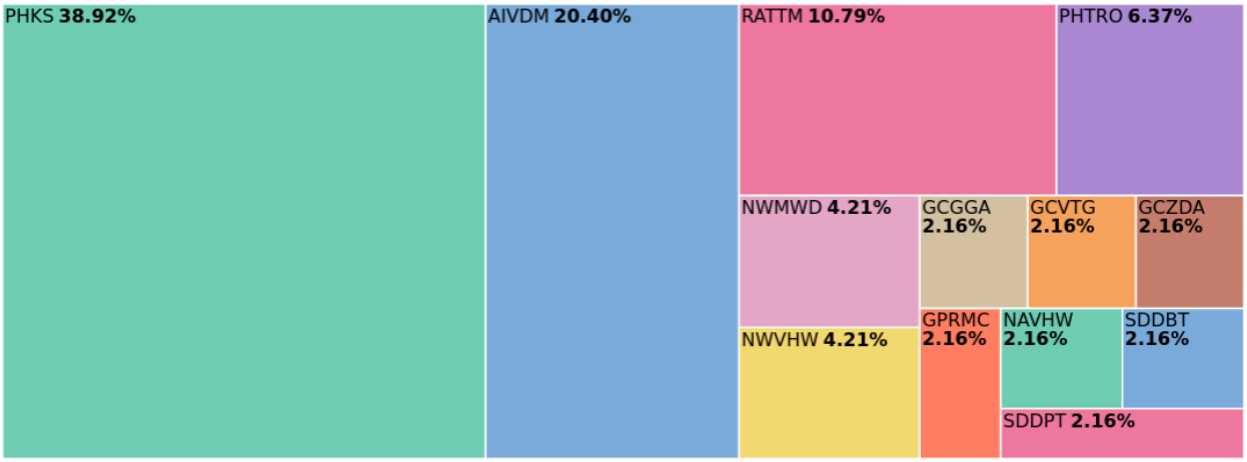

FIGURE IV.34 : Répartition, en nombre, du type de *sentences IDs* sur les fichiers *cap1.pcapng*, *cap2.pcapng* et *cap3.pcapng* (source : archives personnelles).

Ces caractéristiques se confirment lorsque l'on analyse la répartition des paquets de chaque phrase dans le temps : si certaines répartitions n'affichent pas de caractéristique déterministe, car elles dépendent de facteurs extrinsèques [8], pour d'autres, la répartition dans le temps apparaît particulièrement précise et régulière (annexe E). Ce caractère déterministe, qui semble se distinguer, permet de proposer des exemples de mesures particulières pour ces différentes phrases et la sélection d'attributs.

Nous analysons ces fichiers dans le tableau IV.4 pour les *sentences* qui affichent un profil déterministe (c'est-à-dire toutes sauf les sentences AIVDM et les trames propriétaires PH et IO). Nous constatons que plusieurs fréquences peuvent être isolées : 1 Hz pour les *sentences* issues du *talker* RA (OSD et RSD), 2 Hz pour les *talkers* GC, GP, NA, SD et SP, 4 Hz pour le *talker* NW et 10 Hz pour la *sentence* RATTM, les approximations étant dues à la fenêtre de capture, à la technologie de capture et à la précision de l'horloge sur l'ordinateur de capture.

Ce déterminisme dans le temps pourrait ainsi permettre de détecter, sur une durée donnée, un cycle régulier de trames spécifique au système donné et faciliter la détection d'anomalies, par exemple en utilisant le concept de *Cybernetic-DNA*, qui pourrait s'appliquer

8. Par exemple, le nombre de navires détectés au radar ou à l'AIS pour les *sentences* RATTM et AIVDM

Tableau IV.4 : Caractéristiques en période et fréquence

Talker ID, Sentence ID	**Période moyenne (s)**	**Fréquence moyenne (Hz)**
GCGGA	0,497	2,00
GCRMC	0,497	2,00
GCVTG	0,497	2,00
GCZDA	0,5	2,00
GPGGA	0,497	2,00
GPRMC	0,497	2,00
NAGGA	0,497	2,00
NAVHW	0,497	2,00
NAVTG	0,497	2,00
NWGLL	0,256	3,90
NWMWD	0,256	3,90
NWMWV	0,256	3,90
NWVHW	0,256	3,90
RAOSD	0,991	1,00
RARSD	1,00	1,00
RATTM	0,099	10,02
SDDBT	0,497	2,00
SDDPT	0,497	2,00
SPDBT	0,497	2,00
SPDPT	0,497	2,00

avec intérêt sur un réseau déterministe comme celui-ci [MK19].

Sur les fichiers capturés, nous avons identifié que certaines *sentences* ont toujours la même taille (tableau IV.5). D'autres trames ont des tailles variables, c'est notamment le cas des *sentences* RATTM, GGA, GLL, TXT ou encore VTG.

Les captures réalisées permettent également d'identifier plusieurs cardinalités. Ainsi, le nombre de *talkers* et les *sentences* associées sont connus et n'évoluent pas dans le temps.

Nous constatons également que certaines phrases NMEA sont émises par plusieurs *talkers*. Il convient de noter que, si les caractéristiques du réseau NMEA sont liées à des capteurs (et peuvent donc être modifiées), elles peuvent aussi être transformées par des appareils intermédiaires, comme des multiplexeurs : les caractéristiques identifiées sont alors spécifiques

Tableau IV.5 : Exemples de *sentences* de tailles caractéristiques

Sentence IDs	**Taille de la trame (octets)**
DPT	70
MWD	77
MWV	71
NHW	76
OSD	79
RMC	121
RSD	93
TRO	71
VDM	91
VHW	76
VTG	86
ZDA	81

Tableau IV.6 : *Talkers ID* et *sentence ID* des fichiers *cap1*, *cap2* et *cap3*

Équipement	***Talker ID***	***Sentence ID***
192.168.0.1	NW, PH, SD, SP	TRO, MWD, VTG, DPT, DBT, VHW
192.168.0.2	RA, IO	TTM, OSD, RSD, TXT
192.168.0.3	PH, AI, GP, NA, NA, PH	KS, VDM, GGA, VHW, VTG, TRO, RMC

au multiplexeur, et non au capteur analysé. Suite à nos travaux sur les *talkers ids* et *sentence ids*, nous avons également émis l'hypothèse qu'il était possible, à partir des fichiers de capture, de reconstituer le réseau INS à l'origine du trafic.

À partir de nouveaux fichiers de capture, nous parvenons à modéliser l'architecture fonctionnelle du réseau NMEA sous-jacent (figure IV.35). Nous représentons les thématiques des phrases NMEA sous différentes couleurs : noir pour l'AIS, bleu pour les informations relatives au positionnement et à l'heure, orange pour les informations propriétaires, jaune pour celles de navigation, rouge pour le radar, vert pour les informations liées à l'environnement.

Cette modélisation permet d'émettre plusieurs hypothèses. Tout d'abord, certains équi-

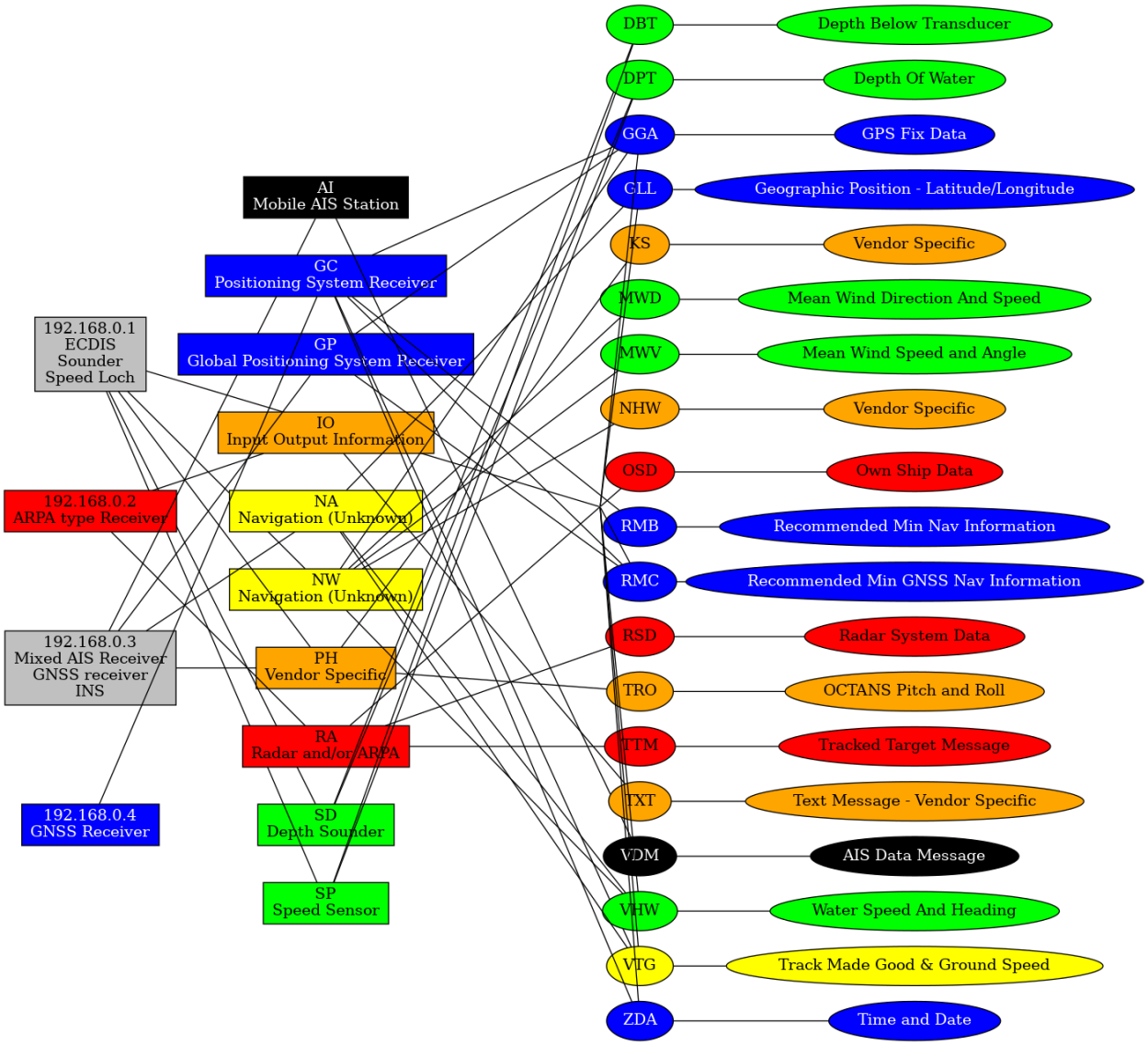

FIGURE IV.35 : Modélisation du réseau NMEA et des *talkers IDs* et *sentences IDs* à partir de fichiers de capture (source : archives personnelles).

pements à origine des phrases NMEA (les quatre adresses IP à gauche du schéma) sont directement raccordés sur le réseau. C'est le cas de l'équipement 192.168.0.2, qui peut être identifié comme un radar de type ARPA. Ce radar émet, en plus des phrases de type RATTM et RARSD, des phrases propriétaires (IOTXT) qui pourraient permettre de l'identifier avec plus de précision (marque, voire type) mais, d'après les références trouvées en source ouverte, il existe plusieurs fabricants dont les radars émettent ce type de phrases. Le raccordement direct sur le réseau peut également être confirmé pour l'équipement 192.168.0.4, qui présente toutes les caractéristiques d'un récepteur GNSS : il s'agit probablement du second

récepteur GPS du navire en question, pour lequel le *talker id* a été modifié de GP en GC pour permettre de séparer l'origine des positions entre les deux récepteurs.

Ensuite, les équipements disposant des adresses IP 192.168.0.1 et 192.168.0.3 sont, quant à eux, à l'origine de multiples phrases de *talkers* différents. Il s'agit donc, très probablement, de multiplexeurs ou de logiciels ou matériels qui assurent ces fonctions. Pour l'équipement 192.168.0.1, il cumule des fonctions d'ECDIS et reçoit puis ré-émet des informations liées aux paramètres environnementaux (vitesse, hauteur d'eau). Pour l'équipement 192.168.0.3, il s'agit probablement d'un récepteur AIS couplé avec un récepteur GNSS et d'une centrale inertielle ou de capteurs de roulis/tangage.

Le réseau peut alors être modélisé comme à la figure IV.36.

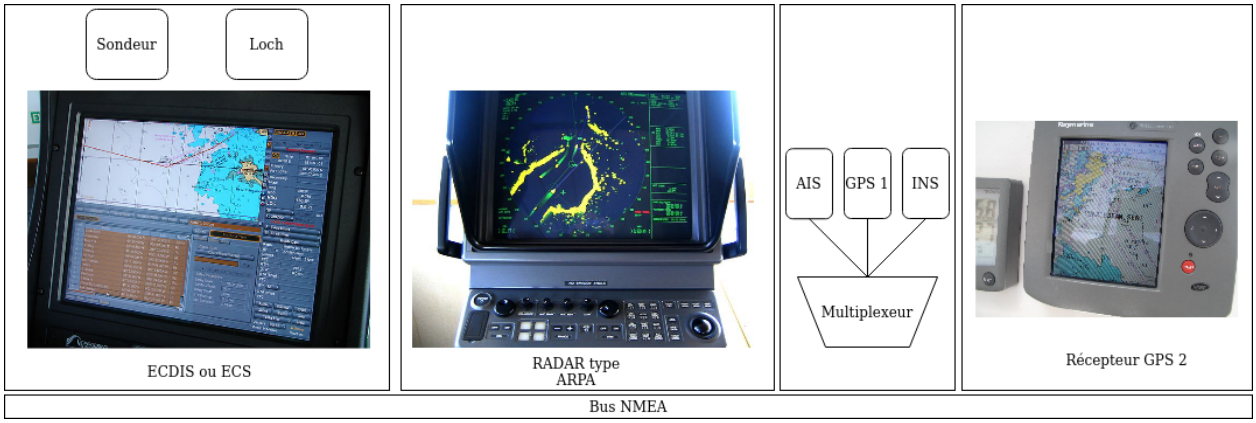

FIGURE IV.36 : Modélisation de l'architecture globale du réseau NMEA à partir des fichiers *cap1*, *cap2* et *cap3* (sources : ECDIS : Wikimedia Commons, image non modifiée, auteur : Hervé Cozanet, licence : CC BY-SA 3.0, RADAR : Wikimedia Commons, image non modifiée, auteur : Clipper, licence : CC BY-SA 2.5, GPS : Wikimedia Commons, image non modifiée, auteur : Fairley, licence : CC BY-SA 2.0).

IV.4.5 Résultats

Pour détecter l'exploitation d'une vulnérabilité intrinsèque (injection de trames leurrées), la détection d'anomalies sur le réseau de transport est généralement réalisée par des systèmes classiques de détection d'intrusion. Étant données les conséquences importantes et l'occurrence d'incidents récents de leurrage et de brouillage GNSS, nous avons choisi de concentrer nos travaux sur la détection d'anomalies sur la charge utile NMEA 0183 de données GNSS (vulnérabilités extrinsèques). Nous avons mis en œuvre, au sein du *Naval Cyber Range*, un outil de leurrage GPS et l'avons paramétré pour qu'il puisse être efficace sur un

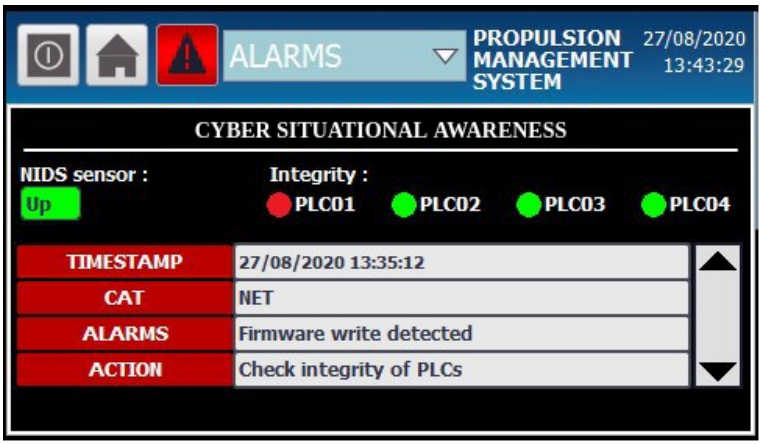

FIGURE IV.37 : Partage d'information et amélioration de la *Maritime Cyber Situational Awareness* par la mise en œuvre d'un panneau de contrôle et d'alerte de l'opérateur d'un système industriel sur le *Naval Cyber Range* (source : archives personnelles).

équipement GPS maritime. Ces opérations de leurrage ont été réalisées en laboratoire, à très faible puissance, en utilisant un raccordement direct entre l'émetteur et le récepteur par le biais d'un câble coaxial et sans émission dans l'espace radiofréquence. Notre objectif final est que, à chaque leurrage, le capteur détecte les anomalies et en informe l'opérateur via l'ECS.

