Etudes des Activités humaines : de l'expérimentation à l'analyse

David Brosset

HABILITATION À DIRIGER DES RECHERCHES

L'UNIVERSITE DE BRETAGNE OCCIDENTALE

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

Par
David BROSSET

Etudes des Activités humaines : de l'expérimentation à l'analyse

Habilitation présentée et soutenue à l'école navale, Lanvéoc, le 13/09/2022
Unité de recherche : Institut de Recherche de l'Ecole navale/Arts et Métiers sciences et technologies
Chaire de cyberdéfense des systèmes navals

Rapporteurs avant soutenance :

Jean-Philippe BABAU	Université de Bretagne Occidentale, BREST
Aurélien FRANCILLON	Professeur des Universités, EURECOM, Campus SophiaTech - BIOT
Jérôme GENSEL	Professeur des Universités, Université Grenoble Alpes - ST-MARTIN-D'HERES

Composition du Jury :

Président :	Laurent NANA TCHAMNDA	Professeur des Universités, Université de Bretagne Occidentale, BREST
Examinateurs :	Jean-Philippe BABAU	Professeur des Universités, Université de Bretagne Occidentale, BREST
	Aurélien FRANCILLON	Professeur des Universités, EURECOM, Campus SophiaTech - BIOT
	Jérôme GENSEL	Professeur des Universités, Université Grenoble Alpes ST-MARTIN-D'HERES
	Michael HAUSPIE	Maître de conférences, IUT de Lille - VILLENEUVE-D'ASCQ

À Marianne et Morgan

Remerciements

Mes remerciements vont en premier lieu à l'ensemble des personnes qui ont contribué à ces travaux de recherche. Les recherches présentées ici n'ont jamais été réalisées seul et c'est d'ailleurs tout l'intérêt d'embrasser la carrière de chercheur : le travail en équipe, l'émulation et le partage de connaissances et compétences. Étudiants, doctorants, chercheurs, collègues et amis recevez toute ma gratitude. L'habilitation à diriger des recherches est une très bonne occasion pour montrer le fruit de ces années de partage et mettre en valeur ses co-auteurs.

Merci aux membres du jury : Jean-Philippe Babau, Aurélien Francillon, Jérôme Gensel, Michael Hauspie et Laurent Nana. Vos questions et remarques ont permis de soulever de nouvelles pistes de recherche passionnantes. Recevez toute ma gratitude d'avoir pris le temps d'évaluer ce travail et de m'avoir fait l'honneur d'être présent.

Écrire des remerciements est un passage obligé dans l'écriture d'un manuscrit. Il s'agit d'un exercice parfois difficile surtout s'il est mené comme un article de recherche [1]. Le risque est évidemment d'oublier une personne et d'oublier d'en oublier une autre. Mais oublions ce point et voici une liste non exhaustive des personnes avec lesquelles j'ai eu le plaisir et l'honneur de travailler : Alexandru, Arthur, Bastien, Christophe, Benjamin, Clet, Cyril, Damien, Douraid, Éric, Erwan, Étienne, François, Françoise, Guillaume, Hanan, Ines, Jacques, Jessica, John, Lamia, Maël, Mallorie, Marius, Mathias, Mathieu, Mickaël, Maxence, Mohamed, Nicolas, Olivier, Patrick, Pedro, Perrine, Quentin, Robin, Sébastien, Shoko, Thibaud, Thomas, Xavier et tant d'autres. Il manque tant de personnes que j'ai croisé et qui ont influencé ces travaux.

Je remercie également la Marine, l'école navale ainsi que la chaire de cyberdéfense des systèmes navals. Un grand merci aux services de l'école navale qui nous aident au quotidien dans nos missions de recherche.

La partie finale des remerciements est toujours celle qui porte le plus d'émotion. Merci à mes parents de m'avoir toujours soutenu, accompagner et guider. Vous ne saurez jamais à

1. Bastien Sultan. Maîtrise des correctifs de sécurité pour les systèmes navals. Thèse de doctorat. Chaire de cyberdéfense des systèmes navals, 2020.

quel point vous êtes importants pour moi. Merci à toute ma famille pour leur soutien et leur compréhension. Plus particulièrement à Gaby et mes enfants, Marianne et Morgan. Vous m'apportez tellement. Les enfants, l'écriture de ce manuscrit touche à sa fin et nous allons passer plus de temps ensemble. Enfin !

*

* *

Aucune raison de remercier un mode de transport cette fois-ci même maritime. Des propos sibyllins, mais je suis sûr qu'elle m'a porté chance.

*

* *

Table des matières

Table des figures

Liste des tableaux

Introduction

Durant ces années de recherche, plusieurs thématiques de l'informatique ont été abordées, notamment les sciences de l'information spatiale, les métaheuristiques, les systèmes multiagents, la théorie de l'information, l'analyse de cyberattaques ou la conception de cyber-ranges. La première étape de l'écriture d'un manuscrit d'habilitation à diriger des recherches, et sans doute la plus importante, est la mise en évidence du point commun des travaux de recherche, l'identification du fil directeur. Des systèmes d'information géographique à la génération de données pour l'apprentissage des sondes de détection de cyberattaques sur les systèmes navals, de nombreux concepts ont été utilisés. La figure 1 montre un nuage de mots réalisé à partir des publications écrites depuis le doctorat.

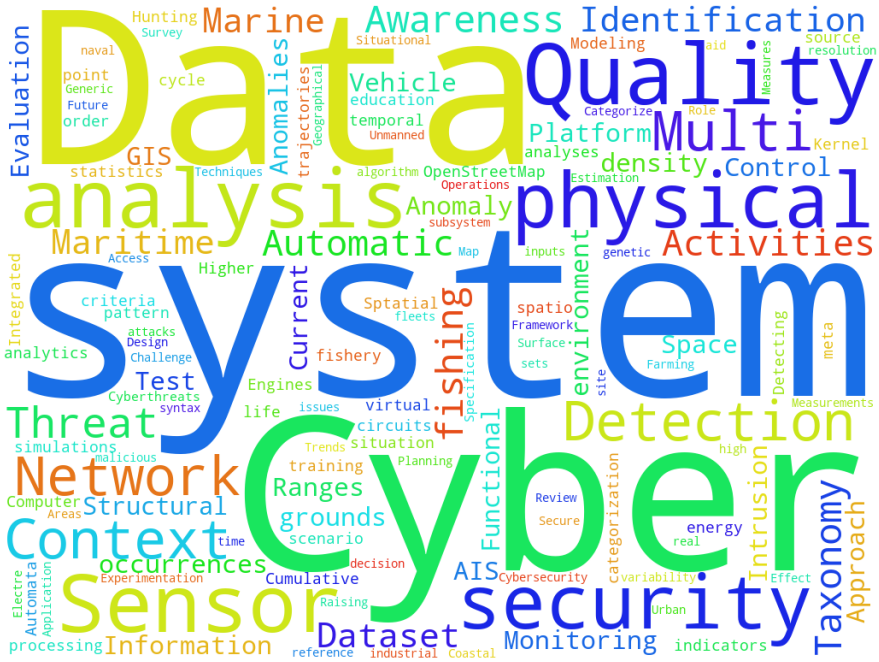


FIGURE 1 – Nuage de mots extraits des mots clés des articles publiés

Si les concepts sont nombreux, un point commun des recherches réalisées reste l'étude des activités humaines. En effet, des navigations pédestres en milieu naturel à la détection de cyberattaques sur des systèmes maritimes, il s'agit toujours d'activités humaines. Le thème des activités humaines est vaste et couvre un spectre de disciplines important et varié des sciences cognitives à la cybersécurité. Les objectifs des études sur les activités humaines dépendent bien sûr de la nature de l'activité concernée et de la discipline scientifique. Néanmoins, nous pouvons citer quelques grands objectifs :

— la compréhension des mobilités humaines ;
— la compréhension de phénomènes sociétaux ;
— la détection d'évènements ;
— la prévention de situations ;
— la simulation de phénomènes.