En effet, lorsque la détection d'anomalies est réalisée, il apparaît essentiel que l'opérateur de l'installation en soit informé en temps opportun, afin de réaliser les actions nécessaires pour faire cesser l'attaque et, si possible, qu'il soit aidé et soutenu dans ses actions de *situation resolution*. La détermination du *CoA* peut se baser sur la connaissance de l'attaquant (TTP) pour anticiper ses prochaines actions et concourir à la *situation projection*, mais elle également très dépendante du type de système d'information et des résiliences (techniques, organisationnelles) existantes. Ce sujet fait l'objet de plusieurs travaux de recherche, notamment dans le cadre du projet COCOA [9].

Dans le cadre de nos travaux sur notre plate-forme prototype, nous avons recherché la mise en œuvre d'une solution au niveau tactique, car elle s'avère généralement absente des équipements de terrain. C'est notamment le cas sur les systèmes OT, lorsque les informations de détection cyber remontent vers les SOC, mais ne sont pas partagées au niveau de l'exploitant, qui pourtant est souvent le plus à même de constater si la possible alarme cyber a pu avoir des conséquences cyber physiques. Le développement du prototype dans le cadre de nos travaux permet un apport concret au niveau tactique, en permettant la mise en place de panneaux de contrôle et d'alerte dédiés directement sur les systèmes industriels et les

9. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao#overview

Tableau IV.7 : Exemples de *Talker ID*, *Sentence ID* cyber et COA proposés dans le cadre du projet CARMEN

Talker	***Sentence***	**Description**	**COA proposé**
CY	AIJ	Cyber / AIS Jamming	*Strengthen visual surface awareness*
CY	AIS	Cyber / AIS Spoofing	*Strengthen visual surface awareness*
CY	GPJ	Cyber / GPS Jamming	*Use alternative positioning solutions*
CY	GPN	Cyber / GPS Nav Alert	*Check GPS nav information*
CY	GPS	Cyber / GPS Spoofing	*Use backup positioning solutions*
CY	GPT	Cyber / GPS Timing Alert	*Check GPS timing information*
CY	NET	Cyber / Network intrusion	*Check NMEA network integrity*
CY	WDG	Cyber / Watchdog	*Check cyber sensor function*

SIM. Ainsi, la figure IV.37 présente le panneau d'information mis en place sur les armoires des automates des systèmes industriels du *Naval Cyber Range* et qui permet à l'opérateur de visualiser rapidement l'état du capteur, l'intégrité des programmes des différents automates, mais aussi les alarmes détectées et les propositions de résolution.

Nous avons également travaillé au niveau du standard NMEA lui-même, afin de pouvoir partager les informations de détection du capteur cyber. Nous proposons ainsi une évolution du standard NMEA 0183 pour y inclure des informations liées à la cybersécurité dans le cadre d'un projet appelé *Cyber Situational AwaReness Made Easy for NMEA (CARMEN)*. Le concept repose sur la création d'un nouveau *talker* NMEA appelé CY, correspondant à la sonde de détection. Pour chaque évènement redouté du standard NMEA, nous avons ensuite créé un identifiant de *sentence* spécifique (*cf* tableau IV.7). À terme, le projet CARMEN inclura l'ensemble des évènements redoutés en fonction des capteurs et actionneurs présents sur un réseau NMEA et dont un capteur cyber pourrait vérifier la cohérence.

À titre d'exemple, dans le cas de la figure IV.38, nous exploitons une vulnérabilité intrinsèque du réseau NMEA qui permet d'intercepter des trames NMEA et d'en injecter de nouvelles afin de fausser l'affichage de la position sur l'ECS. Sur notre plate-forme prototype, en absence d'anomalie, et s'il fonctionne correctement, le capteur cyber envoie en permanence une trame d'indication de bon fonctionnement ($CYWDG). Cette information est relayée sur l'ECS qui indique un bon fonctionnement du capteur et l'absence d'anomalies. En cas de détection d'une anomalie sur le capteur (en cas de leurrage : non respect du déterminisme, adresse de l'émetteur inconnu, position incohérente par rapport à la cinématique, etc.), la

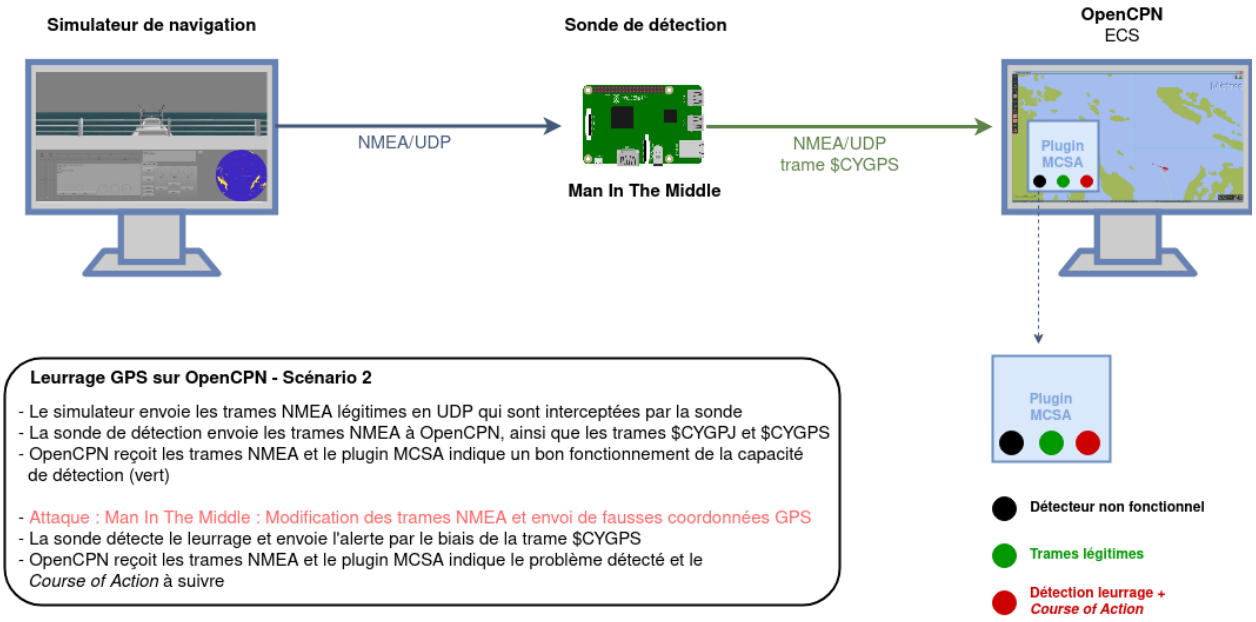

FIGURE IV.38 : Exploitation d'une vulnérabilité intrinsèque du protocole NMEA et circuit d'affichage vers l'ECS pour affichage du CoA approprié (source : Chaire de cyberdéfense des systèmes navals, reproduite avec l'aimable autorisation de l'auteur).

sonde émet une alerte de type $CYGPS et le composant additionnel présent sur l'ECS affiche une alerte (point rouge) et propose un moyen de contournement (*Course of Action*, par exemple : utiliser un moyen de positionnement alternatif).

Dans le cas de la figure IV.39, nous exploitons une vulnérabilité extrinsèque du réseau NMEA (leurrage du capteur GPS), qui permet d'injecter de mauvaises informations de position (ou de temps) afin de fausser l'affichage de la position ou le fonctionnement sur l'ECS. Lors de l'opération de leurrage, menée par l'émetteur *Software Defined Radio (SDR)*, le capteur détecte l'anomalie (en cas de leurrage : changement des informations liées à la constellation, position incohérente par rapport à la cinématique, variation forte du temps, etc.) et émet une alerte de type $CYGPS et le composant additionnel présent sur l'ECS affiche une alerte simplifiée (point rouge) et propose un moyen de contournement (*Course of Action*, par exemple : utiliser un moyen de positionnement alternatif).

Au niveau de l'ECS, en l'absence de leurrage GPS, le prototype CARMEN indique que le lien avec le capteur est fonctionnel et qu'aucun leurrage n'est détecté (Figure IV.40).

Nous réalisons ensuite un leurrage GPS avec un décalage de position important : le prototype CARMEN indique immédiatement la détection et propose un moyen alternatif (Figure IV.41). Le leurrage est volontairement important pour que le décalage de la position

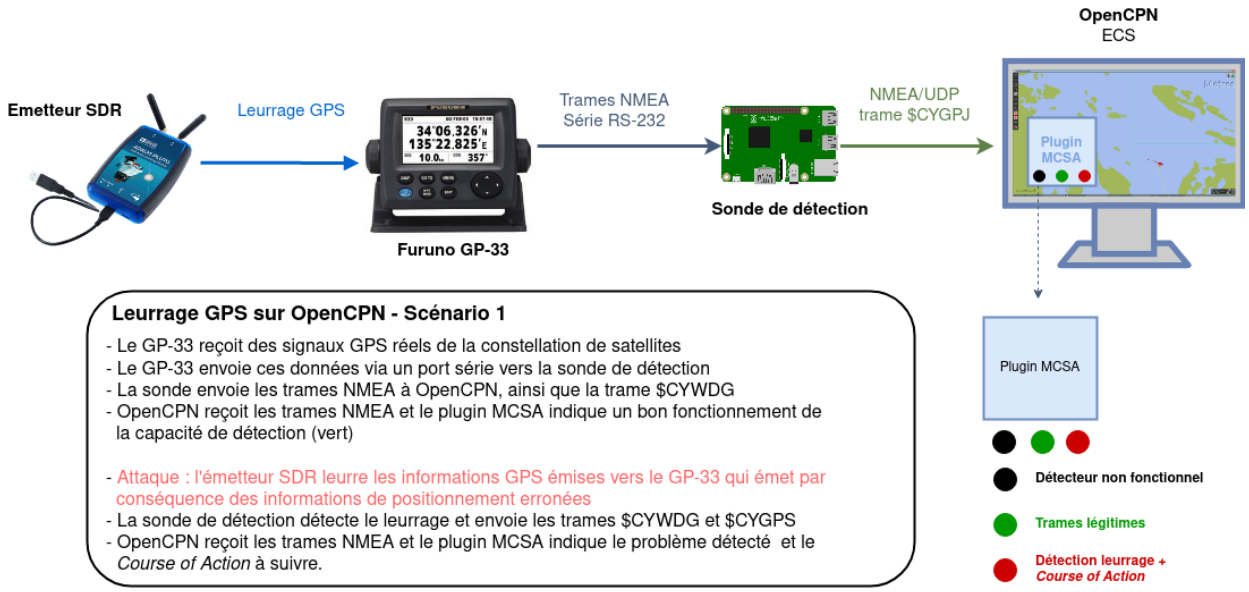

FIGURE IV.39 : Exploitation d'une vulnérabilité extrinsèque du réseau GPS et circuit d'affichage vers l'ECS pour affichage du CoA approprié (source : Chaire de cyberdéfense des systèmes navals, reproduite avec l'aimable autorisation de l'auteur).

FIGURE IV.40 : Présentation du composant additionnel CARMEN dans l'ECS en l'absence de leurrage (source : Chaire de cyberdéfense des systèmes navals, reproduite avec l'aimable autorisation de l'auteur).

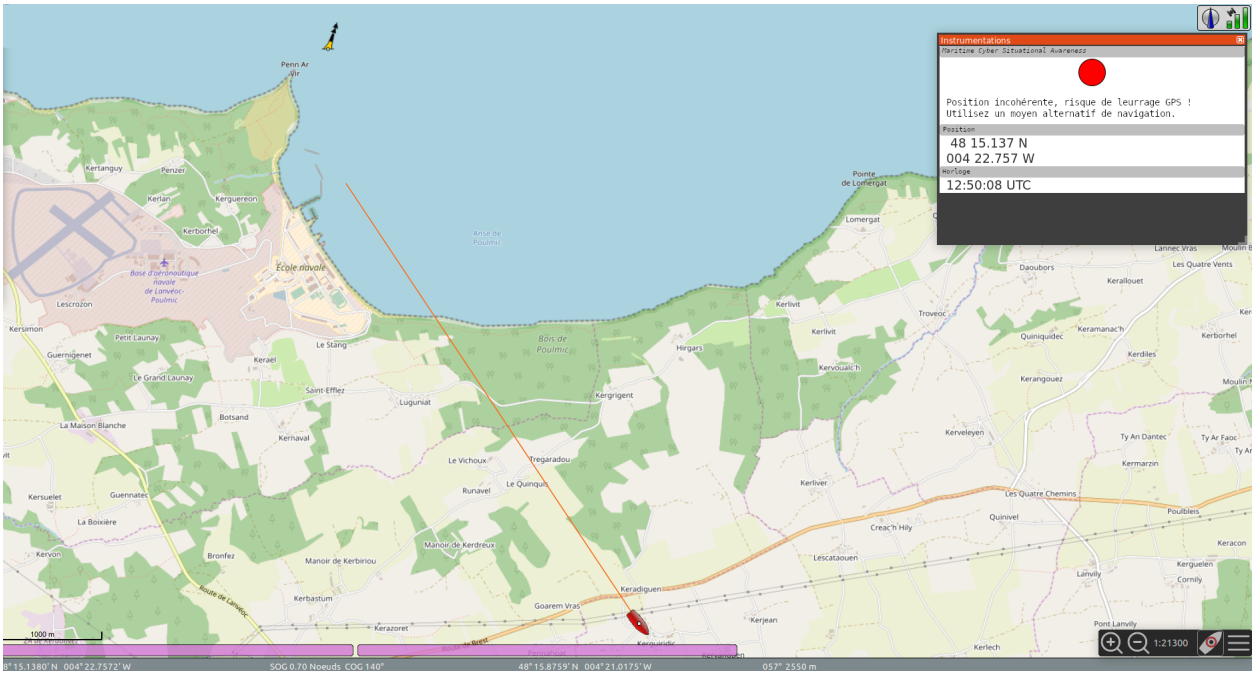

FIGURE IV.41 : Présentation du composant additionnel CARMEN dans l'ECS en présence de leurrage, avec affichage du CoA approprié (source : Chaire de cyberdéfense des systèmes navals, reproduite avec l'aimable autorisation de l'auteur).

soit particulièrement visible : la qualité de détection est, en réalité, beaucoup plus fine.

IV.5 Conclusion

Dans ce chapitre, nous avons traité les questions de recherche QR1 (architecture de collecte et modélisation), QR2 (analyse et représentation de données) et QR3 (détection d'anomalie sur un système d'information maritime). Nos expérimentations sur plate-forme prototype nous ont conduit à intégrer dans le *Naval Cyber Range* de l'École navale plusieurs composants essentiels, en termes de détection d'anomalies, de visualisation et de partage d'information sur des protocoles maritimes. Cette intégration a notamment été réalisée au travers d'une architecture applicative qui permet l'élaboration de la *Maritime Cyber Situational Awareness*.

Afin de valider nos travaux, nous avons proposé un ensemble de critères de mesure de qualité qui permettent d'assurer que l'établissement de la MCSA s'effectue avec un haut niveau de confiance dans les données collectées pour éviter toute mauvaise interprétation tout au long des phases de *perception*, *comprehension*, *projection* et *resolution*.

Par la suite, nous avons travaillé sur la plate-forme à la réalisation de tableaux de bord dynamiques et sur le code source d'un analyseur réseau et d'un NIDS, afin d'améliorer la précision des données qu'ils génèrent et des graphes qui en découlent. Le gain en précision permet de faciliter la compréhension de la situation et la prise de décision, tout en améliorant également la qualité de la cartographie des systèmes d'information maritimes.

Les apports de la *Maritime Cyber Situational Awareness* aux travaux d'analyse dynamique des risques (*Dynamic Risk Assessment*) ont ensuite été démontrés. L'utilisation de bases de données orientées graphe et l'ajout de données complémentaires issues de CSIRT ont permis de souligner la plus-value de ces outils pour les analystes de SOC : ces travaux, inconcevables sans une architecture adaptée au monde maritime, ont permis de réaliser un lien efficace entre toutes les phases de la MCSA, de la détection à la résolution pour les niveaux opératif et tactique.

Enfin, les travaux réalisés sur plate-forme expérimentale ont permis de démontrer la plus-value d'une architecture adaptée et performante de cyber-surveillance à des fins de détection d'anomalies sur des systèmes d'information maritime. Pour cela, les recherches ont essentiellement porté sur les caractéristiques et les vulnérabilités du standard NMEA 0183 et des systèmes de positionnement par satellite, notamment par la recherche de caractéristiques déterministes et d'attributs pertinents pour la détection d'anomalies par apprentissage automatique.

L'absence d'information de l'opérateur en cas d'anomalie cyber, fréquemment rencontrée sur les systèmes *Operational Technology*, a motivé le développement du projet CARMEN. Ce projet a permis de proposer une évolution du standard NMEA 0183 pour y inclure des échanges d'informations d'intérêt cyber entre un capteur de détection et un ECS ou un ECDIS. Lors d'une phase de prototypage sur la plate-forme du *Naval Cyber Range*, la détection d'anomalies, la compréhension de l'évènement et sa résolution ont pu faire l'objet d'une instrumentation sous forme de prototype et présentées de manière simple, mais complète, à l'opérateur sur les systèmes industriels et de navigation.