Afin d'y répondre, notre recherche s'est développée autour de divers terrains d'application pouvant se répartir en deux grandes catégories : le monde physique et le monde numérique.

Dans un premier temps nous nous sommes concentrés sur des activités dans le monde physique avec l'étude de descriptions de randonnées pédestres en milieu naturel et des mobilités urbaines. Ces activités sont composées de déplacements spatio-temporels qui peuvent être plus ou moins contraints par des réseaux structurant l'espace. Ces contraintes sont plus facilement identifiables dans les travaux menés sur les déplacements urbains multimodaux avec le réseau des rues et des lignes de transport en commun que pour les déplacements en milieu naturel.

Dans un deuxième temps, les problématiques se sont tournées vers les activités numériques et notamment dans le domaine de la cybersécurité. L'activité réseau sur Internet, les communications dans les systèmes cyberphysiques ou bien les messages réseau dans les systèmes industriels sont autant de données qui ont fait l'objet de travaux durant ces années de recherche.

Ainsi, nous considérons les activités humaines dans le monde réel ou dans le monde numérique de la même façon et nous en servons pour illustrer les trois domaines que sont l'acquisition, la modélisation et l'analyse d'activités humaines. Ce sont bien ces trois catégories qui découpent le manuscrit et non pas la chronologie des travaux de recherche effectués ou la nature de l'activité (humaine ou numérique).

Un point sur le concept d'activité, au cœur de ce manuscrit, doit être fait. La notion d'ac-

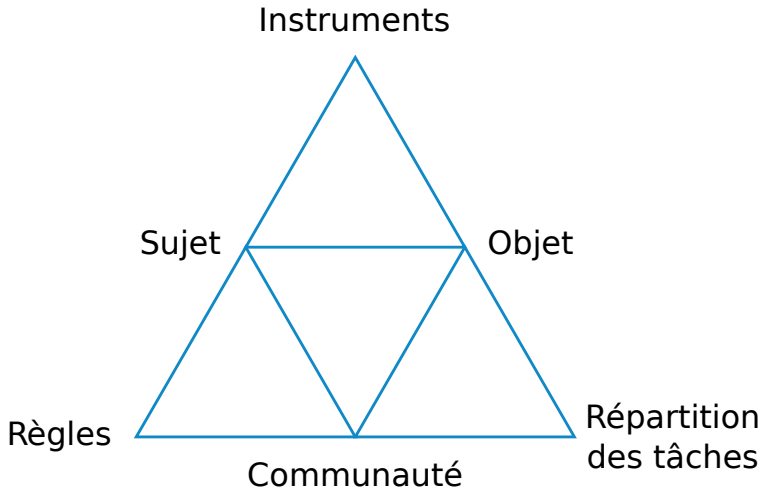


FIGURE 2 – Modélisation d'une activité selon (Eng87)

tivité repose tout d'abord sur la théorie de l'activité. Les premières approches de modélisation ont débuté en psychologie sur les principes d'exécution d'une activité (VC78 ; Leo78). La théorie de l'activité montre l'influence des facteurs environnementaux ainsi que l'objectif du sujet sur le déroulement de l'activité (Eng87 ; Eng01). En effet, une des premières modélisations était un triangle constitué du sujet, de l'objectif en passant par les instruments utilisés. Le modèle évolua avec la prise en compte des aspects culturels et sociétaux, indispensables à une meilleure compréhension des activités notamment dans le domaine de l'éducation et l'apprentissage (cf. Figure 2).

Six éléments constituent ce modèle :

— **Sujet** : Acteur engagé dans le processus ;
— **Objet** : Objectifs, buts recherchés par le sujet ;
— **Communauté** : Contexte social ou ensemble des acteurs impliqués dans le processus ;
— **Instruments** : Outils utilisés par les sujets et influençant leurs interactions ;
— **Répartition des tâches** : Division des activités entre les sujets ;
— **Règles** : Règles régissant les activités dans le système.

Un des points importants de cette théorie est la notion d'objectif ou de but. Sans prise en compte de ce critère, l'étude d'une activité est impossible. Une activité est considérée comme un ensemble d'actions humaines à mener pour atteindre un objectif. Différents acteurs peuvent intervenir dans la réalisation des activités et de nombreux outils externes sont utilisables par les acteurs. Des règles régissent les actions et peuvent être d'ordre social ou législatif. Une activité est donc liée à un objectif conscient et une motivation. Elle mène à

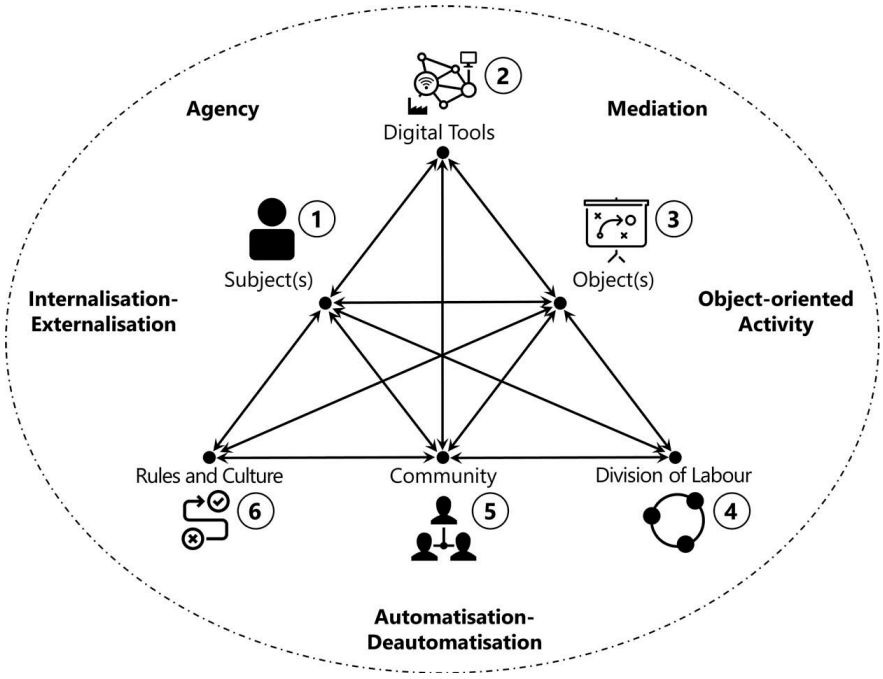


FIGURE 3 – Théorie de l'activité adaptée aux outils numériques (Bla19)

l'exécution de différentes actions.

Qu'il s'agisse d'activités dans la réalité ou dans le monde numérique, la théorie de l'activité permet de modéliser et comprendre les processus en jeu. Elle permet également de construire des protocoles expérimentaux d'acquisition de données plus cohérents avec la prise en compte par exemple d'objectifs bien définis ou l'engagement des acteurs.

L'utilisation de systèmes numériques a modifié la modélisation des activités (OP13). L'adaptation de la théorie pour prendre en compte les nouveaux usages, numériques, particulièrement dans le domaine de l'apprentissage, a été réalisée par (Bla19). La figure 3 montre les modifications apportées comme les *outils numériques* ainsi que les sept dynamiques (*Agency, Mediation, Object-oriented Activity, Automatisation, Deautomatisation, Internalisation, Externalisation*).