En faisant remonter l'information de *Maritime Cyber Situational Awareness* sur l'outil de *Maritime Situational Awareness* constitué par l'ECS ou l'ECDIS, l'intérêt de la fusion entre SA est démontré. L'état de connaissance global proposé à l'officier de quart et au capitaine du navire lui permet d'établir un lien entre anomalie cyber et de situation surface, tout en l'aidant à prendre la décision la plus appropriée.

Chapitre V

Conclusion générale et perspectives

V.1 Problématique

Les navires modernes peuvent être considérés comme des systèmes de systèmes complexes, de plus en plus numérisés et qui disposent de systèmes IT, OT et cyber physiques essentiels à la conduite de leur mission. Ils exploitent des matériels, logiciels et protocoles faillibles qui peuvent les fragiliser et les mettre à la portée d'une compromission par un attaquant motivé. La perception et la compréhension d'un évènement cyber, sa projection dans le temps et sa résolution, qui sont des domaines de recherche actuels, se complexifient d'autant plus lorsqu'on les applique au contexte maritime et à un objet mobile comme un navire.

Nous avons proposé d'adapter et d'enrichir un concept existant, appelé *situational awareness*, à la cybersécurité du domaine maritime en le déclinant sous l'appellation de *Maritime Cyber Situational Awareness*. L'objectif de cette démarche était d'appliquer une méthodologie suivie avec succès dans d'autres domaines, notamment en aéronautique, à la cybersécurité maritime, non pas en utilisant directement les outils comme les *Head-Up Display*, mais plutôt pour la pertinence de ses principes fondateurs. L'application directe de ce concept au monde maritime s'avère difficile, car les contraintes spécifiques au milieu ne permettent pas de le surveiller comme un système d'information IT classique.

Nous avons ainsi identifié trois questions de recherche : l'architecture de collecte et la modélisation (QR1), l'analyse et la représentation des données (QR2) et la détection d'anomalies dans un contexte maritime (QR3).

V.2 Travaux réalisés

Au cours de nos travaux, nous avons voulu démontrer que, pour répondre de manière appropriée à la problématique de la détection d'anomalies dans le monde maritime, il convenait en premier lieu de connaître et comprendre le secteur dans son ensemble. C'est la raison pour laquelle nous avons commencé par réaliser une analyse sectorielle maritime globale, et plus particulièrement des navires, de leurs contraintes et de leurs vulnérabilités systémiques en termes de cybersécurité. C'est fort de ces constats que le concept de *Maritime Cyber Situational Awareness* a ensuite été élaboré, en adaptant et déclinant le principe de *situational awareness* déjà employé dans le monde militaire.

Par la suite, nos travaux sur la QR1 nous ont amené à définir l'architecture globale potentielle qui pourrait s'avérer efficace pour assurer la cybersurveillance d'un navire et d'une flotte de navires civils, tant pour la partie embarquée que pour la partie terrestre. Nous avons démontré que cette architecture est réalisable et peut s'avérer qualitative, à condition qu'elle soit adaptée aux particularités du milieu maritime. Afin de valider le niveau de qualité atteint, des critères précis ont été définis puis mis en œuvre sur prototype. Il ont permis de démontrer l'efficacité de l'architecture, y compris dans le cas de contraintes particulières comme la dégradation du réseau support.

L'analyse et la visualisation des données demeurent un enjeu de recherche important pour la cybersécurité, dans un contexte de données hétérogènes et de volume important. Pour répondre à la QR2, des outils modernes et avancés ont été choisis, comme les bases de données graphes et les technologies de traitement en masse des données, afin d'apporter des réponses concrètes et rapides aux questions qui se posent en termes de cybersécurité sur des systèmes de systèmes complexes et interconnectés. Nous avons également contribué à l'amélioration de deux outils importants pour l'analyse et la visualisation des données, à savoir un capteur de détection d'intrusion et un outil d'analyse de trames réseau.

Pour répondre à la QR3, les travaux sur le standard NMEA et notamment le projet CARMEN ont permis de mettre en avant les particularités et les vulnérabilités du standard. Face à l'augmentation du nombre de cas de brouillage et de leurrage GNSS, la recherche se heurte à un nombre de jeux de données insuffisant. Un prototype a donc été élaboré afin de générer les jeux de données nécessaires aux travaux de recherche sur la détection d'anomalies sur les informations de position, de navigation et de temps essentielles pour un navire. Pour faire suite à la problématique soulevée par cette question de recherche, les travaux se sont axés sur le partage de l'information vers les systèmes surveillés, qui fait régulièrement défaut.

Ainsi, l'expérimentation CARMEN sur un bus regroupant GNSS et ECS sur le *Naval Cyber Range* a permis d'afficher les informations de détection directement au niveau de l'Interface Homme Machine (IHM) de l'ECS, dans un format compréhensible par l'utilisateur, apportant ainsi une preuve de concept de la fusion de la *Maritime Cyber Situational Awareness* et de la *Maritime Situational Awareness*.

Enfin, au-delà des apports pour le monde maritime, les travaux sur le *Naval Cyber Range* ont doté l'École navale et, plus largement, la Marine, d'un outil réaliste et, à l'heure actuelle, toujours unique en Europe qui ouvre de nombreuses perspectives de recherche en détection d'anomalies, mais aussi en protection des systèmes maritimes.

V.3 Discussion

Le concept de *Maritime Cyber Situational Awareness* permet de répondre en grande partie aux problématiques de cybersécurité évoquées pour le secteur. Il comporte, cependant, des limitations. Dans cette section, nous avons la volonté d'engager une discussion et une réflexion ouvertes sur les limitations de nos travaux.

Tout d'abord, le parti pris de réaliser une recherche plutôt holistique du secteur doit être expliqué. Lors de la réalisation de l'état de l'art, il a été constaté que le nombre de références scientifiques relatives à la cybersécurité maritime était limité, notamment en ce qui concerne l'analyse des causes systémiques des vulnérabilités des systèmes d'information maritimes : y consacrer une partie de nos travaux nous a donc semblé nécessaire.

Ensuite, la qualité de la cybersurveillance repose essentiellement sur des capteurs. En l'état actuel de la recherche et surtout des solutions logicielles proposées, le choix reste relativement contraint aux outils de détection par signatures ou utilisant une approche comportementale. Les deux solutions présentent chacune leurs défauts et limitations en termes de qualité de détection. Plutôt que de réaliser une nouvelle étude sur les performances ou les lacunes de l'un ou de l'autre, notre approche d'utiliser des capteurs réseaux ou hôtes avait surtout comme objectifs de contribuer, en plus de la détection d'anomalies, à l'amélioration de la connaissance des systèmes (KU), souvent trop lacunaire dans le monde maritime.

L'architecture que nous avons retenue et expérimentée, notamment sur la partie partage d'information, s'est focalisée sur le niveau tactique. Ce choix s'explique par le fait que le partage au niveau tactique s'avère probablement le plus efficace en termes de réaction et de

corrélation sur un système cyber physique, mais aussi parce que le prototype utilisé sur le *Naval Cyber Range* est de niveau tactique. De nombreux travaux restent cependant à mener au niveau « haut » même si, bien souvent, ils peuvent dépasser le strict cadre maritime (remontée vers une instance nationale de cybersécurité, par exemple).

Les critères de qualité retenus et mesurés lors de nos travaux sont particulièrement liés au *Naval Cyber Range* et n'ont pas la volonté d'être exhaustifs ou strictement représentatifs d'une réalité de terrain. Il manque, notamment, la représentation de navires de types différents aux systèmes d'information spécifiques, ou encore une flotte complète. Cependant, cette architecture générique nous a permis à plusieurs reprises de lever des anomalies ou des doutes sur le fonctionnement de certains capteurs, sur leur mise à jour, ainsi que sur le fonctionnement des réseaux supports. Ce modèle d'architecture générique présente donc un intérêt à être poursuivi. D'autres critères ou sous-critères de mesure de qualité pourraient probablement être ajoutés ultérieurement.

De nombreux travaux de recherche ont déjà été menés sur les enjeux de la visualisation et de son utilisation à des fins de détection d'anomalies. C'est la raison pour laquelle nous avons souhaité concentrer nos efforts dans les directions qui nous ont semblé les plus pertinentes et réalistes. Cela a été le cas pour les graphes à coordonnées parallèles, mais aussi et surtout pour l'évaluation dynamique des risques. Ce concept, parfois difficile à modéliser, prend tout son sens dans le contexte maritime, notamment grâce à l'utilisation de bases de données graphes qui facilitent grandement sa mise en œuvre pour le rendre facilement réalisable.

Les travaux de détection d'anomalie sur le standard NMEA 0183 ont permis de faire ressortir plusieurs attributs déterministes qui pourront être utilisés à des fins de détection d'anomalie à base de techniques d'apprentissage automatique. En raison du volume et de l'hétérogénéité des données et capteurs, mais aussi parce que le sujet divergeait en partie du thème initial de la thèse et nécessiterait lui-même une thèse à part entière, toutes les pistes n'ont pu être explorées, notamment en ce qui concerne le caractère déterministe de certaines valeurs.

Enfin, les travaux réalisés dans les sections IV.4.5 et IV.5 dans le cadre du projet CARMEN et notamment les propositions de *Course of Action*, gagneraient à être enrichis. Il convient cependant de rappeler que la visualisation sur l'ECS, l'ECDIS ou sur le système industriel s'adresse avant tout à un opérateur non expert, l'expert ayant plutôt recours aux informations remontées, par exemple, dans le LE et analysées par le SIEM ou une base de données orientée graphes.

V.4 Perspectives

À la figure V.1, nous proposons un certain nombre de perspectives de recherche et de valorisation de nos travaux sur le concept de *Maritime Cyber Situational Awareness*, sur les données, le modèle en lui-même ou encore l'architecture. Si certaines ont d'ores et déjà été prises en compte au sein de la chaire, où plusieurs thèses à venir pourront bénéficier des axes de recherche et de valorisation identifiés, d'autres restent à initier.

V.4.1 Données

Parmi les points que nous identifions, évoquons tout d'abord la capture de données en masse et les capacités d'analyse associées, qui doivent permettre d'élargir l'emploi des solutions évoquées et de valoriser les données à d'autres fins que strictement cyber : on peut penser à la détection d'anomalie matérielle sur les systèmes cyber physiques (D1) ou à des usages à des fins de détection opérationnelle (D2).

Les travaux relatifs à la qualité des données issues des capteurs peuvent être poursuivis : la modélisation et la création du *Naval Cyber Range* permettent dorénavant de disposer d'une quantité importante de données réalistes, qui gagneront à être valorisées et mises à disposition du monde de la recherche et de l'enseignement (D3).

Les démonstrations réalisées sur le thème de l'évaluation dynamique des risques (*Dynamic Risk Assessement*) sont annonciatrices de recherches d'intérêt. La MCSA et l'architecture mise en œuvre permettent désormais d'aboutir à des résultats pertinents. Il conviendra de poursuivre les expérimentations afin de valider la plus-value de la DRA dans les contextes multiples et complexes du monde maritime (D4).

Le suivi chronologique de l'émission des trames NMEA sur un réseau en grande partie déterministe comme un INS pourrait faire l'objet d'une analyse intéressante en utilisant des techniques de traitement du signal ou de *Cybernetic-DNA*, afin d'identifier des motifs de répartition dans le temps des *sentences* et *talker* IDs et de renforcer la détection d'anomalies par une approche originale. La détection d'anomalies sur la charge utile et notamment sur les données dynamiques (position et navigation), mais aussi sur le temps, nécessitera des travaux complémentaires (D5).

Les travaux de fusion et la corrélation des données de la MCSA avec les autres SA (sécurité, sûreté...) mériteront d'être poursuivis. Cette fusion de données issues de différents

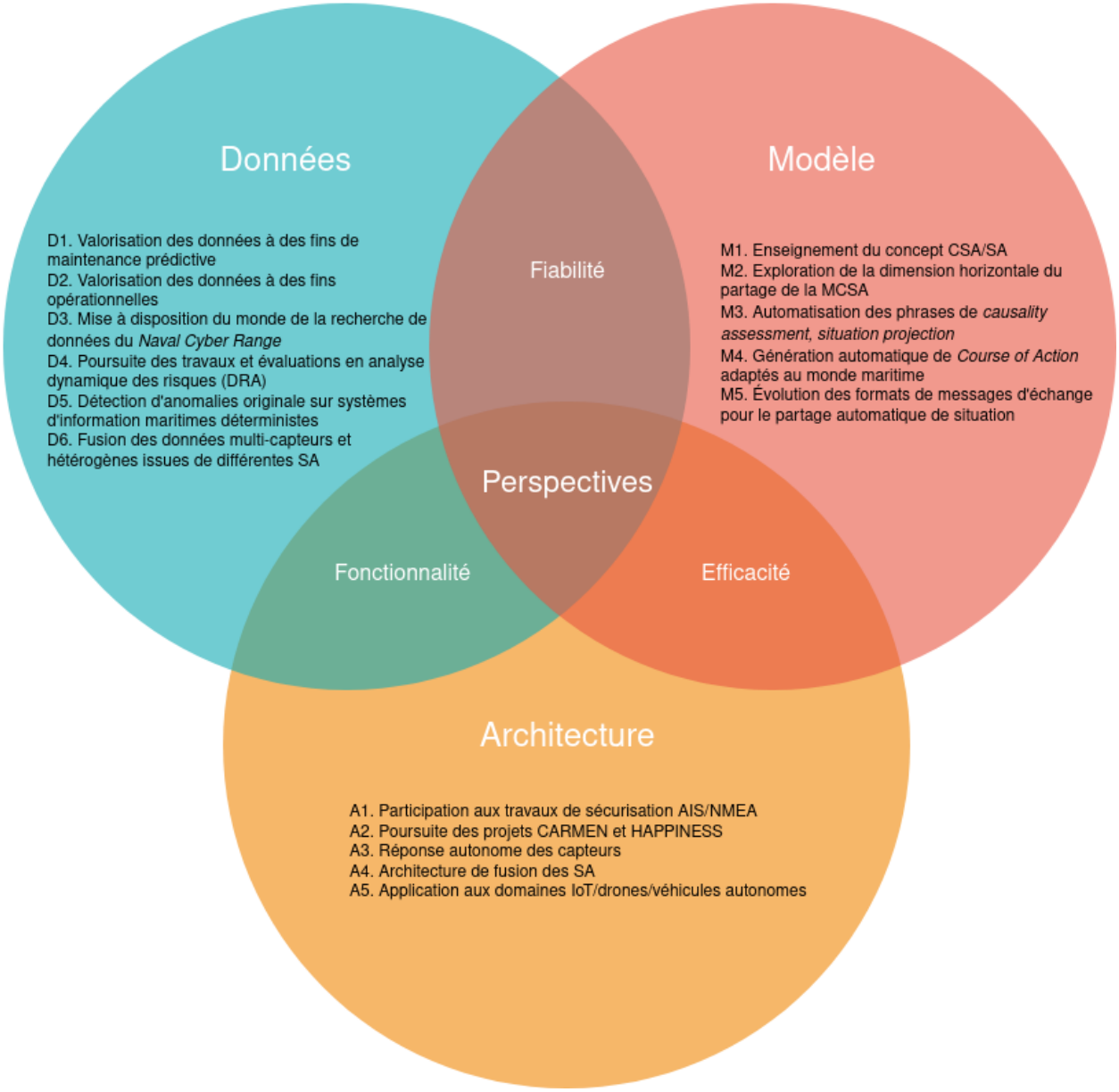

FIGURE V.1 : Perspectives de recherche et de valorisation du concept de *Maritime Cyber Situational Awareness* (source : archives personnelles).

capteurs permettra encore d'améliorer la finesse de détection. Ainsi, tout en limitant le nombre de faux positifs, le couplage de données issues de capteurs radiofréquence (RF) et cyber permettra d'obtenir des données d'un haut niveau de complétude et de précision, face à une menace prégnante sur le spectre radioélectrique. La même logique pourra être suivie pour corréler alertes issues d'un capteur cyber (*eg* : détection d'une anomalie réseau) avec l'évolution incohérente d'un capteur cyber physique ou d'un capteur radioélectrique, par exemple par l'utilisation d'un mécanisme de *scoring*, afin de de pondérer l'ensemble des vecteurs de détection au sein d'un indicateur unique (D6).

V.4.2 Modèle

Le concept de CSA demeure relativement méconnu de la communauté cyber, notamment francophone. Sans nécessairement rentrer dans le détail et les subtilités du principe, son enseignement pourrait être envisagé dans le cadre de certaines formations. En effet, la démarche intellectuelle qu'il oblige à réaliser et sa progressivité nous semblent pertinentes pour tout analyste en cyberdéfense (M1).