Les activités humaines sont également des trajectoires spatio-temporelles. Ce lien entre espace et temps complexifie les études, car étudier l'un sans l'autre n'a pas de sens. Torsten Hägerstrand, avec le domaine de la Time Geography, est un nom incontournable lorsque l'on aborde la relation entre ces deux dimensions (Häg70). La définition du domaine Time Geography selon l'encyclopédie des SIG est la suivante (Mil08) : *"Time geography is an individualistic, bottom-up approach to analyzing and simulating human phenomena such as*

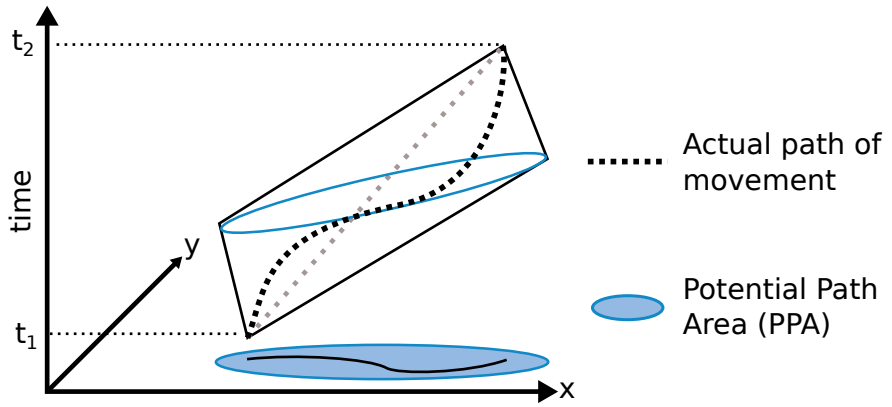


FIGURE 4 – Prisme spatio-temporel (Häg70)

transportation, urban and socio-economic systems. Time geography examines how humans allocate scarce time resources among activities in geographic space, the use of transportation and communication technologies to facilitate this allocation, and the patterns and relationships that emerge from these allocations across the population. "

Le prisme spatio-temporel provenant de cette théorie permet une visualisation pertinente d'un déplacement et des régions spatiales et des intervalles temporels en interaction. La figure 4 illustre cette représentation.

Ces théories et concepts ont permis de travailler sur différentes activités dites réelles ou numériques. De plus en plus, les activités dans le monde réel sont reliées à des activités numériques. Ce mélange de nature d'activités réelles/numériques ou l'utilisation de systèmes numériques dans la médiation de l'activité est de plus en plus important et concerne de nombreux domaines comme les communications, l'éducation, la santé, l'interaction homme-machine, les sciences de l'information, la gestion de l'information ou la conception de systèmes (KNSM21).

L'essor des objets connectés et plus particulièrement des montres d'activités illustre parfaitement ce phénomène. Ces montres de sport permettent de mieux s'entraîner en connaissant plus de paramètres sur ses activités et ses performances, mais elles peuvent également alimenter d'autres activités numériques avec le partage automatique d'informations sur les réseaux sociaux. Ainsi une activité sportive peut également déclencher une activité de publication sur les réseaux sociaux. Cette double activité n'est parfois pas maîtrisée ou mal maîtrisée et peut conduire à rendre publiques des informations sensibles. Ainsi, des itinéraires de courses à pied autour de bases militaires ont été rendus publics sur des plateformes sportives telles que Strava ou Polar permettant de localiser ces bases et parfois d'identifier

précisément les personnes (Bur18). Une activité dans le monde réel peut ainsi se propager (volontairement ou non) dans le monde numérique, engendrant potentiellement des risques de confidentialité. Cela a donc amené nos recherches, au cours de ces dernières années, à prendre naturellement le chemin de la cybersécurité.

Différentes expérimentations ont été réalisées dans les travaux. Le chapitre I porte sur l'acquisition de données en décrivant plus en détail le cyberrange maritime qui a été conçu ces dernières années pour permettre la production de données numériques maritimes utiles à la recherche. En effet, si les phases d'acquisition de données furent pour la majorité des travaux la première étape de recherche, le cyberrange maritime est au cœur d'un projet européen dont les perspectives et applications sont nombreuses.

Avoir à disposition des données réelles (ou proches de la réalité) est indispensable pour la recherche, mais trop souvent très complexe à réaliser. L'essor de l'IA (un nième pour être juste) et surtout celui de l'apprentissage profond ont mis en lumière une des grandes difficultés de ce type de méthode à savoir la quantité et qualité (correctement catégorisées avec étiquettes) des données nécessaires à leur mise en œuvre.

Ces données doivent être ensuite modélisées. Différentes approches ont été utilisées avec la théorie des graphes comme base commune. Le chapitre II explique cette approche de modélisation pour différentes applications.

L'analyse des informations modélisées est le sujet du chapitre III. Quatre analyses ont été choisies pour illustrer les approches développées :

— la géolocalisation de descriptions d'itinéraire ;
— la génération de cartes schématiques ;
— l'analyse de cyberattaques ;
— la détection d'anomalies dans les systèmes cyberphysiques.

Un chapitre est enfin consacré à la conclusion et aux perspectives de travail qui sont nombreuses dans chacune des trois catégories de travaux (acquisition, modélisation et analyse). Notre conclusion s'attachera à dessiner les contributions possibles dans ce domaine, en cohérence avec les travaux présentés dans ce manuscrit.

Chapitre I

Acquisition de données

Sommaire

Un des tout premiers défis dans la plupart des actions de recherche est l'obtention de données. Ces données quelle que soit leur nature, doivent être pertinentes, c'est à dire utilisable pour les travaux de recherche, de qualité et en quantité suffisante.

La pertinence, dans notre recherche, concerne la bonne adéquation entre les hypothèses et questions de recherche à traiter avec les données. Nous parlons ici de forme des données (formats, types) et également de représentativité. Ce critère est fortement lié à la source même des données. Par exempe, dans le cas de données sur les communications réseau, une grande différence existe entre une matrice de conversations entre serveurs sur Internet et un jeu de données contenant une capture de l'ensemble des échanges réseau avec les données transmises sur un réseau d'entreprise. Évidemment, nous pouvons décliner un nombre très important de types de données entre ces deux exemples en faisant varier par exemple la précision ou l'échantillonnage. Nous commençons alors à discuter de qualité de données. La qualité des données, au plutôt la qualité de l'information, car une donnée est utilisable

une fois qu'elle est transformée en information, est complexe à manipuler. Les thèses de doctorat de Pedro Merino Laso (ML17) et Olivier Jacq (Jac21) consacrent des chapitres entiers à la définition et à la quantification de la qualité d'information dans des contextes d'analyse de cyberattaques pour les systèmes cyberphysiques maritimes. Enfin, la quantité de données est un critère naturellement important pour toute recherche. Sans une quantité de données importante, il est impossible de tirer la moindre conclusion pertinente, tout au mieux des tendances "observées lors de ces tests préliminaires, mais qui restent à confirmer par des expériences utilisant des jeux de données conséquents et pertinents". Cet argument fait partie des plus utilisés dans les publications scientifiques (tous domaines confondus) montrant l'importance de la quantité de données et surtout leur difficulté d'acquisition.

Pour obtenir les données "idéales" pour un projet de recherche précis, plusieurs solutions existent :

1. Les obtenir immédiatement, car elles font partie du problème de recherche. Cependant, la qualité et/ou la quantité trop importantes peuvent être des obstacles scientifiques à surmonter.
2. Trouver des données libres et en accès ouvert. Cette stratégie, il faut l'avouer, n'est jamais très efficace même si c'est la première à tester. L'achat de données est également une possibilité. Il est ainsi possible d'avoir la quantité et la qualité des données que l'on souhaite.
3. Enfin une dernière solution est de générer les données pour le projet de recherche. Pour certains domaines et certaines thématiques de ces domaines, il s'agit d'une solution tout à fait viable et parfois même la seule, car elle permet de maîtriser des biais qu'il serait impossible d'éliminer de jeux de données réelles.