Les niveaux d'abstraction de la MCSA et l'utilisation horizontale ou verticale de la connaissance figurent probablement parmi les points les plus importants à retenir pour l'avenir : la cybersécurité sera toujours mal perçue par les opérateurs et autorités si elle diverge du fonctionnement classique de l'organisation par ses processus ou ses systèmes d'information dédiés : elle doit apprendre à mieux s'intégrer dans les opérations et partager, avec l'abstraction requise, ses analyses au plus près des opérateurs et des décideurs (M2).

Les travaux liés à la recherche de causalité (*causality assessment*), de *situation projection* et, surtout, de *situation resolution* gagneront à se poursuivre plus finement en mettant en perspective d'une part, les TTP des attaquants et, d'autre part, des modèles comme celui du MITRE. Cela permettrait d'envisager la génération automatique de scénarios de réponse à incident adaptés au monde maritime (*Course of Action*) et la poursuite des travaux sur la perception de l'attaquant et de ses intentions (M3, M4).

Au niveau haut, le partage de situation cyber pourra permettre l'évolution de standards comme ADatP-3[1] pour faciliter la diffusion de renseignements et d'incidents semi-automatisés entre navires, et entre navires et centres à terre, y compris entre navires de

1. L'ADatP-3, *Allied Data Processing Publication number 3*, est un standard OTAN de rédaction de messages opérationnels. Il permet de fixer les modèles de messages formels échangés entre les forces de différents pays dans le cadre d'une opération de l'OTAN.

pavillons différents. Ce point s'avèrera particulièrement pertinent pour les flottes de navire autonomes (contrôles d'intégrité et alertes réciproques en cas d'attaque pour assurer la résilience de la flotte et l'accomplissement de la mission) (M5).

V.4.3 Architecture

La poursuite du projet CARMEN pour la détection d'anomalies sur les réseaux de positionnement, de navigation et de temps et le partage de situation tactique cyber se poursuivra en parallèle d'un nouveau projet de recherche de l'École navale, appelé *Holistic APProach of Integrated Navigation Equipment for cyberSecurity at Sea (HAPPINESS)*. L'objectif de ce dernier projet est de créer un caisson étanche embarqué équipé de différents capteurs et d'antennes AIS, GPS et 4G, permettant de transmettre en temps réel des informations AIS et GPS au format NMEA de positions côtières vers la terre, afin de les injecter sur le *Naval Cyber Range*, mais aussi à des fins de production de jeux de données complémentaires et de captation de ces informations au format radioélectrique. Ces travaux alimenteront les évolutions et adaptations des standards AIS et NMEA devenues indispensables pour corriger, en profondeur, les vulnérabilités par conception dont ils sont l'objet. Les données issues de ces deux standards n'étant pas nécessairement fiables, leur corrélation avec d'autres sources de données (imagerie satellite, par exemple) mériterait d'être approfondie pour augmenter le niveau de confiance (A1, A2).

Sur la base des travaux réalisés, la boucle d'information de la détection vers l'opérateur à bord du navire paraît réalisable. Il semble donc pertinent de poursuivre les travaux sur les capacités de réponse autonome des capteurs (par exemple : bascule automatique sur un système intègre en cas de détection) et sur l'adaptation de l'architecture pour permettre la fusion des SA. L'emploi des capteurs à des fins d'automatisation de *Cyber Battle Damage Assessment* offre des perspectives intéressantes en termes de recherche sur l'évaluation des dommages et la résilience (A3, A4).

Pour terminer, certaines des contraintes évoquées pour le monde maritime s'avèrent très proches de celles rencontrées dans le contexte des véhicules autonomes, des drones et de l'Internet des objets. L'ouverture d'une dernière perspective vers l'application de ces travaux dans ces domaines contraints nous apparaît donc pertinente (A5).

Liste de publications

1. O. Jacq, X. Boudvin, D. Brosset, Y. Kermarrec, J. Simonin, *Detecting and hunting cyberthreats in a maritime environment : specification and experimentation of a maritime cybersecurity operations centre*, 2018 2nd Cyber Security in Networking Conference (CSNet), 1-8
2. O. Jacq, D. Brosset, J. Simonin, Y. Kermarrec, *Use of Suricata, ElasticStack, Neo4j and Linkurious for network defence*, Suricon 2019
3. O. Jacq, D. Brosset, Y. Kermarrec, J. Simonin, *Cyber attacks real time detection : towards a Cyber Situational Awareness for naval systems*, 2019 International Conference on Cyber Situational Awareness, Data Analytics
4. O. Jacq, PM Laso, D. Brosset, J. Simonin, Y. Kermarrec, MA Giraud, *Maritime Cyber Situational Awareness Elaboration for Unmanned Vehicles*, Maritime Situational Awareness Workshop, 2019

Bibliographie

[A+02] National Marine Electronics Association et al. *NMEA 0183–Standard for interfacing marine electronic devices*. NMEA, 2002.

[ABPG20] Andrej Androjna, Tanja Brcko, Ivica Pavic, and Harm Greidanus. Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, 8(10) :776, 2020.

[Al-16] Al-Mohannadi Hamad and Mirza, Qublai and Namanya, Anitta and Awan, Irfan and Cullen, Andrea and Disso, Jules. Cyber-attack modeling analysis techniques : An overview. In *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pages 69–76. IEEE, 2016.

[All] International Maritime Electronics Alliance. An IP/Ethernet Interface Standard for Marine Electronic Devices. https://www.nmea.org/Assets/onenet%202017%20update.pdf. Consulté le 20/05/2018.

[Bar10] Barford, Paul and Dacier, Marc and Dietterich, Thomas G and Fredrikson, Matt and Giffin, Jon and Jajodia, Sushil and Jha, Somesh and Li, Jason and Liu, Peng and Ning, Peng and others. Cyber sa : Situational awareness for cyber defense. In *Cyber situational awareness*, pages 3–13. Springer, 2010.

[Bea17] Beaumont, Peter and Wolthusen, S. Cyber-risks in maritime container ports : An analysis of threats and simulation of impacts. *ISG MSc Information Security thesis series 2017*, 2017.

[Ben18] Bruno Bender. Rapport internet "cybersécurité & domaine maritime", 2018.

[BG17] Ive Botunac and Marijan Gržan. Analysis of software threats to the automatic identification system. *Brodogradnja : Teorija i praksa brodogradnje i pomorske tehnike*, 68(1) :97–105, 2017.

[Bla18] Félix Blanc. Géopolitique des câbles : une vision sous-marine de l'internet. *Les carnets du centre d'analyse, de prévision et de stratégie*, 2018.

[Bol19] Bolbot, Victor and Theotokatos, Gerasimos and Boulougouris, Evangelos and Vassalos, Dracos. Safety related cyber-attacks identification and assessment for autonomous inland ships. In *International Seminar on Safety and Security of Autonomous Vessels (ISSAV)*, 2019.

[BPW14] Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit. A security evaluation of ais automated identification system. In *Proceedings of the 30th annual computer security applications conference*, pages 436–445, 2014.

[Bra11] Branlat, Matthieu and Morison, Alexander and Woods, DD. Challenges in managing uncertainty during cyber events : Lessons from the staged-world study of a large-scale adversarial cyber security exercise. In *Human Systems Integration Symposium*, pages 10–25, 2011.

[Bri19] Jean-Jacques Bridey. La France, puissance maritime. *Revue Défense Nationale*, (8) :7–11, 2019.

[BSG+20] Paul M Berges, Basavesh Ammanaghatta Shivakumar, Timothy Graziano, Ryan Gerdes, and Z Berkay Celik. On the feasibility of exploiting traffic collision avoidance system vulnerabilities. *arXiv preprint arXiv :2006.14679*, 2020.

[Bur14] Ryan Burton. Cybersécurité et marétique, un enjeu européen ? *Centre d'études stratégiques de la marine*, 2014. Consulté le 20/05/2018.

[Bur16] Joe Burton. Cyber attacks and maritime situational awareness evidence from Japan and Taiwan. In *2016 International Conference on Cyber Situational Awareness, Data analytics and Assessment (CyberSA)*, pages 1–4. IEEE, 2016.

[BUTN18] Hayretdin Bahşi, Chibuzor Joseph Udokwu, Unal Tatar, and Alexander Norta. Impact assessment of cyber actions on missions or business processes : A systematic literature review. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, page 11. Academic Conferences and publishing limited, 2018.

[Car13] Cardenas, Alvaro A and Manadhata, Pratyusa K and Rajan, Sreeranga P. Big data analytics for security. *IEEE Security & Privacy*, 11(6) :74–76, 2013.

[Cen] Royal Caribbean Press Center. Symphony of the seas fact sheet. https://www.royalcaribbeanpresscenter.com/fact-sheet/31/symphony-of-the-seas/. Consulté le 20/05/2018.

[Chi14] Chifflier, Pierre and Fontaine, Arnaud. Architecture système sécurisée de sonde IDS réseau. *Computer & Electronics Security Applications Rendez-vous (C&ESAR)*, 2014.

[CIC] CICDE. Glossaire interarmées de terminologie opérationelle (GIATO).

[Cim11] Cimpean, Dan and Meire, Johan and Bouckaert, Vincent and Vande Casteele, Stijn and Pelle, Aurore and Hellebooge, Luc. Analysis of cyber security aspects in the maritime sector. Technical report, ENISA, 2011.

[Cla16] Bryan Clark. Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists*, 72(4) :234–237, 2016.

[Com12] North Atlantic Military Commitee. Mc 0422/4 NATO military policy on information operations, July 2012.

[Cos18] Benjamin Coste. *Détection contextuelle de cyberattaques par gestion de confiance à bord d'un navire.* Thèse de doctorat, 2018.

[CTSdG12] Gabriel D Cavalcante, Sebastien Tricaud, Cleber P Souza, and Paulo Licio de Geus. Interactive analysis of computer scenarios through parallel coordinates graphics. In *International Conference on Computational Science and Its Applications*, pages 314–325. Springer, 2012.

[da19] Ministère des armées. Droit international appliqué aux opérations dans le cyberespace. *Droit international appliqué aux opérations dans le cyberespace*, 2019. Consulté le 11/09/2019.

[Das14] Das, Niva and Sarkar, Tanmoy. Survey on host and network based intrusion detection system. *International Journal of Advanced Networking and Applications*, 6(2) :2266, 2014.

[Dia14] Diallo, David and Feuillet, Mathieu. Détection d'intrusion dans les systèmes industriels : Suricata et le cas de Modbus. *C&ESAR2014.(cf. p 44)*, 2014.

[DiR15] DiRenzo, Joseph and Goward, Dana A and Roberts, Fred S. The little-known challenge of maritime cyber security. In *Information, Intelligence, Systems and Applications (IISA), 2015 6th International Conference on*, pages 1–5. IEEE, 2015.

[dllea13] Direction de l'information légale et administrative. Livre blanc défense et sécurité nationale, 2013, 2013.

[dS16] Compagnie Européenne d'Intelligence Stratégique. Impacts sur l'économie française de la fermeture d'un ou plusieurs détroits maritimes majeurs. *Étude prospective et stratégique*, 2016.

[Dut13] Dutt, Varun and Ahn, Young-Suk and Gonzalez, Cleotilde. Cyber situation awareness : modeling detection of cyber attacks with instance-based learning theory. *Human Factors*, 55(3) :605–618, 2013.

[End95] Mica R Endsley. Toward a theory of situation awareness in dynamic systems. In *Toward a theory of situation awareness in dynamic systems*, volume 37, pages 32–64. SAGE Publications Sage CA : Los Angeles, CA, 1995.

[Fer97] Jacques Ferber. Les systèmes multi-agents : un aperçu général. *Techniques et sciences informatiques*, 16(8), 1997.

[Fit15] Fitton, Oliver and Prince, Daniel and Germond, Basil and Lacy, Mark. The future of maritime cyber security, 2015.

[For13] Ford, Gary and McMahon, Chris and Rowley, Chris. Naval surface ship in-service information exploitation. *Procedia CIRP*, 11 :92–98, 2013.

[Foy05] Foyle, David C and Andre, Anthony D and Hooey, Becky L. Situation awareness in an augmented reality cockpit : Design, viewpoints and cognitive glue. In *Proceedings of the 11th International Conference on Human Computer Interaction*, volume 1, pages 3–9, 2005.

[Fra14] Franke, Ulrik and Brynielsson, Joel. Cyber situational awareness–a systematic review of the literature. *Computers & Security*, 46 :18–31, 2014.

[Gar18] Phani Kumar Garimella. It-ot integration challenges in utilities. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, pages 199–204. IEEE, 2018.

[GGDM+18] G Gonzalez-Granadillo, Samuel Dubus, Alexander Motzek, Joaquin Garcia-Alfaro, Ender Alvarez, Matteo Merialdo, Serge Papillon, and Hervé Debar. Dynamic risk management response system to handle cyber threats. *Future Generation Computer Systems*, 83 :535–552, 2018.

[Goe15] Goetz, Pierre and Cahuzac-Soave, Olivia. Impact de la numérisation sur l'exercice du commandement, 2015.

[HBB+20] Hanan Hindy, David Brosset, Ethan Bayne, Amar Seeam, Christos Tachtatzis, Robert Atkinson, and Xavier Bellekens. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. *IEEE Access*, 2020.

[Hum15] Christopher Humphries. *User-centred security event visualisation.* Thèse de doctorat, Rennes 1, 2015.

[Ins] Marine Insight. 10 world's biggest container ships in 2017. https://www.marineinsight.com/know-more/10-worlds-biggest-container-ships-2017/. Consulté le 20/05/2018.

[Jac] Olivier Jacq. Les incidents (connus)... https://cybermaretique.fr/les-incidents-connus/. Consulté le 11/09/2019.

[Jac18] Jacq, Olivier and Boudvin, Xavier and Brosset, David and Kermarrec, Yvon and Simonin, Jacques. Detecting and hunting cyberthreats in a maritime environment : Specification and experimentation of a maritime cybersecurity operations centre. In *2018 2nd Cyber Security in Networking Conference (CSNet)*, pages 1–8. IEEE, 2018.

[Jac19a] Jacq, Olivier and Brosset, David and Kermarrec, Yvon and Simonin, Jacques. Cyber attacks real time detection : towards a cyber situational awareness for naval systems. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pages 1–2. IEEE, 2019.

[Jac19b] Jacq, Olivier and Laso, Pedro Merino and Brosset, David and Simonin, Jacques and Kermarrec, Yvon and Giraud, Marie-Annick. Maritime cyber situational awareness elaboration for unmanned vehicles. In *Maritime Situational Awareness Workshop*, 2019.

[Jgu16] Ines Jguirim. *Modélisation et génération d'itinéraires contextuels d'activités urbaines dans la ville*. Thèse de doctorat, Ecole doctorale des sciences de la mer, 2016.

[Jon16] Jones, Kevin D and Tam, Kimberly and Papadaki, Maria. Threats and impacts in maritime cyber security. *Engineering & Technology Reference*, 2016.

[Kat17] Sokratis K Katsikas. Cyber security of the autonomous ship. In *Proceedings of the 3rd ACM workshop on cyber-physical system security*, pages 55–56. ACM, 2017.

[Kav18] Kavallieratos, Georgios and Katsikas, Sokratis and Gkioulos, Vasileios. Cyber-attacks against the autonomous ship. In *Computer Security*, pages 20–36. Springer, 2018.

[KDC+18] Alexandre Kabil, Thierry Duval, Nora Cuppens, Gérard Le Comte, Yoran Halgand, and Christophe Ponchel. From cyber security activities to collaborative virtual environments practices through the 3D cybercop platform. In *International Conference on Information Systems Security*, pages 272–287. Springer, 2018.

[KHL+21] Mathias Karlsson, Sandra Haraldson, Mikael Lind, Eddie Olsson, Trond Andersen, and Miluše Tichavska. *Data Visualisation Tools for Enhanced Situational Awareness in Maritime Operations*, pages 355–372. Springer International Publishing, Cham, 2021.

[Kri13] Krile, Srećko and Kezić, Danko and Dimc, Franc. NMEA communication standard for shipboard data architecture. *NAŠE MORE : znanstveno-stručni časopis za more i pomorstvo*, 60(3-4) :68–81, 2013.

[KSB+19] Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. Matched and mismatched SOCs : A qualitative study on security operations center issues. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1955–1970, 2019.

[Kuc07] Kuchar, JE and Drumm, Ann C. The traffic alert and collision avoidance system. *Lincoln Laboratory Journal*, 16(2) :277, 2007.

[Lab20] Richard Labévière. *Reconquérir par la mer : La France face à la nouvelle géopolitique des océans.* Temporis, Paris, 2020.

[Lag10] Philippe Lagadec. Visualisation et analyse de risque dynamique pour la cyberdéfense. In *Symposium sur la Sécurité des Technologies de l'Information et de la Communication*, pages 3–31, 2010.

[Lev17] Oskar Levander. Autonomous ships on the high seas. *IEEE spectrum*, 54(2) :26–31, 2017.

[LMWW21] Mikael Lind, Michalis Michaelides, Robert Ward, and Richard Thomas Watson, editors. *Maritime Informatics.* Progress in IS. Springer International Publishing, 2021.

[LPV13] David López, Oscar Pastor, and L Garcıa Villalba. Dynamic risk assessment in information systems : state-of-the-art. In *Proceedings of the 6th International Conference on Information Technology, Amman*, pages 8–10, 2013.

[Mav17] Mavroeidis, Vasileios and Bromander, Siri. Cyber threat intelligence model : an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In *2017 European Intelligence and Security Informatics Conference (EISIC)*, pages 91–98. IEEE, 2017.

[McG00] McGuinness, Barry and Foy, Louise. A subjective measure of sa : the crew awareness rating scale (cars). In *Proceedings of the first human performance, si-*

tuation awareness, and automation conference, Savannah, Georgia, volume 16, 2000.

[Mer15] Merk, Olaf and Busquet, Bénédicte and Aronietis, Raimonds. The impact of mega-ships, case-specific policy analysis, 2015.

[mf] Cluster maritime français. Livre bleu de la marétique. https://issuu.com/opteam/docs/seagital-livre-bleu-12112013. Consulté le 20/05/2018.

[Mil19] Natalia Miloslavskaya. *Network Security Intelligence Centres for Information Security Incident Management*. Thèse de doctorat, University of Plymouth, 2019.

[MK19] Mary C Kay Michel and Michael C King. The future of cyber analytics : Identity classification for systematic and predictive insight. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pages 1–4. IEEE, 2019.

[ML17] Pedro Merino Laso. *Détection de dysfonctionements et d'actes malveillants basée sur des modèles de qualité de données multi-capteurs*. Thèse de doctorat, Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire, 2017.

[nat] Marine nationale. Dossier d'information marine 2019. https://cols-bleus-fr.s3.amazonaws.com/exemplaires/pdf/DIM-2019.pdf.

[Nic19] Hellesen Niclas. Cyber situational security awareness architecture (cssa) for industrial control systems. Master's thesis, NTNU, 2019.

[Onw12] Onwubiko, Cyril and Owens, Thomas. Review of situational awareness for computer network defense. In *Situational Awareness in Computer Network Defense : Principles, Methods and Applications*, pages 1–9. IGI Global, 2012.

[oS] Internal Chamber of Shipping. ICS - key facts. http://www.ics-shipping.org/shipping-facts/key-facts. Consulté le 20/05/2018.

[OTA17] OTAN. AAP-06 glossaire OTAN de termes et définitions (anglais et français), 2017.

[Pan18] Panero, Pablo and Vlsan, Liviu and Brillault, Vincent and Schuszter, Ioan Cristian. Building a large scale intrusion detection system using big data technologies. *PoS*, page 014, 2018.

[Por14] Porathe, Thomas and Prison, Johannes and Man, Yemao. Situation awareness in remote control centres for unmanned ships. In *Proceedings of Human Factors in Ship Design & Operation, 26-27 February 2014, London, UK*, page 93, 2014.

[PPM18] Nikolaos Polatidis, Michalis Pavlidis, and Haralambos Mouratidis. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Computer Standards & Interfaces*, 56 :74–82, 2018.

[Rø14] Rødseth, Ørnulf Jan and Tjora, Åsmund. A system architecture for an unmanned ship. In *Proceedings of the 13th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT)*, 2014.

[SHJ+19] Shamika N Sirimanne, J Hoffman, W Juan, R Asariotis, M Assaf, G Ayala, H Benamara, D Chantrel, J Hoffmann, A Premti, et al. Review of maritime transport, 2019. Technical report, tech. rep, 2019.

[Sic18] Franck Sicard. *Prise en compte des risques de cyber-attaques dans le domaine de la sécurité des systèmes cyber-physiques : proposition de mécanismes de détection à base de modèles comportementaux.* Thèse de doctorat, Grenoble Alpes, 2018.

[Sto11] Stouffer, Keith A and Falco, Joseph A and Scarfone, Karen A. SP 800-82. guide to Industrial Control Systems (ICS) security : Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), 2011.

[Str17] Strom, Blake E and Battaglia, Joseph A and Kemmerer, Michael S and Kupersanin, William and Miller, Douglas P and Wampler, Craig and Whitley, Sean M and Wolf, Ross D. Finding cyber threats with ATT&CK-based analytics. Technical report, Technical Report MTR170202, MITRE, 2017.

[Svi19] Svilicic, Boris and Kamahara, Junzo and Rooks, Matthew and Yano, Yoshiji. Maritime cyber risk management : An experimental ship assessment. *The Journal of Navigation*, 72(5) :1108–1120, 2019.

[Tad10] Tadda, George P and Salerno, John S. Overview of cyber situation awareness. In *Cyber situational awareness*, pages 15–35. Springer, 2010.

[Tam18a] Tam, Kimberly and Jones, Kevin. Cyber-risk assessment for autonomous ships. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–8. IEEE, 2018.

[Tam18b] Tam, Kimberly and Jones, Kevin D. Maritime cybersecurity policy : the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, 3(2) :147–164, 2018.

[Tam19] Tam, Kimberly and Jones, Kevin. Factors affecting cyber risk in maritime. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pages 1–8. IEEE, 2019.

[TO21] Dominic Thomas and Steven O'Malley. *The Necessity of Standards for Maritime Informatics in Ship Operations*, pages 33–45. Springer International Publishing, Cham, 2021.

[TXLJ19] Yaodong Tao, Wei Xu, Hongbin Li, and Shenglong Ji. Experience and lessons in building an ics security testbed. In *2019 1st International Conference on Industrial Artificial Intelligence (IAI)*, pages 1–6. IEEE, 2019.

[Vei12] Veillard, Luc and Anquez, Mathieu and Histrimont, Jean-Pierre. Vulnérabilités de la France face aux flux maritimes. *Étude prospective et stratégique*, page 140, 2012.

[WDWI16] Cynthia Wagner, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. Misp : The design and implementation of a collaborative threat intelligence sharing platform. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pages 49–56. ACM, 2016.

[Yad15] Yadav, Tarun and Rao, Arvind Mallari. Technical aspects of cyber kill chain. In *International Symposium on Security in Computing and Communication*, pages 438–452. Springer, 2015.

[Yen10] Yen, John and McNeese, Michael and Mullen, Tracy and Hall, David and Fan, Xiaocong and Liu, Peng. RPD-based hypothesis reasoning for cyber situation awareness. In *Cyber situational awareness*, pages 39–49. Springer, 2010.

[Zha19] Zhang, Haiyan and Peng, Minfang and Guerrero, Josep M and Gao, Xingle and Liu, Yanchen. Modelling and vulnerability analysis of cyber-physical power systems based on interdependent networks. *Energies*, 12(18) :3439, 2019.

[Zim14] Carson Zimmerman. Ten strategies of a world-class cybersecurity operations center. *MITRE corporate communications and public affairs. Appendices*, 2014.

Annexes

Annexe

A *Information Technology* et *Operational Technology*

Les différences les plus fréquemment évoquées entre l'*Information Technology* et l'*Operational Technology* sont listées dans le tableau A.1.

Tableau A.1 : Principales différences entre *Information Technology* et *Operational Technology*

Catégorie	**Système IT**	**Système OT**
Exigences en performances	Non temps-réel. Le temps de réponse doit être cohérent. Débit élevé nécessaire. Un délai et une gigue élevés sont acceptables. Les impacts en cas d'urgence sont peu critiques. Un contrôle d'accès strict peut être mis en œuvre au degré nécessaire pour assurer la sécurité.	Temps réel. La réponse de réponse est critique. Un débit modeste est acceptable. L'accès aux systèmes industriels devrait être strictement contrôlé mais ne devrait pas entraver ou interférer avec une interaction homme-machine.
Exigences en disponibilité	Les réponses comme le redémarrage sont acceptables. Des pertes de disponibilité peuvent être tolérées en fonction des besoins opérationnels du système.	Les réponses comme le redémarrage peuvent ne pas être acceptables, en raison des exigences en disponibilité des processus industriels. Les exigences en disponibilité peuvent nécessiter des systèmes redondants. Les indisponibilités doivent être planifiées et prévues des jours / semaines en avance. La haute disponibilité nécessite des essais rigoureux avant déploiement.

(Suite du tableau page suivante)

Catégorie	Système IT	Système OT
Exigences en maîtrise de risques	Objectif : maîtrise des données. La confidentialité et l'intégrité des données sont essentielles. La tolérance à la faute est moins importante : une indisponibilité momentanée n'est pas un risque majeur. Le risque à impact majeur est le retard dans la réalisation d'opérations commerciales.	Objectif : contrôler le monde physique. La sécurité de l'homme est essentielle, suivie par la protection du processus industriel. La tolérance à la panne est essentielle, une indisponibilité même momentanée peut ne pas être acceptable. Les risques à impact majeur sont la non conformité à une exigence, les impacts environnementaux, la perte de vie humaine, d'équipement ou de production.
Enjeux logiciels	Les systèmes sont conçus pour être employés avec les systèmes d'exploitation classiques. Les mises à jour sont appliquées directement à l'aide d'outils de déploiement automatisé.	Systèmes d'exploitation disparates et éventuellement propriétaires, souvent sans capacité native de sécurité. Les évolutions logicielles doivent être réalisées avec précaution, généralement par les concepteurs du produit, en raison d'algorithmes de contrôle spécialisés et de matériel et de logiciel potentiellement modifiés.

(Suite du tableau page suivante)

Catégorie	Système IT	Système OT
Contraintes en ressources	Les systèmes sont conçus avec suffisamment de ressources pour permettre l'ajout d'applications tierces comme les solutions de sécurité.	Les systèmes sont conçus spécifiquement pour le processus industriel en question et pourraient ne pas avoir assez de mémoire et de capacité de calcul pour permettre l'ajout de capacités de sécurité.

Annexe B

Évènements redoutés génériques pour les systèmes d'information maritimes.

Nos travaux ont permis d'établir une liste des évènements redoutés génériques qui pourraient toucher un navire de commerce, de guerre, ou une infrastructure portuaire. Une majorité des évènements identifiés peuvent également s'appliquer aux drones maritimes et navires autonomes. L'homologation d'un système d'information [1] prévoit qu'une analyse de risques soit réalisée au niveau du système d'information, analyse dont le périmètre se limite à la zone fonctionnelle du système et à ses interconnexions. L'intérêt d'une vision plus macroscopique est de disposer d'une analyse de risques du navire dans son ensemble, voire par type de navire, voire pour le secteur maritime dans son ensemble. Bien que moins fine, elle permet une meilleure vue d'ensemble.

Atteintes à la navigation :

— altération du système de navigation électronique et de la cartographie, entraînant une perte de positionnement du navire et un risque de collision ;
— perte de la surveillance du trafic d'une zone maritime, ayant pour conséquence un risque accru de collision ;
— brouillage ou leurrage GPS, modification du référentiel géodésique sur un navire ciblé ou les navires avoisinants, entraînant un risque accru de collision ;
— altération de la détection du radar de navigation, ayant pour conséquence une perte de compréhension de la situation de surface (*Maritime Situational Awareness*) ;
— altération de la détection du sondeur (apparition d'une alarme « haut fond »), pouvant entraîner une désorganisation de la passerelle et la prise de mauvaises décisions ;

1. https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/

— émission de fausses pistes AIS, violations en intégrité ou disponibilité du protocole, entraînant la perte de la compréhension de la situation surface et des prises de décision inappropriées ;
— atteinte en disponibilité du système ECDIS, pouvant impacter la navigation du navire.

Atteinte aux systèmes de communication :
— coupure des communications radio externes, entraînant un isolement total du navire ;
— coupure des communications internes (VoIP, ToIP, autocommutateur), ayant pour conséquence une désorganisation du navire ;
— usure des équipements par augmentation de la puissance, ayant pour conséquence leur dégradation prématurée et leur indisponibilité ;
— altération des horloges, entraînant des défauts de synchronisation, des incohérences, voire des dysfonctionnements des installations embarquées.

Atteinte aux systèmes de plate-formes :
— attaque globale sur le système d'exploitation du navire permettant la gestion globale des installations de plate-formes, entraînant une impossibilité d'action sur ces installations ;
— atteinte du domaine électricité : usine électrique haute tension, distribution basse tension, ou de l'éclairage : ces attaques impactent fortement le bord : arrêt des chambres froides... ;
— atteinte du domaine auxiliaire : eaux noires, eaux douce, servitudes, froid : vidange des eaux noires / eau de cale, altération des osmoseurs, perte de l'eau réfrigérée ;
— atteinte du domaine sécurité : perte de la détection pour la lutte contre les sinistres, voies d'eau, incendie, eau de mer ;
— atteinte au domaine mobilité : atteinte sur la commande du propulseur principal, appareil à gouverner, propulseur azimutal, système de positionnement dynamique : mise en fonctionnement erratique, accélération de la propulsion, blocage de la barre, pouvant entraîner, en complément d'une usure prématurée, des collisions.

Atteinte aux systèmes portuaires :
— atteinte à la disponibilité d'informations et de fonctions essentielles par l'emploi d'un rançongiciel, empêchant le port de fonctionner nominalement ;
— prise en main à distance du *smart port* en exploitant l'interconnexion croissante entre les systèmes pour réaliser des actions discrètes de modification ou destructrices sur les installations ;
— modification des systèmes d'information logistiques des ports (mouvement des na-

vires, des passagers, du fret ou des moyens de manutention et de transport), ayant pour conséquence une désorganisation du port ;

— atteinte en disponibilité des services portuaires (pilotage, avitaillement...), des quais, grues et aires de stockage, empêchant l'accueil et le débarquement ou départ de navires, etc.

— leurrage ou brouillage GPS entravant le fonctionnement automatisé ou semi-automatisé d'un portique de déchargement.

Annexe C

Modélisation d'attaque sur un système ECDIS à partir des *frameworks* MITRE.

La modélisation d'attaque sur un système ECDIS est réalisée en utilisant les *frameworks* MITRE PRE-ATT&CK™ et ATT&CK™. L'objectif de la modélisation est de déterminer les capteurs les plus appropriés pour détecter la menace. S'agissant d'une menace avancée et obfusquée, conformément aux recommandations du MITRE, les solutions antivirales sont volontairement absentes des outils de protection. La modélisation repose sur la première phase tactique et technique de reconnaissance et d'instrumentation, puis d'une seconde phase d'exploitation à proprement parler.

La méthode d'attaque utilise successivement des méthodes d'ingénierie sociale, afin d'émettre un courriel forgé en se faisant passer pour le fournisseur de cartes marines, afin de réaliser une mise à jour sur un système ECDIS d'un navire en mer, localisé grâce à sa position AIS. A défaut de mise à jour, la pièce jointe contient une charge virale qui réalise le chiffrement de l'ECDIS et parcourt le réseau à la recherche d'autres ECDIS afin d'en réaliser le chiffrement.

Bien que le *framework* NIST ne soit pas centré sur les processus, ils sont ici identifiés au mieux afin de faciliter la compréhension du modèle. A chaque étape, le capteur cyber qui permettrait l'identification de la menace est précisé (HIDS, NIDS). Il est considéré que l'ensemble des éventuels journaux est collecté par un HIDS.

Le MITRE concentre ses recommandations de surveillance sur les hôtes, notamment par l'utilisation de *sysmon*, afin de permettre la détection de menaces avancées non détectables par des antivirus et utilisant généralement des flux réseaux chiffrés. L'analyse des types de

capteurs à employer montre cependant que, en complément de l'analyse des journaux et activités remontées par des hôtes, la détection d'anomalie par des capteurs de type HIDS permet de détecter des violations d'intégrité de fichiers, par exemple. Enfin, un capteur de type NIDS est efficace sur du trafic non chiffré mais peut aussi permettre d'identifier des flux réseaux illégitimes ou une détection d'anomalie se basant sur une évolution de volumétrie ou de comportement du réseau.