Par ailleurs, il est essentiel de parler de la différence entre données issues d'études rétrospectives et celles provenant d'études prospectives. Les données provenant d'expériences rétrospectives sont à manipuler avec précaution. Outre le fait que le protocole expérimental ne soit pas toujours entièrement explicité, le jeu de données peut contenir des critères de confusion qu'il sera difficile de contrôler. L'analyse de ce type de données peut faire face au paradoxe de Simpson et produire des conclusions totalement erronées. En effet, certains paramètres peuvent être des facteurs de confusion sans qu'il soit possible de le déterminer par manque de connaissances sur les données étudiées. Ainsi il est toujours préférable de construire son propre protocole expérimental dans le cadre d'une étude prospective.

Dans ce chapitre nous allons détailler quatre exemples d'acquisition de données pour trois stratégies différentes. Le premier exemple est la mise en place d'une expérience de

navigation pédestre. Les trois autres exemples concernent des données de communication de réseau informatique avec la mise en œuvre d'un Honeypot et la génération de données par réseau virtuel puis avec la création d'un cyberrange maritime.

I.1 Descriptions d'itinéraires

Notre recherche concernant le milieu naturel, une expérimentation fut réalisée afin de faire ressortir les ressemblances et les différences entre navigations en environnement naturel (Bro08) et urbain (Den97 ; PM04). Le cadre choisi fut la course d'orientation pour obtenir des descriptions dans un milieu le plus naturel possible,*i.e*, ne suivant peu des routes et avec peu de références de bâtiments. La course d'orientation est une pratique sportive pouvant être pratiquée selon plusieurs modalités (à pied, à cheval, en ski ...) dont l'objectif est de suivre un itinéraire précis dont les étapes sont matérialisées par des balises qui permettent aux concurrents de valider leur passage. Ce sport comptant plus de 70 fédérations internationales est reconnu comme pratique sportive par le Comité International Olympique. La fédération française de course d'orientation (`http://www.ffcorientation.fr`) compte moins de 10 000 licenciés ce qui la classe comme une petite fédération sportive.

Une des particularités de la course d'orientation est le type des cartes utilisées en repérage pour localiser les balises. L'échelle peut aller jusqu'au 1/5000 et la légende est extrêmement précise concernant la végétation et le relief entre autres (Figure I.2). Pour la végétation, la légende contient des informations sur comment le coureur peut la traverser. Ainsi, ces cartes contiennent déjà des éléments utiles pour la description de dynamiques. La figure I.1 montre quelques exemples de forêts avec la légende de course d'orientation associée.

Une expérimentation fut organisée afin de collecter des descriptions verbales d'itinéraires pendant une course à pied. Le protocole était relativement simple, les coureurs décrivaient le parcours entre deux balises spécifiques à l'arrivée. Ces descriptions ont ensuite été utilisées pour les comparer à celles disponibles dans des travaux similaires.

Le tableau I.1 présente les caractéristiques des trois expérimentations. L'originalité de nos travaux est de s'intéresser à un environnement naturel tandis que les expériences menées par (Den97 ; PM04) étaient en environnement urbain. Cette différence d'environnement n'est pas anecdotique, car il a fallu identifier un cadre de pratique, la course d'orientation, et un terrain expérimental identique, le campus de l'école navale, pour obtenir des descriptions d'itinéraire comparables.

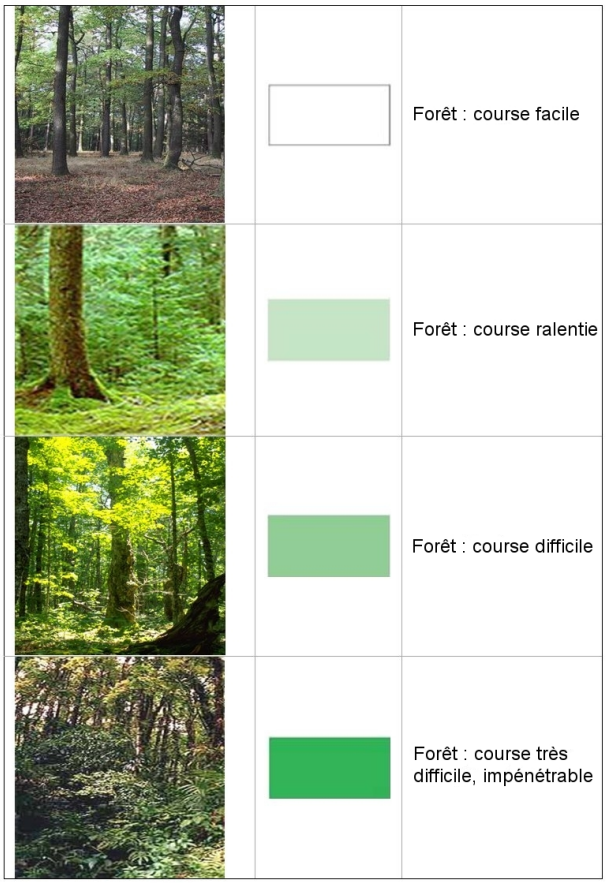


FIGURE I.1 – Végétation et degré de pénétrabilité

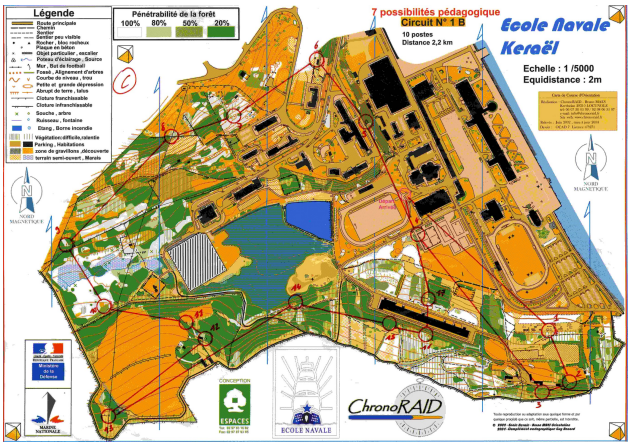


FIGURE I.2 – Exemple d'une carte de course d'orientation

Cette première approche d'acquisition de données consistait à identifier un protocole original pour collecter des descriptions d'itinéraire. L'originalité de cette approche vient du type d'environnement étudié. En effet, les itinéraires en environnement naturel sont peu étudiés. Le faible nombre de descriptions obtenues, qui restent comparables à ceux de la littérature, ainsi que l'absence de profils d'utilisateurs (pour conserver une bonne acceptation des participants) sont les points à améliorer prioritairement.

TABLE I.1 – Caractéristiques des expérimentations

Expérimentation	**Type de descriptions recueillies**	**Environnement**	**Nombre de participants**
(Den97)	Descriptions orales	Environnement urbain	20
(PM04)	Descriptions textuelles	Environnement urbain	46
(Bro08)	Descriptions orales	Environnement naturel	14

I.2 Traces réseau

L'obtention de traces réseau exploitables se heurte à plusieurs obstacles. Tout d'abord, ces traces sont différentes en fonction des réseaux à étudier (réseau d'entreprise, trafic Internet). Avoir recours à de la simulation est pertinent, mais reste encore perfectible, comme la simulation du trafic Internet rendue difficile de par la taille du réseau, l'hétérogénéité des machines et les dynamiques complexes des comportements (FP01 ; Fer17 ; Sha20).

Les comportements observables dans une capture réseau sont de deux types : un comportement dit "normal" et un comportement "anormal" incluant des cyberattaques ou des tentatives de cyberattaques. Une difficulté majeure est de faire émerger des caractéristiques salientes dans les échanges réseau pour identifier les échanges normaux, appelé "network baseline" en investigation numérique (DH12).

Notre objectif est d'obtenir des traces réseau reflétant un trafic de type *"network baseline"* pour une configuration donnée. Cela correspond à une régularité des échanges réseau sur une période de temps d'un point de vue ports utilisés, taille des paquets, volume du trafic ou encore nombre d'adresses communicant.