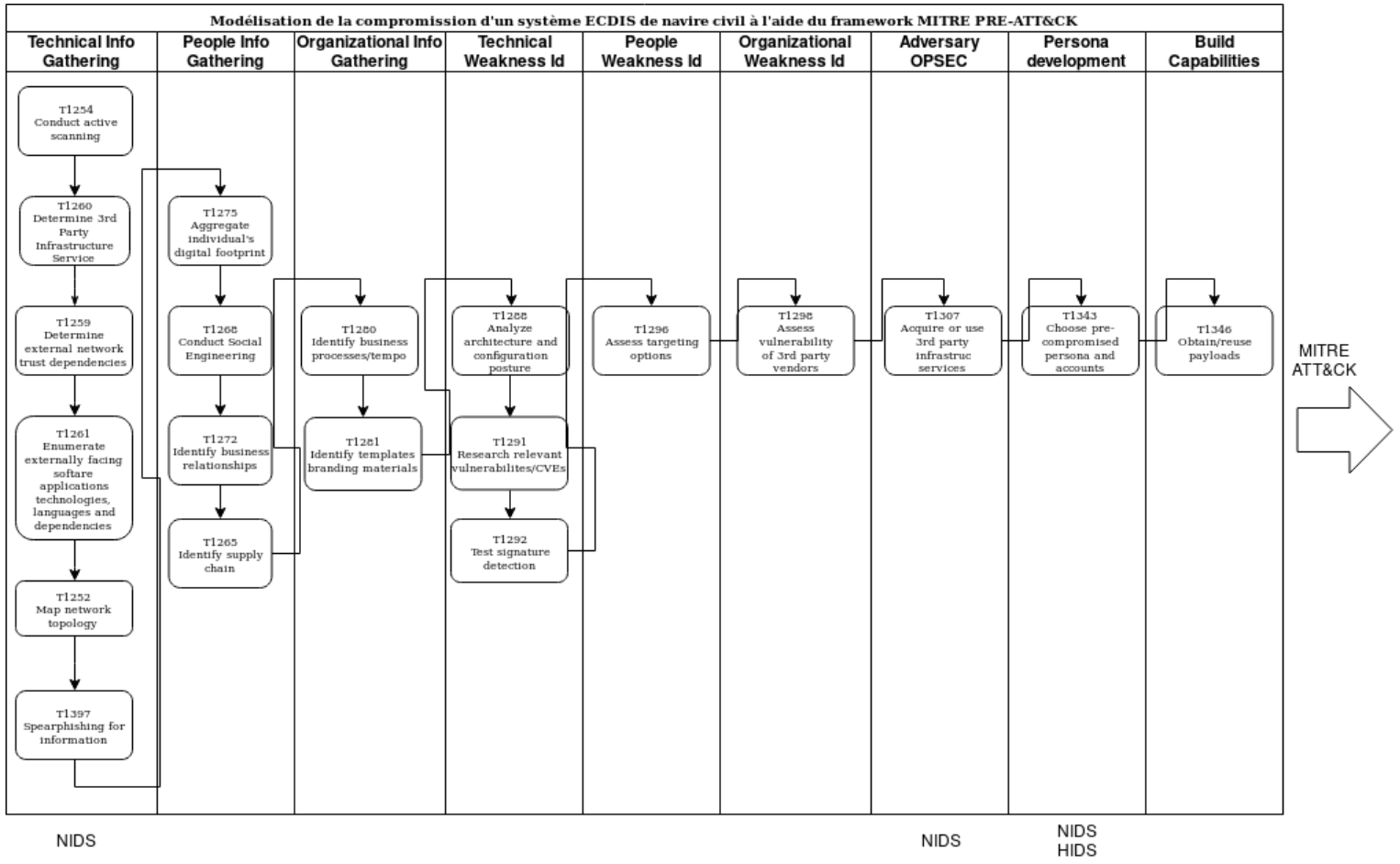

FIGURE C.1 : Modélisation pré-exploitation du *framework* NIST Pre-ATT&CK sur une attaque avancée sur un système ECDIS (source : archives personnelles).

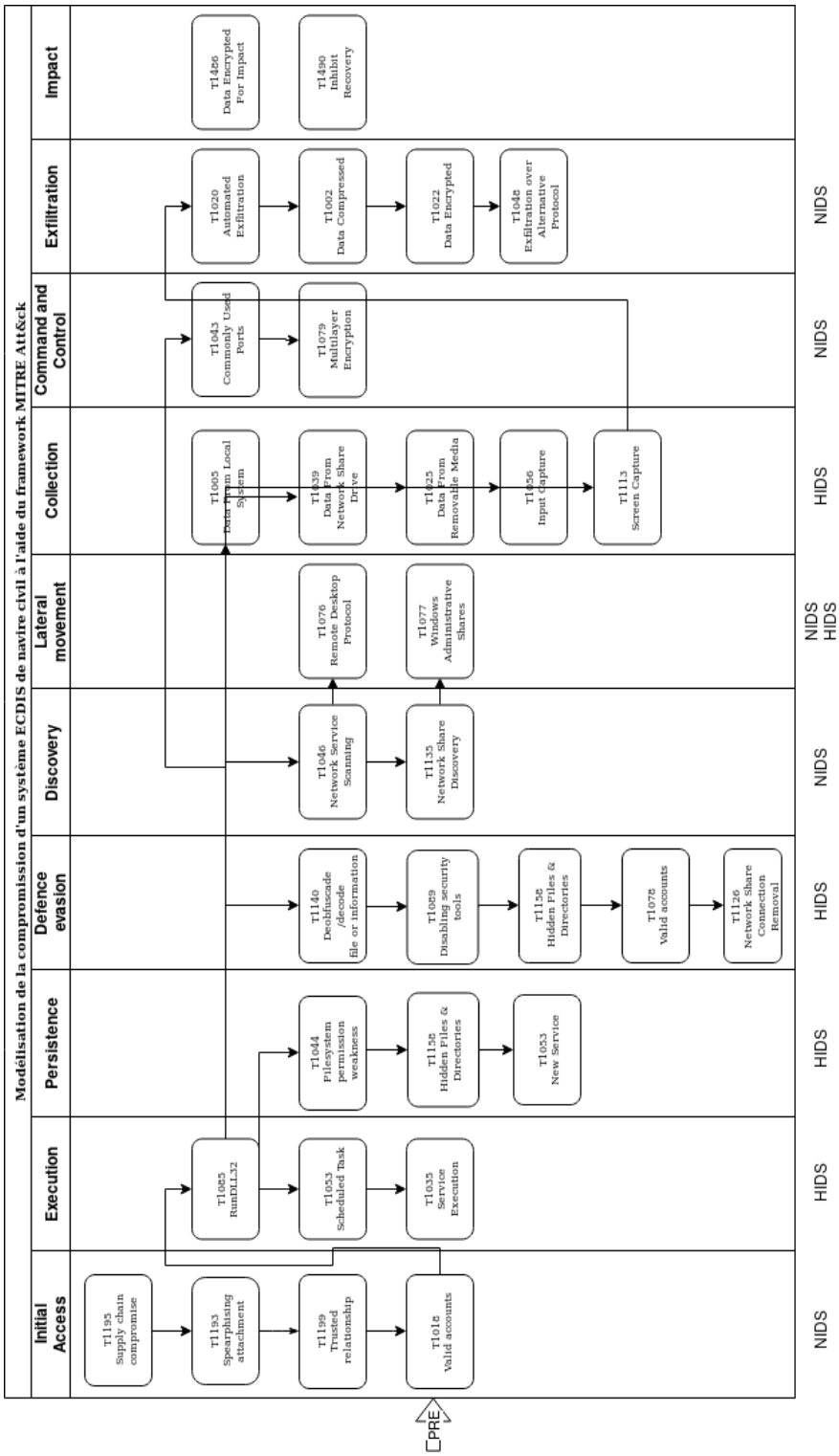

FIGURE C.2 : Modélisation post-exploitation du *framework* NIST ATT&CK sur une attaque avancée sur un système ECDIS (source : archives personnelles).

Annexe D

Visualisation du déterminisme d'un réseau NMEA à partir du trafic réseau capturé en fonction du *talker id*.

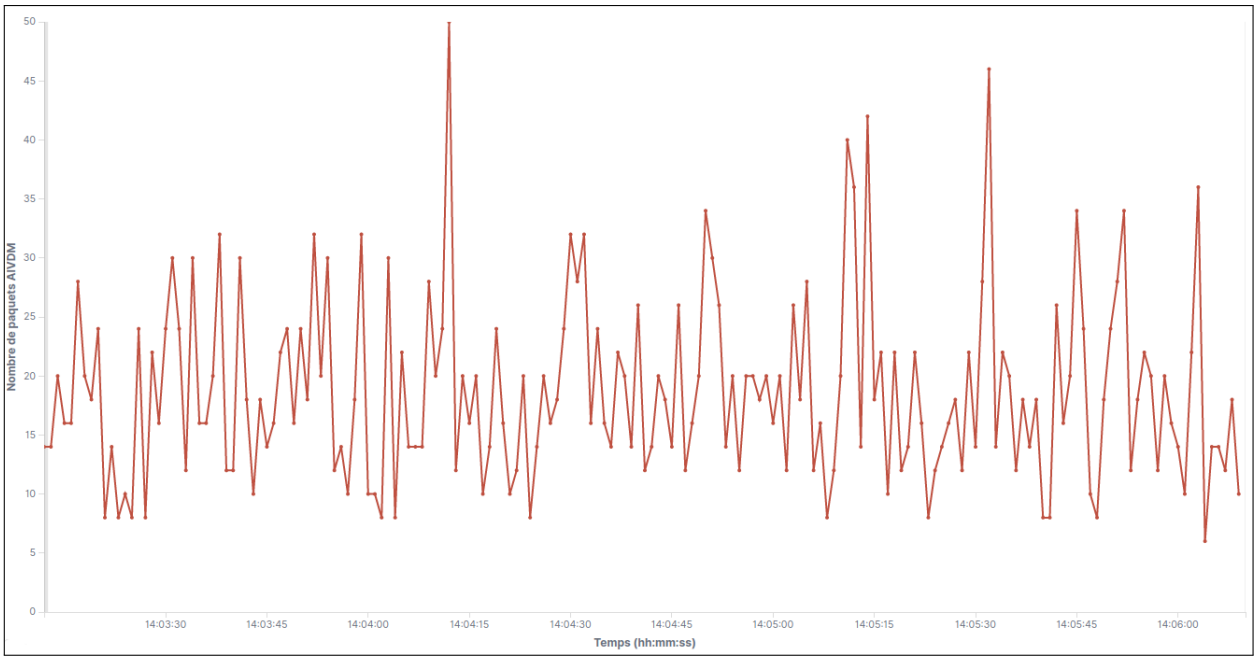

FIGURE D.1 : Évolution temporelle de la *sentence* AIVDM (source : archives personnelles).

La figure D.1 montre que la répartition dans le temps du nombre de *sentences* AIVDM ne présente pas, *a priori*, de caractère déterministe. En effet, le trafic AIS amenant à l'émis-

FIGURE D.2 : Évolution temporelle de la *sentence* GCGGA (source : archives personnelles).

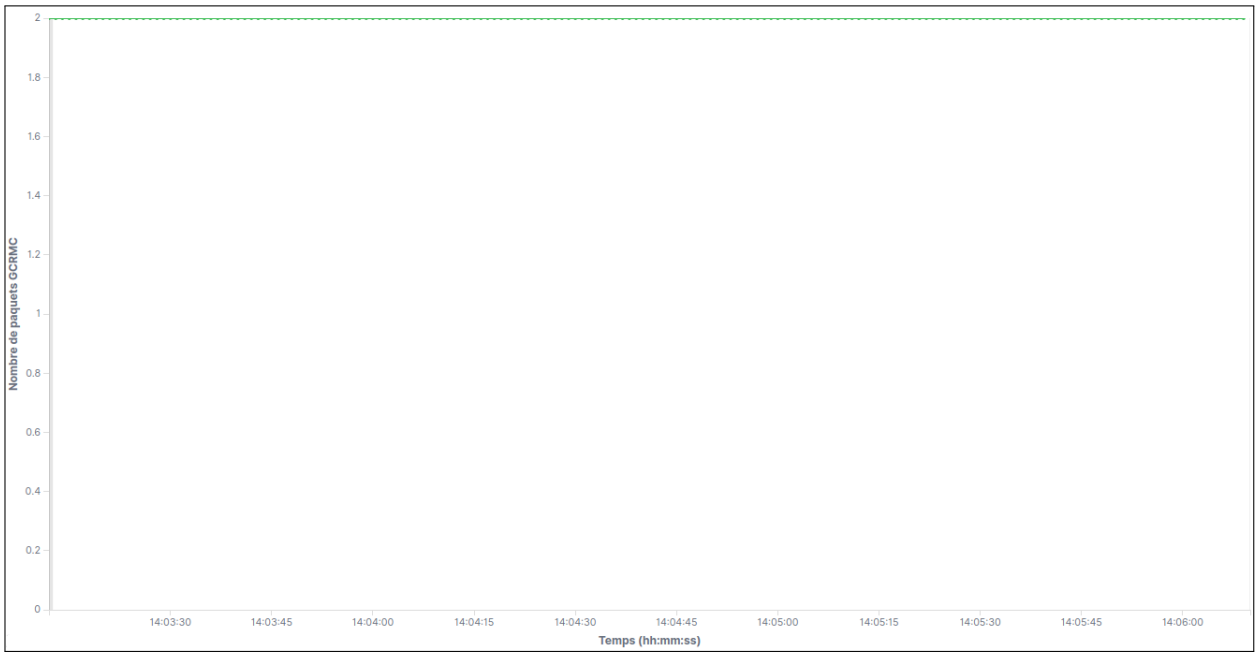

FIGURE D.3 : Évolution temporelle de la *sentence* GCRMC (source : archives personnelles).

sion de trames AIVDM évolue dans le temps, en fonction de la position du navire, du nombre de navires à proximité, de la propagation ionosphérique, *etc.*

L'ensemble des *sentences* émises par le *talker* GC et présenté dans les figures D.2,

FIGURE D.4 : Évolution temporelle de la *sentence* GCVTG (source : archives personnelles).

FIGURE D.5 : Évolution temporelle de la *sentence* GCZDA (source : archives personnelles).

FIGURE D.6 : Évolution temporelle de la *sentence* GPGGA (source : archives personnelles).

FIGURE D.7 : Évolution temporelle de la *sentence* GPRMC (source : archives personnelles).

D.3, D.4 et D.5 dénote un fort caractère déterministe : en effet, ce capteur GNSS émet ses informations de manière très régulière et linéaire sur le réseau NMEA : une droite horizontale relie les points d'émission des *sentences*.

FIGURE D.8 : Évolution temporelle de la *sentence* IOTXT (source : archives personnelles).

L'ensemble des *sentences* émises par le *talker* GP et présenté dans les figures D.6 et D.7 dénote un fort caractère déterministe : en effet, ce capteur GNSS émet ses informations de manière très régulière et linéaire sur le réseau NMEA. Là aussi, une droite horizontale relie les points d'émission des *sentences*.

L'ensemble des *sentences* émises par le *talker* IO et présenté dans la figure D.8 dénote un fort caractère déterministe : ce capteur émet ses informations de manière très régulière et linéaire sur le réseau NMEA. Là aussi, une droite horizontale relie les points d'émission des *sentences*.

L'ensemble des *sentences* émises par le *talker* NA et présenté dans les figures D.9, D.10 et D.11 dénote un fort caractère déterministe : ce capteur émet ses informations de manière très régulière et linéaire sur le réseau NMEA. Là aussi, une droite horizontale relie les points d'émission des *sentences*.

L'ensemble des *sentences* émises par le *talker* NW et présenté dans les figures D.12, D.13, D.14 et D.15 dénote un fort caractère déterministe : ce capteur émet ses informations de manière très régulière et linéaire sur le réseau NMEA. Là aussi, une droite horizontale relie les points d'émission des *sentences*.

L'ensemble des *sentences* émises par le *talker* PH (format propriétaire) et présenté

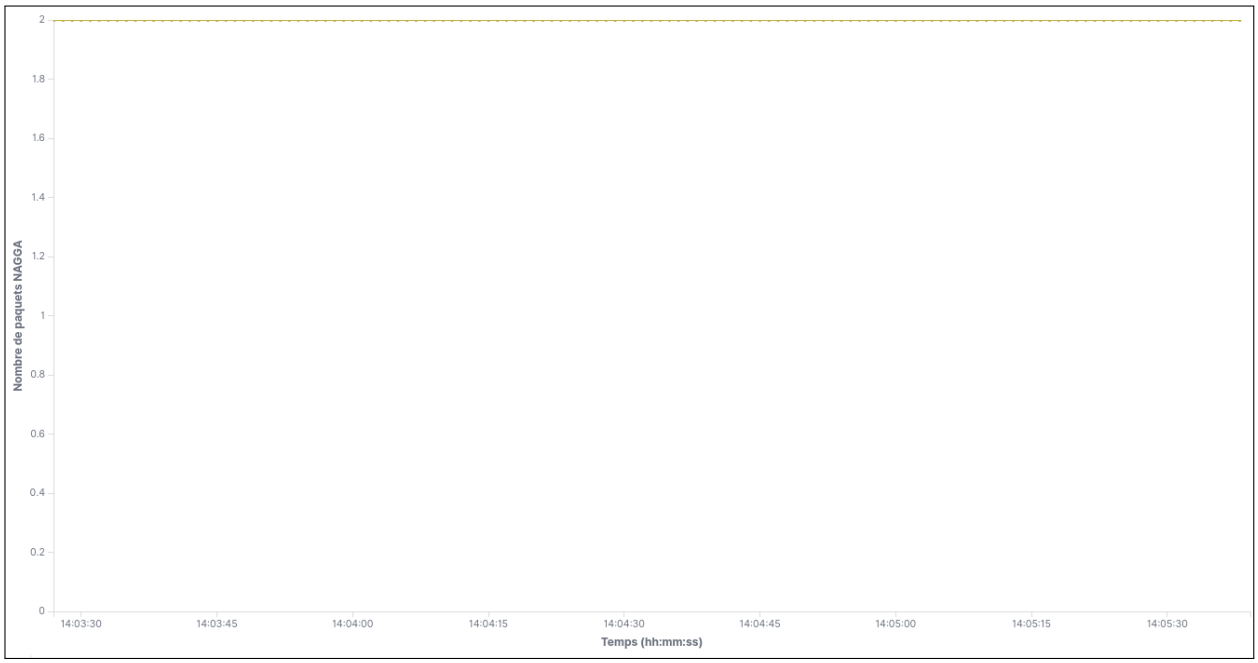

FIGURE D.9 : Évolution temporelle de la *sentence* NAGGA (source : archives personnelles).

FIGURE D.10 : Évolution temporelle de la *sentence* NAVHW (source : archives personnelles).

FIGURE D.11 : Évolution temporelle de la *sentence* NAVTG (source : archives personnelles).

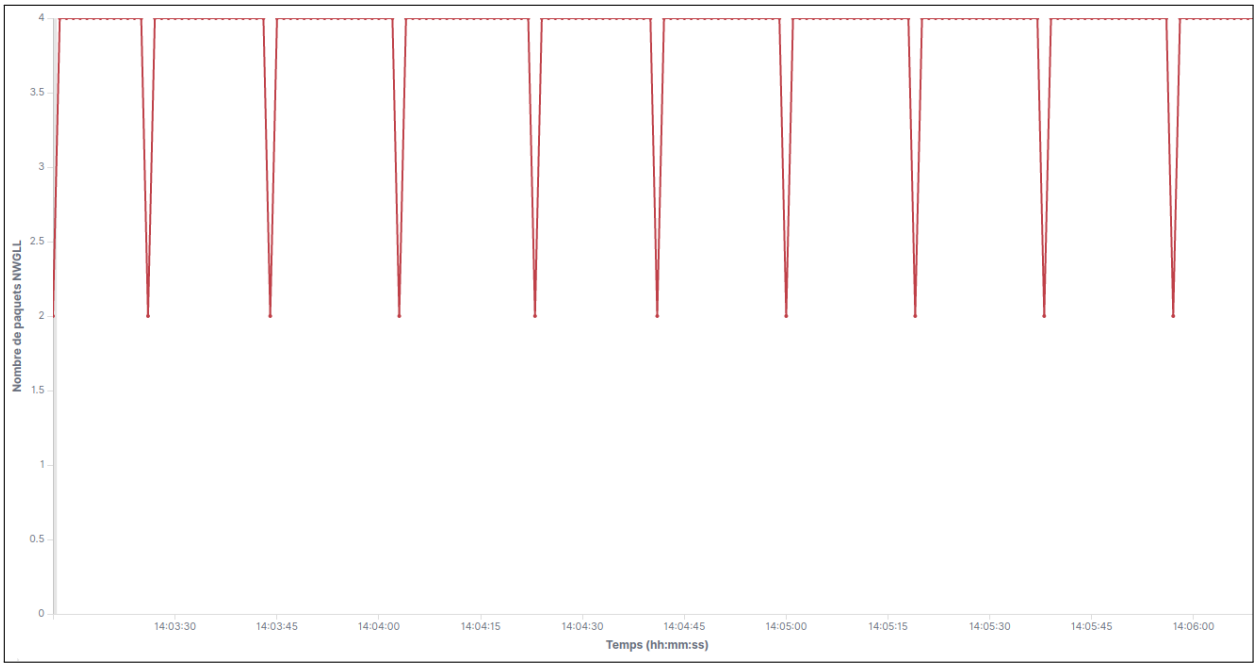

FIGURE D.12 : Évolution temporelle de la *sentence* NWGLL (source : archives personnelles).

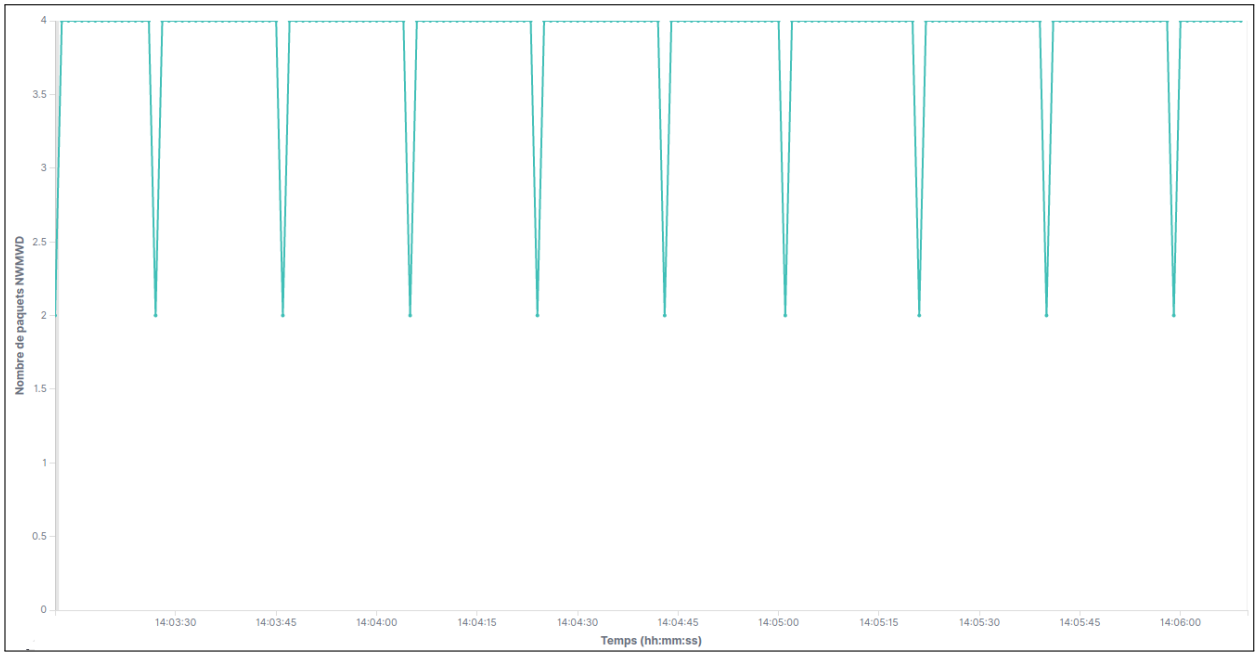

FIGURE D.13 : Évolution temporelle de la *sentence* NWMWD (source : archives personnelles).

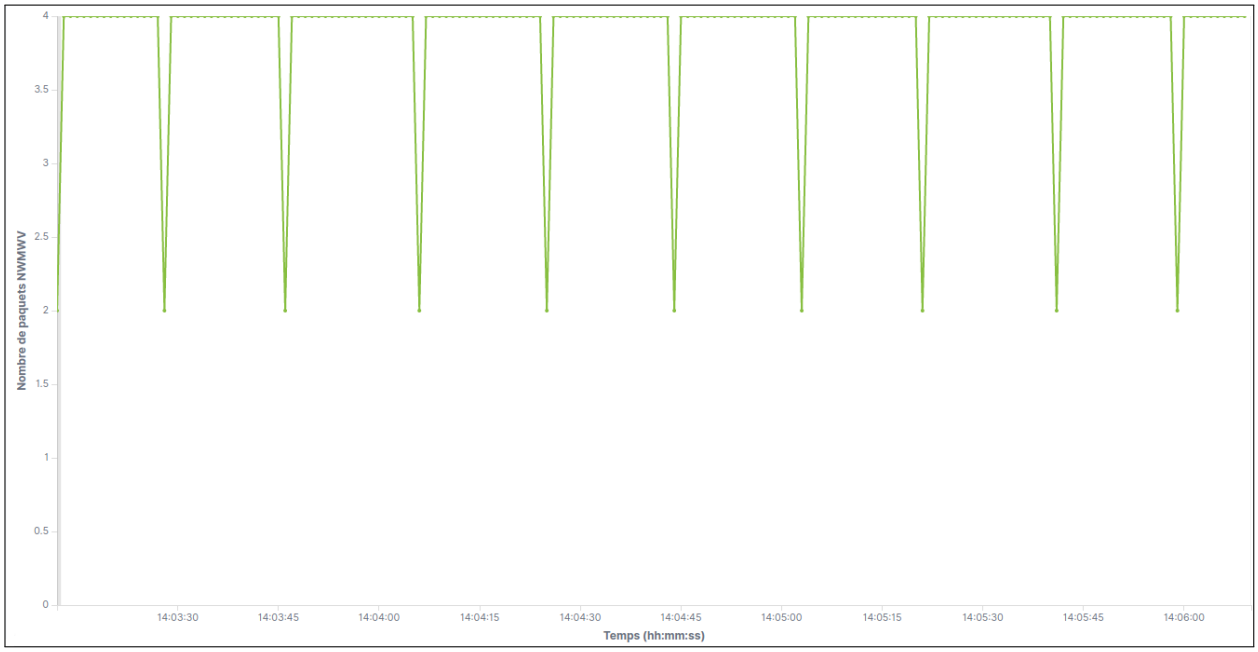

FIGURE D.14 : Évolution temporelle de la *sentence* NWMWV (source : archives personnelles).

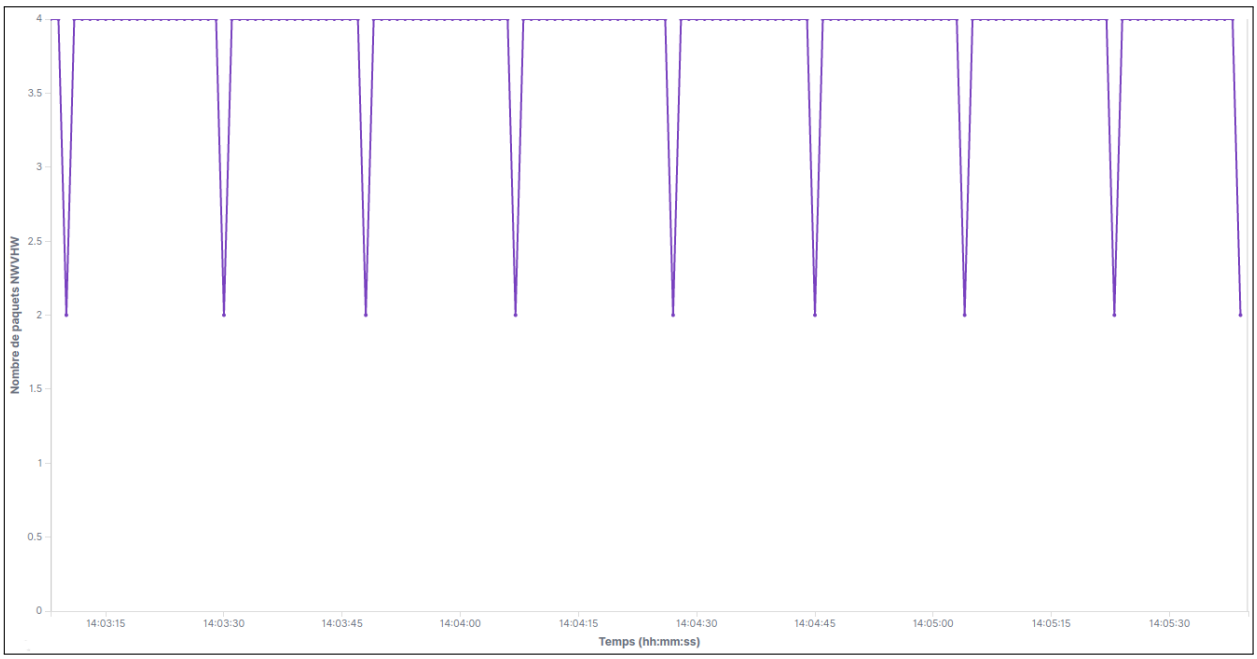

FIGURE D.15 : Évolution temporelle de la *sentence* NWVHW (source : archives personnelles).

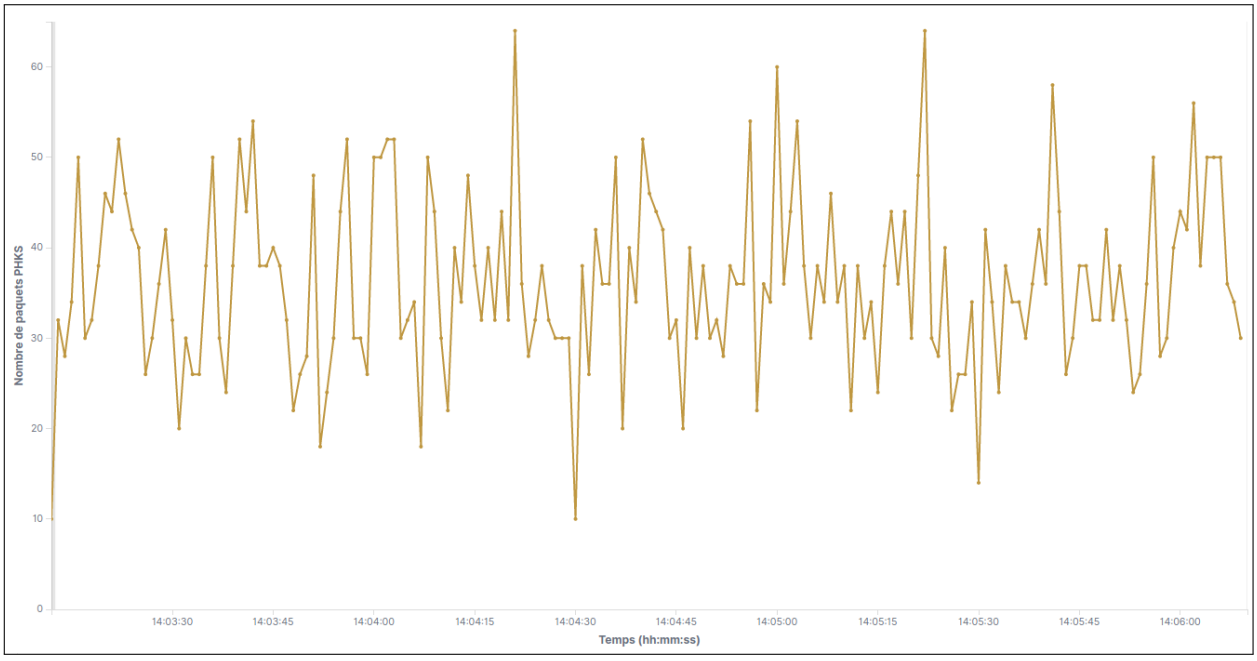

FIGURE D.16 : Évolution temporelle de la *sentence* PHKS (source : archives personnelles).

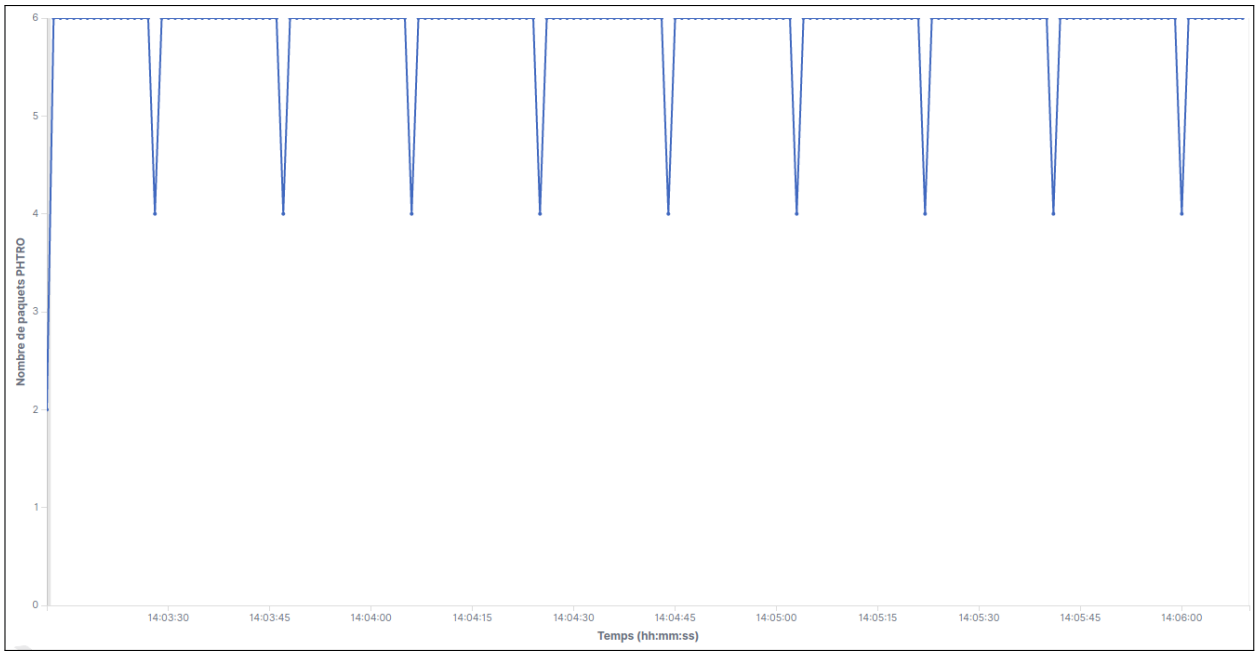

FIGURE D.17 : Évolution temporelle de la *sentence* PHTRO (source : archives personnelles).

dans les figures D.16 et D.17 dénote un fort caractère déterministe pour la *sentence* TRO : ce capteur émet cette information de manière très régulière et linéaire sur le réseau NMEA. Un rapprochement intéressant peut être fait avec le capteur NW, le schéma de répétition étant très similaire. En revanche, la *sentence* PHKS ne présente pas de caractère déterministe évident.