La première méthode que nous avons utilisée est la technique du Honeypot installé sur plusieurs serveurs afin de recueillir les interactions réseau. Il s'agit d'une approche passive. Dans la deuxième approche, des réseaux ont été simulés, mais aussi attaqués pour obtenir des traces réseau de manière contrôlée.

I.2.1 Honeypots

Le concept de Honeypot a été inventé à la suite de la découverte d'une intrusion dans un système informatique dans les années 1990. Clifford Stoll a conçu un réseau à part pour piéger l'attaquant et l'identifier (Sto05). Il s'agit d'un système informatique (réel ou virtuel) ayant pour but premier de leurrer des attaquants afin qu'ils ne s'intéressent pas aux machines importantes (ANK+06). Dès le débuts des années 2000, plusieurs honeypots (deception toolkit) sont disponibles et plusieurs projets importants voient le jour comme le projet *leurré.com* (ADD+05 ; GK12).

Les honeypots sont utilisés à d'autres fins que piéger les attaquants potentiels pour les empêcher de nuire. Ils peuvent être utilisés à des fins de recherches pour améliorer la connaissance sur la menace cyber en collectant des données comme les méthodes d'attaques (Tactics and Technics) utilisés. Pour leurrer les attaquants, ces systèmes doivent ressembler le plus possible à de vrais systèmes en production. Il existe ainsi des honeypots dédiés aux systèmes industriels comme Conpot (`https://github.com/glastopf/conpot`). Ce programme permet de simuler plusieurs protocoles industriels pour concevoir un honeypot sur mesure d'un système industriel complexe. Des techniques de gamification peuvent être couplées à ces honeypots de déception pour encourager les attaquants à continuer de s'intéresser uniquement aux ressources non critiques (BJH+19).

Les honeypots peuvent être classés en trois catégories :

— faible interaction : pas de système d'exploitation, seuls certains services sont simulés. Le projet Conpot est un honeypot à faible interaction. Ces honeypots peuvent leurrer des scans, mais pas des attaques plus complexes.

— moyenne interaction : pas de système d'exploitation, mais les services simulés sont plus complexes et le leurrage plus avancé.

— forte interaction : il s'agit de machines complètes avec systèmes d'exploitation et de vrais services exécutés. Plus réalistes, ils demandent à être surveillés et la connexion à des systèmes en production est déconseillée. Ils sont le plus souvent utilisés en recherche pour la collecte d'informations (ADD+05 ; NWS+16).

En interconnectant plusieurs honeypots, le réseau obtenu est appelé Honeynet. Cela permet de créer une infrastructure complexe qui constitue un leurre efficace.

Dans le cadre d'une expérimentation, nous avons installé 5 honeypots à forte interaction repartis dans le monde : Frémont, Newark aux États-Unis, Londres, Singapour et Tokyo (Figure I.3). Les emplacements ont été choisis en fonction des possibilités du fournis-

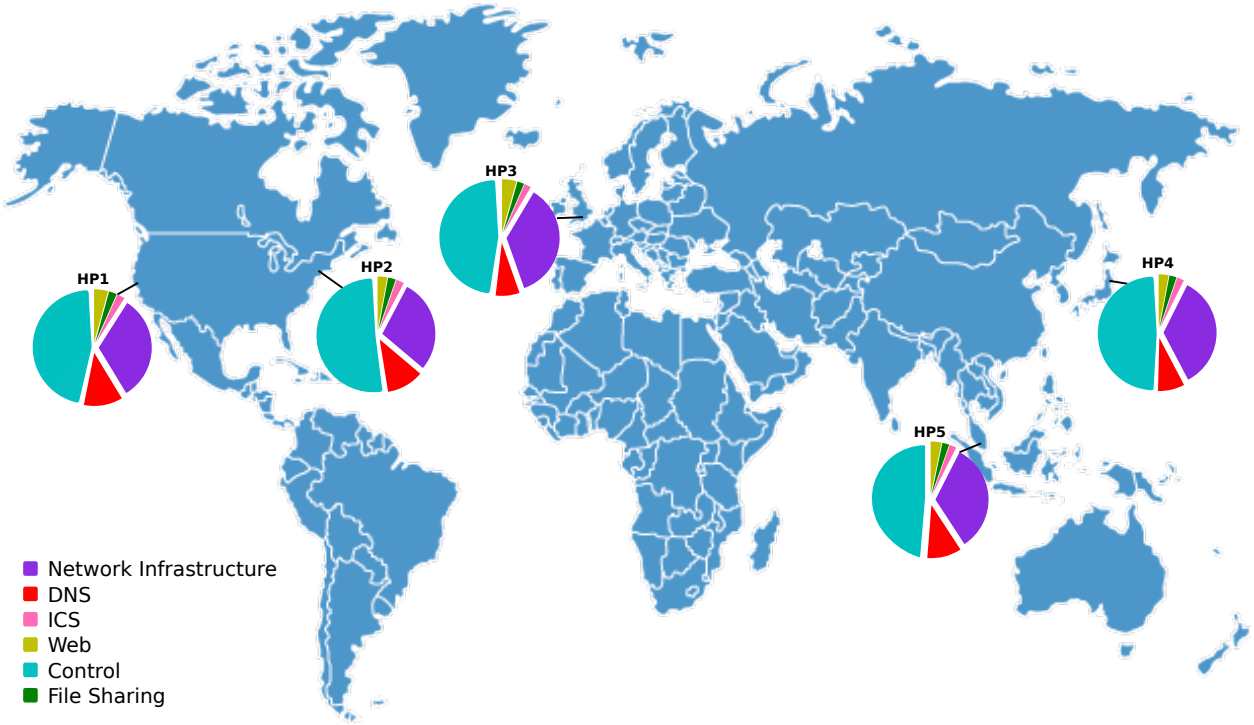


FIGURE I.3 – Honeypots Places

seur de serveurs et pour avoir des emplacements géographiques variés ce qui peut générer des différences dans les traces réseau obtenues (architecture réseau, technologie, filtrage nationaux, etc.)

Pour obtenir des jeux de données comparables sur chaque honeypot, la même configuration a été déployée au même moment. L'installation est la suivante : Ubuntu 16.04, un serveur SSH (openSSH), un serveur FTP (Pure-ftpd) et un serveur Web (Apache2). Le serveur Web héberge une page d'authentification avec un script PHP pour suivre les tentatives de connexion. Aucun nom de domaine n'a été acheté et l'adresse publique des serveurs n'a pas été communiquée ni ne fait pas partie de listes noires à notre connaissance. Tous les messages réseau capturés ont été stockés dans un fichier. L'expérience s'est déroulée pendant un mois et a généré 10Gb de données.

Les caractéristiques des honeypots sont données dans le tableau I.2. La première ligne représente le nombre d'adresses IP distinctes qui ont établi une connexion avec les pots de miel. La deuxième ligne représente le nombre de paquets réseau échangés entre le pot de miel et les attaquants. La troisième ligne indique le nombre de protocoles utilisés pour chaque serveur. La dernière ligne du tableau I.2 indique le nombre de pays depuis lesquels

les attaquants ont opéré en géolocalisant les adresses IP à l'aide de l'API GeoIP basée sur la base de données gratuite GeoLite `https://dev.maxmind.com/geoip/legacy/geolite`.

TABLE I.2 – Statistiques sur les Honeypots

	HP1	HP2	HP3	HP4	HP5
Adresses IP	13.677	23.061	25.458	32.229	23.861
Paquets	2.847.243	9.678.783	9.434.139	10.299.219	10.706.896
Protocoles	41	47	59	48	44
Pays	245	246	241	281	243

Cette méthode d'acquisition de données consistait à déployer des serveurs vulnérables dans différents datacenters répartis géographiquement. Les serveurs ont été choisis et entièrement configurés permettant d'avoir le contrôle complet sur l'expérimentation. L'utilisation d'Honeypots permet d'obtenir rapidement des quantités de données intéressantes pour le renseignement sur la menace par exemple. Néanmoins, cette facilité a un coût, celui d'avoir dans les enregistrements de nombreuses actions automatiques (scan) qui ne reflètent pas des actions humaines.