FIGURE D.18 : Évolution temporelle de la *sentence* RAOSD (source : archives personnelles).

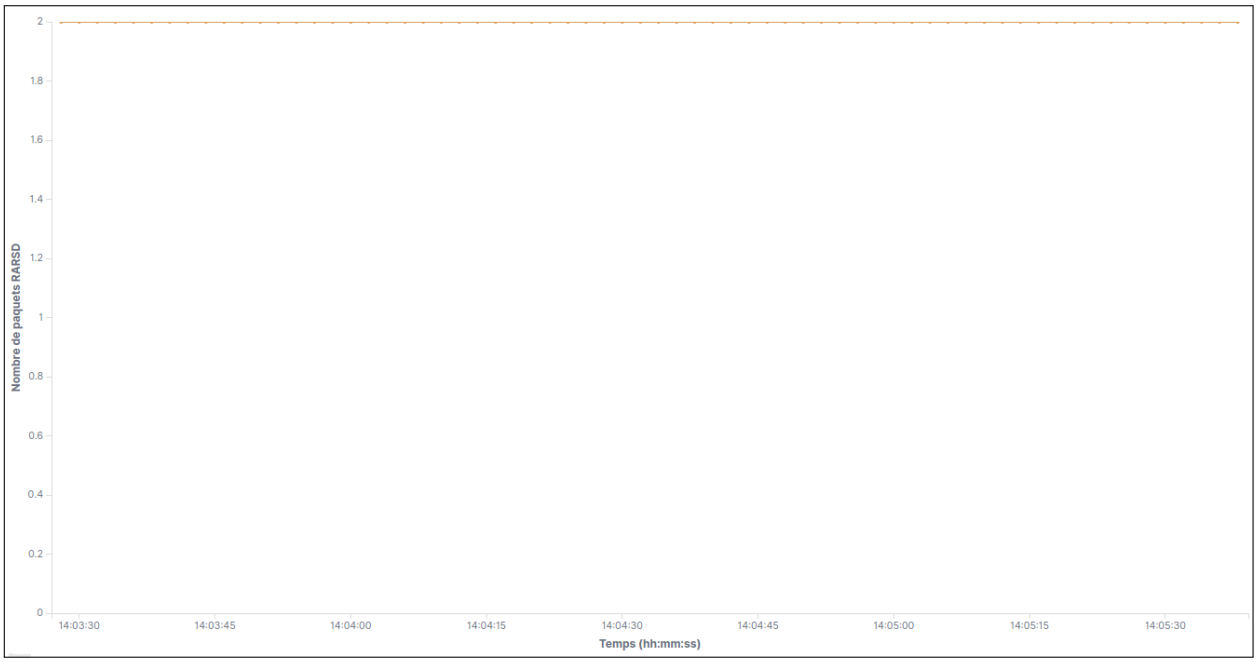

FIGURE D.19 : Évolution temporelle de la *sentence* RARSD (source : archives personnelles).

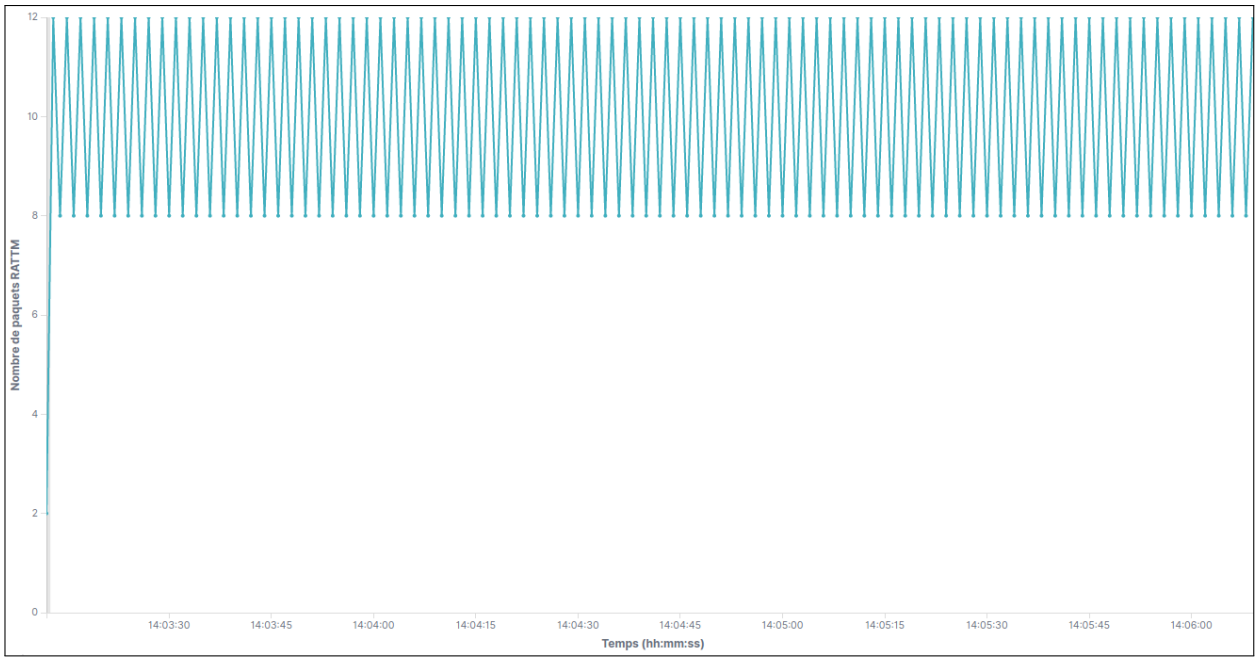

FIGURE D.20 : Évolution temporelle de la *sentence* RATTM (source : archives personnelles).

L'ensemble des *sentences* émises par le *talker* RA et présenté dans les figures D.18, D.19 et D.20 dénote un fort caractère déterministe : ce capteur radar émet ses informations de manière très régulière et linéaire sur le réseau NMEA. Là aussi, une droite horizontale relie les points d'émission des *sentences* RAOSD et RARSD. La *sentence* RATTM (D.20) émet cependant ses informations de manière plus spécifique : le nombre de *sentences* TTM émises évolue de manière régulière, mais à une fréquence relativement élevée.

L'ensemble des *sentences* émises par le *talker* SD et présenté dans les figures D.21 et D.22 dénote un fort caractère déterministe : ce capteur émet ses informations de manière très régulière et linéaire sur le réseau NMEA. Là aussi, une droite horizontale relie les points d'émission.

L'ensemble des *sentences* émises par le *talker* SP et présenté dans les figures D.23 et D.24 dénote un fort caractère déterministe : ce capteur émet ses informations de manière très régulière et linéaire sur le réseau NMEA. Là aussi, une droite horizontale relie les points d'émission.

FIGURE D.21 : Évolution temporelle de la *sentence* SDDBT (source : archives personnelles).

FIGURE D.22 : Évolution temporelle de la *sentence* SDDPT (source : archives personnelles).

FIGURE D.23 : Évolution temporelle de la *sentence* SPBDT (source : archives personnelles).

FIGURE D.24 : Évolution temporelle de la *sentence* SPDPT (source : archives personnelles).

Glossaire

ACARS Aircraft Communications and Reporting System. 46

ADS-B Automatic Dependent Surveillance-Broadcast. 46

AGREMI Agression Électromagnétique Intentionnelle. 32

AIS Automatic Identification System. 21, 47, 72, 106, 107, 109, 110, 112, 114, 130, 150, 153, 157

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information. 3, 75

API Automate Programmable Industriel. 74

APT Advanced Persistent Threat. 55

ARPA Automatic Radar Plotting Aid. 107, 113

ASCII American Standard Code for Information Interchange. 106

BM Bandwidth Manager. 78

BNWAS Bridge Navigational Watch Alarm System. 20

CARMEN Cyber Situational AwaReness Made Easy for NMEA. 116, 117, 121, 124–126, 130

CCR Cargo Control Room. 21

CCTV Closed Circuit TeleVision. 20

CE Central Engine. 78, 81, 93, 97, 103

CMS Combat Management System. 48

CMS Content Management System. 104

CNV Coopération Navale Volontaire. 3

CoA Course of Action. 67, 115

COMEX Compagnie Maritime d'Expertise. 16

CP Central Processor. 78, 81

CPA Closest Point of Approach. 47, 48

CPER Contrat Plan État-Région. 72

CSA Cyber Situational Awareness. 49–52, 70, 129

CSAC Cyber Situational Awareness Console. 77, 79–81

CSIRT Computer Security Incident Response Team. 36, 85, 103, 120

CTI Cyber Threat Intelligence. 36, 63

CVE Common Vulnerabilities and Exposures. 103–105

CVSS Common Vulnerability Scoring System. 104

CZM Commandant de Zone Maritime. 58

DECT Digital Enhanced Cordless Telephone. 20

DFIR Digital Forensics and Incident Response. 78

DNS Domain Name Service. 78, 97

DP Dynamic Positioning. 21

DRA Dynamic Risk Assessment. 101, 102, 127

ECDIS Electronic Chart Display Information System. 21, 48, 56–58, 106, 114, 121, 126, 150, 153

ECS Electronic Chart System. 48, 57, 58, 72, 106, 107, 115–117, 121, 125, 126

EFR Effet Final Recherché. 27, 28

EMR Énergies Marines Renouvelables. 16, 20, 22

ETA Estimated Time of Arrival. 48

FN Faux Négatif. 61

FP Faux Positif. 61

FPC Full Packet Capture. 76

GMDSS Global Maritime Distress and Safety System. 21

GNSS Global Navigation Satellite System. 21, 72, 93, 106, 108, 113, 114, 124, 125, 160, 161

GPS Global Positioning System. 21, 106, 107, 114, 115, 117, 130, 149, 151

GSM Global System for Mobile communications. 20

HAPPINESS Holistic APProach of Integrated Navigation Equipment for cyberSecurity at Sea. 130

HIDS Host-based Intrusion Detection System. 39, 54, 57, 62, 63, 65, 75, 80, 83, 103, 153, 154

HUD Head Up Display. 44, 47

IBS Integrated Bridge System. 62, 108

ICMP Internet Control Message Protocol. 84

ICS Industrial Control System. 56, 57, 72

IEM Impulsion Électro-Magnétique. 32

IFREMER Institut Français de Recherche pour l'Exploitation de la Mer. 16

IHM Interface Homme Machine. 125

INS Integrated Navigation System. 107, 108, 112, 127

IoC Indicator of Compromise. 52, 53, 56, 62, 63, 78, 85

IP Internet Protocol. 20

IT Information Technology. 20, 22, 23, 29, 37, 90, 91, 96, 123

KT Knowledge of Them. 43, 45, 47, 50–53, 62, 63, 66, 105

KU Knowledge of Us. 43, 45–47, 50–53, 62, 63, 66, 96, 101, 105, 125

LE Local Engine. 76, 92, 94, 126

LP Local Preprocessor. 76

MASS Maritime Autonomous Surface Ship. 19

MCS Maintien en Conditions de Sécurité. 5, 23, 29, 37

MCSA Maritime Cyber Situational Awareness. 8, 35, 54, 55, 58–60, 66, 69, 72, 75, 79, 87, 96, 101, 105, 120, 127, 129

MFD Multi-Functions Display. 48

MSA Maritime Situational Awareness. 106

MTU Maximum Transmission Unit. 88

NAVWAR Navigation War. 106

NCS Network Connexion Safety. 75

NIDS Network-based Intrusion Detection System. 39, 54, 57, 62, 63, 65, 66, 75, 76, 82–86, 90, 92, 98, 100, 101, 120, 153, 154

NIST National Institute of Standards and Technology. 20, 72

NMEA National Marine Electronics Association. 47, 72, 96, 105–109, 111–113, 116, 117, 124, 127, 130, 160, 161, 166, 168

NPI Network Probe Isolation. 76

NTP Network Time Protocol. 93

OCDE Organisation de coopération et de développement économiques. 12

OMI Organisation Maritime Internationale. 19

OSI Open Systems Interconnection. 97, 99

OT Operational Technology. 20–23, 29, 37, 57, 72, 90, 96, 115, 123

OTAN Organisation du Traité de l'Atlantique Nord. 26, 42

PCI Plan de Continuité Informatique. 62

PIB Produit Intérieur Brut. 14

PMS Property Management System. 20

PRI Plan de Reprise Informatique. 64

RIC Renseignement d'Intérêt Cyber. 51–53, 56, 65, 78

ROSO Renseignement d'Origine Source Ouverte. 32

RTT Round Trip Time. 87, 88

SA Situational Awareness. 8, 43–49, 53, 59, 60, 65, 81, 121, 127

SDR Software Defined Radio. 117

SGDSN Secrétariat Général de la Défense et de la Sécurité nationale. 3

SHOM Service Hydrographique et Océanographique de la Marine. 16

SIEM Security Information and Event Management. 36, 37, 39, 40, 52, 66, 83, 84, 93, 94, 102, 126

SIM Systèmes d'Information Maritimes. 20, 26–29, 35–37, 55–59, 62, 64, 69, 70, 79, 80, 93, 96, 97, 101, 102, 105, 116

SIRP Security Incident Response Platform. 36, 64, 78

SMTP Simple Mail Transfer Protocol. 83

SNLE Sous-marin Nucléaire Lanceur d'Engins. 17

SOC Security Operations Center. 36–38, 40, 51, 52, 54, 56, 58, 61, 66, 78, 85, 97, 103, 115, 120

SSAS Shipboard Security Alarm System. 21

SSM Ship Shore Manager. 77, 78, 89

STIX Structured Threat Information eXpression. 51

TAP Test Access Port. 75

TAXII Trusted Automated eXchange of Indicator Information. 51

TCAS Traffic Collision Avoidance System. 45, 47

TCP Transport Control Protocol. 99, 108

TTP Tactics, Techniques, Procedures. 36, 53, 55, 65, 67, 115, 129

UDP User Datagram Protocol. 107, 108

USV Unmanned Surface Vehicle. 106

VDR Voyage Data Recorder. 21

VLAN Virtual Local Area Network. 20

VN Vrai Négatif. 62

VP Vrai Positif. 62

VPN Virtual Private Network. 20, 78

VSAT Very Small Aperture Terminal. 87

VTS Vessel Traffic Service. 48

WiFi Wireless Fidelity. 20

ZEE Zone Économique Exclusive. 14, 17

DOCTORAT BRETAGNE LOIRE / MATHSTIC

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Titre : Détection, analyse contextuelle et visualisation de cyberattaques en temps-réel : élaboration de la *Cyber Situational Awareness* du monde maritime

Mots clés : cybersécurité ; maritime ; navire ; port ; détection d'intrusion ; situational awareness

Dans une économie globalisée, le secteur maritime est essentiel au bon fonctionnement des économies et permet d'acheminer 90% des marchandises. Dans un contexte de forte numérisation, le niveau de cybersécurité du secteur maritime reste en retrait par rapport aux autres secteurs d'activité d'importance vitale. Au travers d'une analyse de bout en bout, cette thèse décrit les particularités des systèmes d'information maritimes et modélise le concept de *Maritime Cyber Situational Awareness*.

Ensuite, une proposition d'architecture est décrite pour permettre l'acquisition de cet état de connaissance. Cette solution, éprouvée sur plate-forme, a permis de répondre à l'ensemble des critères d'élaboration. Enfin, les travaux soulignent et détaillent les spécificités du monde maritime pour tirer un profit maximal des données issues de la cybersurveillance.
Les analyses et architectures de cette étude dans un contexte contraint pourront probablement être élargies à d'autres secteurs, comme par exemple les véhicules autonomes ou encore l'Internet des objets.

Title : Real-time detection, contextual analysis and visualization of cyberattacks : Cyber Situational Awareness elaboration for the maritime sector

Keywords : cybersecurity ; maritime ; ship ; port ; intrusion detection ; situational awareness

Abstract: In a globalized economy, the maritime sector plays an essential role for the countries' economies, drawing 90% of the global world trade. In a highly digitalized transformation context, the cybersecurity level of the maritime sector remains low compared to other essential sectors. Through an end-to-end analysis, this thesis aims at describing the unique combined characteristics of maritime information systems. At first, we evaluate the possibility to apply the situational awareness definition to maritime cybersecurity and model the concept of Maritime Cyber Situational Awareness.
.

Then we describe the proposal of an architecture to achieve MCSA elaboration, which has been tested and proven on our experimental platform, taking into account the full requirements.
Finally, our work analyses the particularities of the maritime world to streamline the collected data. The analysis and architectures of this study could also be opened and applied to other sectors, such as autonomous vehicles and the Internet of Things (IoT).