I.2.2 Génération de traces par simulation de réseaux

Les analyses faites sur des traces réseaux issues de serveurs vulnérables nous ont permis de mettre en évidence le caractère déterministe des comportements observés qui s'explique par le nombre important de comportements automatisés comme les scans permanents. La question qui a émergé suite à ces travaux est celle de la génération de traces réseau par simulation de comportements. L'objectif est de produire des traces réseau réalistes pour différents usages notamment l'entraînement de sondes de détection de cyberattaques.

Deux approches ont été définies. La première est à base de scénarios avec des actions qui s'enchaînent selon un script bien défini. La deuxième en cours de développement utilise des approches de simulation multiagents avec une part d'aléatoire qui manque à la première. Les deux approches ont pour point commun la production de données réseau parfaitement étiquetées, c.-à-d. dont les actions sources des messages réseau sont connues et enregistrées. Cette caractéristique permet de pouvoir réaliser de la classification avec des données correctement étiquetées.

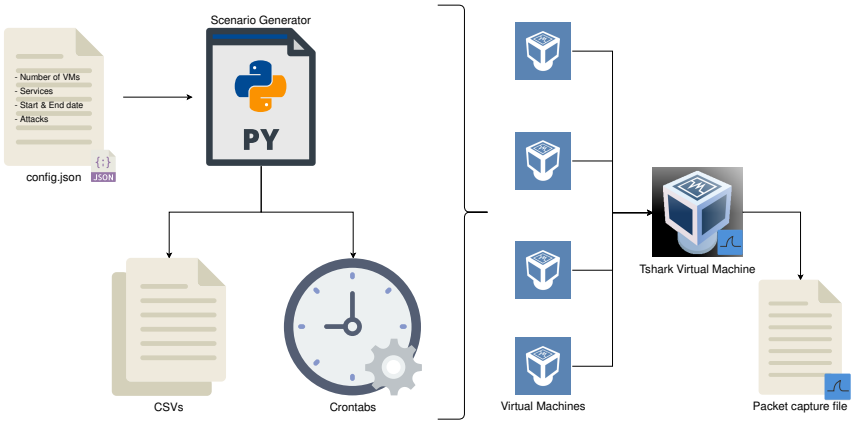


FIGURE I.4 – Architecture de génération de traces réseau (NBH+19)

Approche par scénarios

La figure I.4 présente l'architecture de l'approche par scénarios. Cette approche repose sur la création d'une liste de comportements parmi ceux définis dans un fichier de configuration.

Les scénarios sont donc créés aléatoirement parmi les actions possibles précisées dans la configuration. Le réseau virtuel peut ensuite être créé avec les différentes machines virtuelles ou physiques. Les fichiers planifiant les actions à effectuer sont également créés à cette étape. Déployés sur l'ensemble des machines, ces fichiers permettront l'exécution des actions définies dans le scénario à l'instant précis spécifié. Enfin, les traces réseau sont enregistrées formant un ensemble de données entièrement étiquetées. Cet ensemble de données peut être utilisé pour différents objectifs, mais le but principalement envisagé est l'entraînement de sondes de détection d'intrusion réseau comportementales (NIDS comportementaux).

Pour la génération de données spécifiques à l'entraînement des NIDS comportements, des machines de type attaquant peuvent être intégrées dans le scénario. Les actions de ces machines sont également étiquetées afin d'identifier précisément les attaques dans le réseau. Les attaques sont définies par la spécification de commandes avec paramètres, ce qui permet une grande liberté dans les attaques possibles et outils utilisables.

Les attaques produites sur le réseau virtuel déployé génèrent un trafic qui peut être conséquent ou bien en dessous du nombre de paquets considéré dans le "network baseline" (Figure I.6). En fonction des paramètres utilisés pour les commandes de scan réseau, le trafic généré est très différent (Figure I.5).

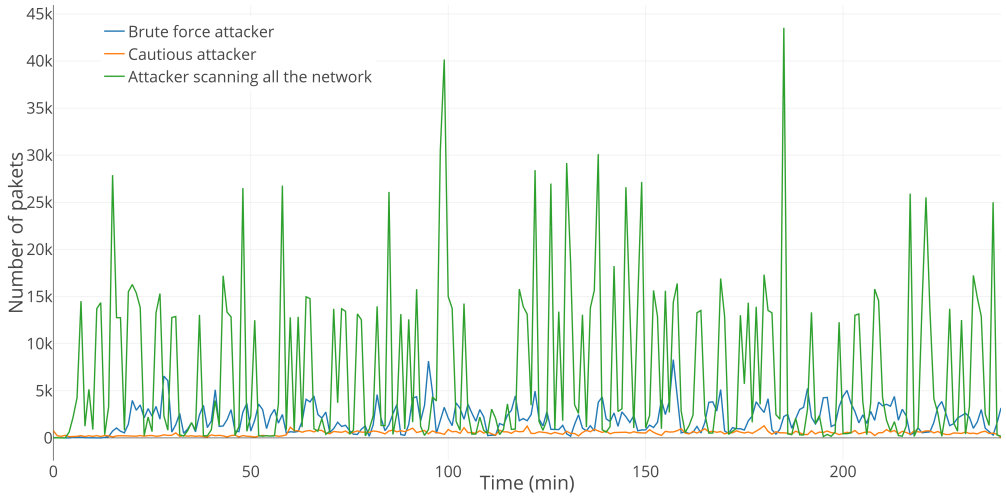


FIGURE I.5 – Différence du nombre de paquets entre différentes attaques (NBH+19)

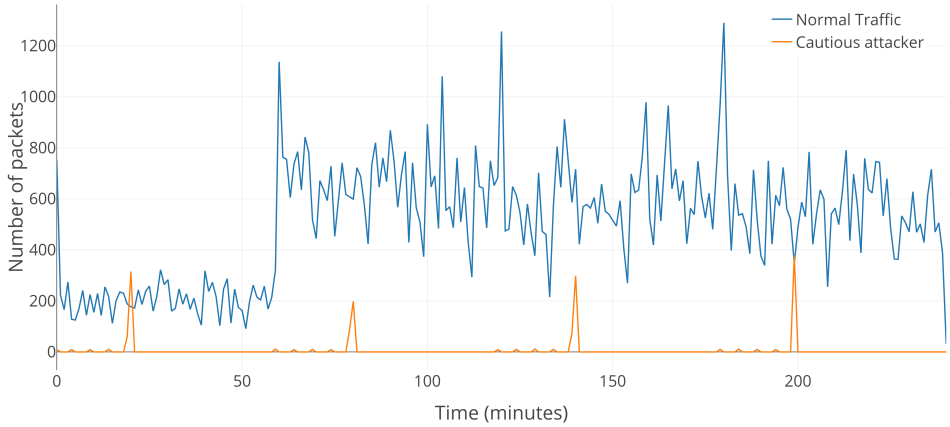


FIGURE I.6 – Scan réseau en mode paranoïaque (NBH+19)

Approche par agents

L'approche de simulation réseau par agents consiste à avoir des comportements utilisateurs avec une part aléatoire plus importante et qui peuvent être plus réalistes. Chaque machine virtuelle ou physique exécute un programme "agent" qui contient un ensemble d'actions à exécuter.

Comme tout simulateur multiagent, l'aléatoire a un rôle important. C'est également le cas dans notre approche par agents dans laquelle sont définies des probabilités de réaliser une action. Le principe retenu est celui de la roue biaisée. Le code I.1 montre comment sont définies les proportions d'actions pour l'agent *passager* défini plus haut.

Listing I.1 – Exemple de configuration d'un agent

```
{

  "14:00-18:00": {
    "web": {
      "bias": 0.59,
      "combo_max": 10,
      "wait_time": 30
    },
    "mail": {
      "bias": 0.1,
      "combo_max": 1,
      "wait_time": 1
    },
    "social": {
      "bias": 0.25,
      "combo_max": 10,
      "wait_time": 10
    },
    "games": {
      "bias": 0.05,
      "combo_max": 50,
      "wait_time": 1
    },
    "technical": {
      "bias": 0.01,
      "combo_max": 1,
      "wait_time": 10
    }
  }
}
```

La différence avec l'approche par scénario est que les actions sont choisies de manière aléatoire. Chaque action exécutée doit par contre être consignée dans un fichier sur chaque machine afin d'avoir l'historique des actions pour étiqueter les traces réseau.

Une autre amélioration en développement est la simulation des actions utilisateur par le contrôle de la souris et du clavier. Certaines librairies, comme *PyAutoGUI* en python, permettent d'enregistrer des sessions d'interactions souris/clavier et de les rejouer. La plus-value la plus intéressante de ce type de simulation est pour la navigation WEB. La librairie *selenium* donne la possibilité d'interagir avec des pages web pour remplir des formulaires, cliquer sur des liens ou récupérer des informations affichées.

Pour la partie permettant d'effectuer automatiquement des attaques, deux méthodes sont envisagées. La première consiste à réaliser un ou plusieurs agents fonctionnant de façon identique aux agents classiques du réseau. La deuxième méthode, plus évoluée au niveau

de la complexité des attaques possibles, utilise des plateformes de simulation d'attaques. Plusieurs outils existent tels que :

— Caldera `https://github.com/mitre/caldera` ;
— Infection Monkey `http://www.guardicore.com/infectionmonkey/` ;
— NeSSi2 `http://www.nessi2.de/index.html` ;
— Foreseeti `https://foreseeti.com/` ;
— SCYTHE `https://www.scythe.io/` ;
— uber metta `https://github.com/uber-common/metta`.

L'outil Caldera développé par l'organisme MITRE est un outil très complet pour mener des tests d'attaques et a été choisi pour la simulation d'attaques. Il fonctionne avec une architecture client-serveur dans laquelle les clients sont les victimes à tester (nommées agent dans Caldera) et le serveur est la machine sur laquelle est installée Caldera. Ce serveur est administré par une page web qui permet de générer les configurations des agents à déployer en fonction du serveur et du système d'exploitation des machines cibles (Windows, macOS et Linux supportés).

La méthode d'acquisition de données réseau par simulation permet d'obtenir une richesse d'actions humaines bien plus importante que l'utilisation d'Honeypots. La méthode par agents utilisant des outils de simulation d'attaques est en cours de conception et devrait donner des enregistrements réseau plus réalistes. Les biais et les signaux "parasites" dus aux outils et à la virtualisation devront cependant être étudiés pour ne pas être utilisés malencontreusement comme attributs par les algorithmes d'apprentissage utilisant ces données.

I.3 Génération d'anomalies

Une autre méthode d'acquisition de données a été réalisée en s'intéressant aux capteurs des systèmes industriels. L'émergence des systèmes cyberphysiques (Cyber Physical Systems en anglais) permet d'obtenir de nombreuses données provenant de capteurs ou d'actionneurs variés. Les travaux menés pour le développement de méthodes de détection d'anomalies dans les CPS ont débuté par la mise en place d'une campagne d'acquisition de mesures (MLBP17b ; MLBP17a ; ML17 ; PMLB18).

Le système étudié est composé de deux cuves remplies d'eau, d'un ensemble de capteurs, de deux pompes et d'un automate contrôlant le processus industriel (Figure I.7).

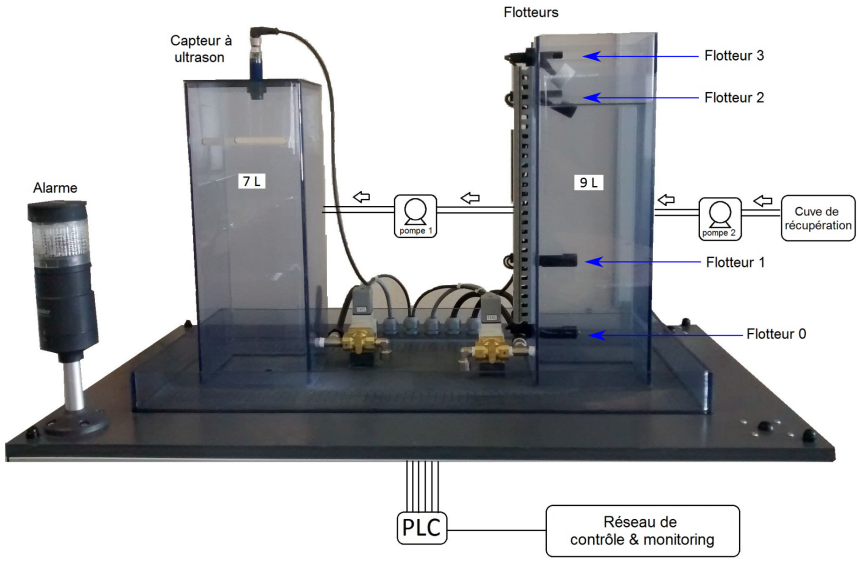


FIGURE I.7 – Système expérimental composé de deux cuves (ML17)

Les données, mises à disposition de la communauté scientifique, sont un ensemble de séries temporelles pour différents cas :

— Utilisation normale ;
— Situation comportant des anomalies ;
— Situation avec des pannes matérielles ;
— Présence de sabotages ;
— Présence de cyberattaques.

Plus précisément 9 situations ont été définies :

— Deux cas de sabotage avec différents objets dans les cuves : lorsqu'un **Sac en plastique** et une quantité variable d'**objets flottants** apparaissent dans la cuve.
— Une anomalie avec une feuille en papier bloquant le capteur à ultrason.
— Des objets bloquants les capteurs de niveau
— Une cyberattaque de type déni de service
— Une autre cyberattaque de type ***spoofing***, envoyant de fausses informations.
— Des vibrations importantes sur les cuves.

Le tableau I.3 donne les caractéristiques des différents fichiers produits lors de l'expérience. Ces fichiers sont de petite taille pour permettre de tester rapidement différentes approches de détection. Ils doivent être utilisés en première phase de test avant de tester la méthode choisie avec des fichiers de grande taille spécifiques aux systèmes à protéger. Ils peuvent par exemple servir à comparer des algorithmes d'apprentissage ainsi que leurs

TABLE I.3 – Caractéristiques des enregistrements produits

Scénario	**Sous-système affecté**	**Type d'événement**	**Durée**	**Taille**
Normal	Aucun	Normal	02 :01 :47	7.3 MB
Sac en plastique	Capteur à ultrason	Accident / Sabotage	00 :33 :20	4.2 MB
Mesure bloquée 1	Capteur à ultrason	Panne / Sabotage	00 :00 :25	74 KB
Mesure bloquée 2	Capteur à ultrason	Panne / Sabotage	00 :00 :17	48 KB
Objets flottants - cuve principale (2 objets)	Capteur à ultrason	Accident / Sabotage	00 :01 :35	272 KB
Objets flottants - cuve principale (7 objets)	Capteur à ultrason	Accident / Sabotage	00 :01 :22	234 KB
Humidité	Capteur à ultrason	Panne	00 :00 :18	52 KB
Panne du flotteur 1	Flotteur 1	Panne	00 :13 :55	1.8 MB
Panne du flotteur 2	Flotteur 2	Panne	00 :03 :40	610 KB
Attaque de déni de service (DoS)	Réseau	Cyberattaque	00 :01 :37	102 KB
Spoofing	Réseau	Cyberattaque	00 :34 :33	3.2 MB
Mauvaise connexion	Réseau	Panne / Sabotage	00 :15 :33	1.7 MB
Coups sur les cuves (intensité basse)	Tout le sous-système	Sabotage	00 :00 :39	112 KB
Coups sur les cuves (intensité moyenne)	Tout le sous-système	Sabotage	00 :00 :32	91 KB
Coups sur les cuves (intensité haute)	Tout le sous-système	Sabotage	00 :00 :33	95 KB

réglages.

Pour obtenir des données encore plus réalistes et surtout provenant de systèmes industriels, nous avons utilisé une plateforme expérimentale qui reproduit un processus industriel. Les anomalies sont simulées, mais sont suffisamment réalistes pour produire des enregistrements utilisables par des méthodes de détection. Si la plateforme est petite, elle permet de produire des données caractéristiques d'un système industriel sans générer de biais important comme pourrait le faire un système en production plus important spécialisé dans un métier.

I.4 Cyber range maritime

Afin d'obtenir des données toujours plus réalistes et proches de vrais systèmes industriels en production, nous avons commencé à élaborer des plateformes plus complexes. Une première réalisation s'est intéressée à deux sous-systèmes d'un navire : la propulsion et la barre (BBB+17). Deux automates industriels, dédiés chacun à un sous-système, un coordinateur central ainsi qu'un ensemble de microcontrôleurs simulant des capteurs et des actionneurs composent la plateforme. Bien que simple, cette plateforme a permis de tester différentes attaques et de collecter des données originales.

La volonté d'avoir des données plus réalistes et en plus grande quantité nous a amenés à concevoir une plateforme simulant le réseau industriel d'un navire qui s'est transformée au fil des ans en un véritable cyberrange maritime.

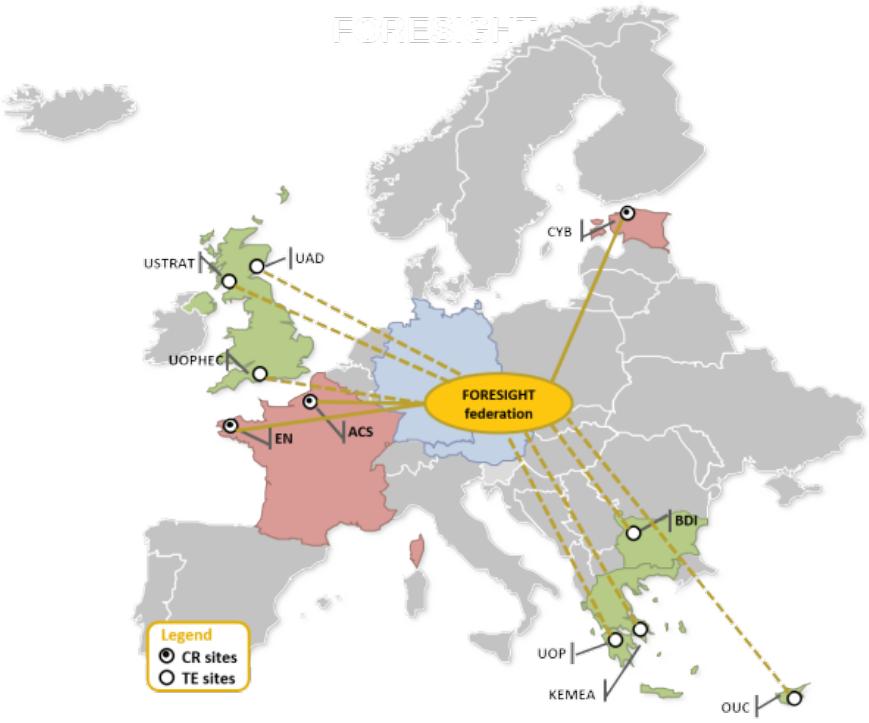


FIGURE I.8 – Consortium du projet européen FORESIGHT

Ce cyberrange maritime fait partie des trois plateformes d'entraînement à la cybersécurité du monde industriel du projet FORESIGHT (`https://foresight-h2020.eu/`). Le consortium est composé de 23 membres académiques et industriels de 7 états européens différents (Figure I.8).

L'objectif de ce projet européen est la création d'une fédération de cyberranges et de plateformes d'entraînement en cybersécurité industriel avec trois domaines d'étude spécifiques :

— La cybersécurité des réseaux électriques ;
— La cybersécurité des aéroports ;
— La cybersécurité des navires.

La figure I.9 illustre l'architecture globale du projet en montrant les différentes interactions entre les plateformes. En effet, un des points importants du projet est la fédération des infrastructures d'apprentissage permettant la construction de parcours pédagogiques originaux et complexes.

Dans un premier temps nous allons détailler l'architecture du cyberrange d'un point de vue réseau puis la partie simulation de navigation sera expliquée. La génération de données sera illustrée par une première expérimentation dans la dernière section.

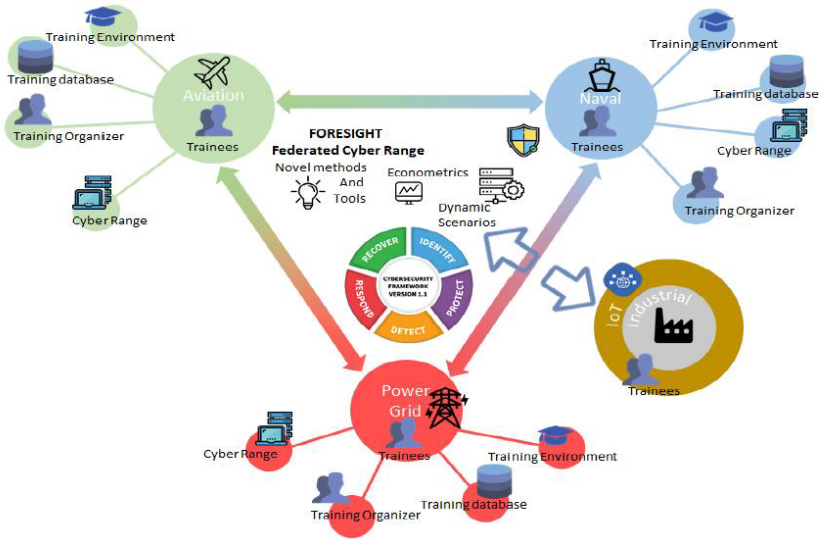


FIGURE I.9 – Architecture globale du projet européen FORESIGHT

I.4.1 Architecture

Le cyberrange maritime est basé sur l'architecture réseau d'un navire de type passager (de taille moyenne avec moins d'une centaine de personnes à bord) avec une structuration en 4 couches selon le modèle Purdue Enterprise Reference Architecture, appelé simplement modèle de Purdue (Wil94). Ce modèle est une référence dans le domaine des systèmes de contrôle industriel depuis les années 90. Il consiste à segmenter l'architecture en couches fonctionnelles.

Le navire simulé est constitué des couches suivantes (I.10) :

— La couche instrumentation (Instrument layer) : capteurs et actionneurs ;
— La couche processus (Process layer) : automates et switches industriels ;
— La couche système d'exploitation du navire (Integrated Ship Control Layer) ;
— La couche fonctionnelle du navire (General Ship Layer).

Une dernière couche a été ajoutée pour représenter les interactions du bateau avec l'extérieur avec notamment l'armateur et les entreprises de maintenance. À chaque niveau un ou plusieurs points permettent de tester la sécurité du bateau et de réaliser des exercices. Ces points appelés *Hacking Points* sont au nombre de huit :

— HP1 : permet de simuler des accès de l'extérieur du bateau par Internet ;
— HP2 : point d'accès de l'armateur et des entreprises de maintenance ;
— HP3 : accès au réseau loisir des passagers ;
— HP4 : accès au réseau du personnel de bord ;

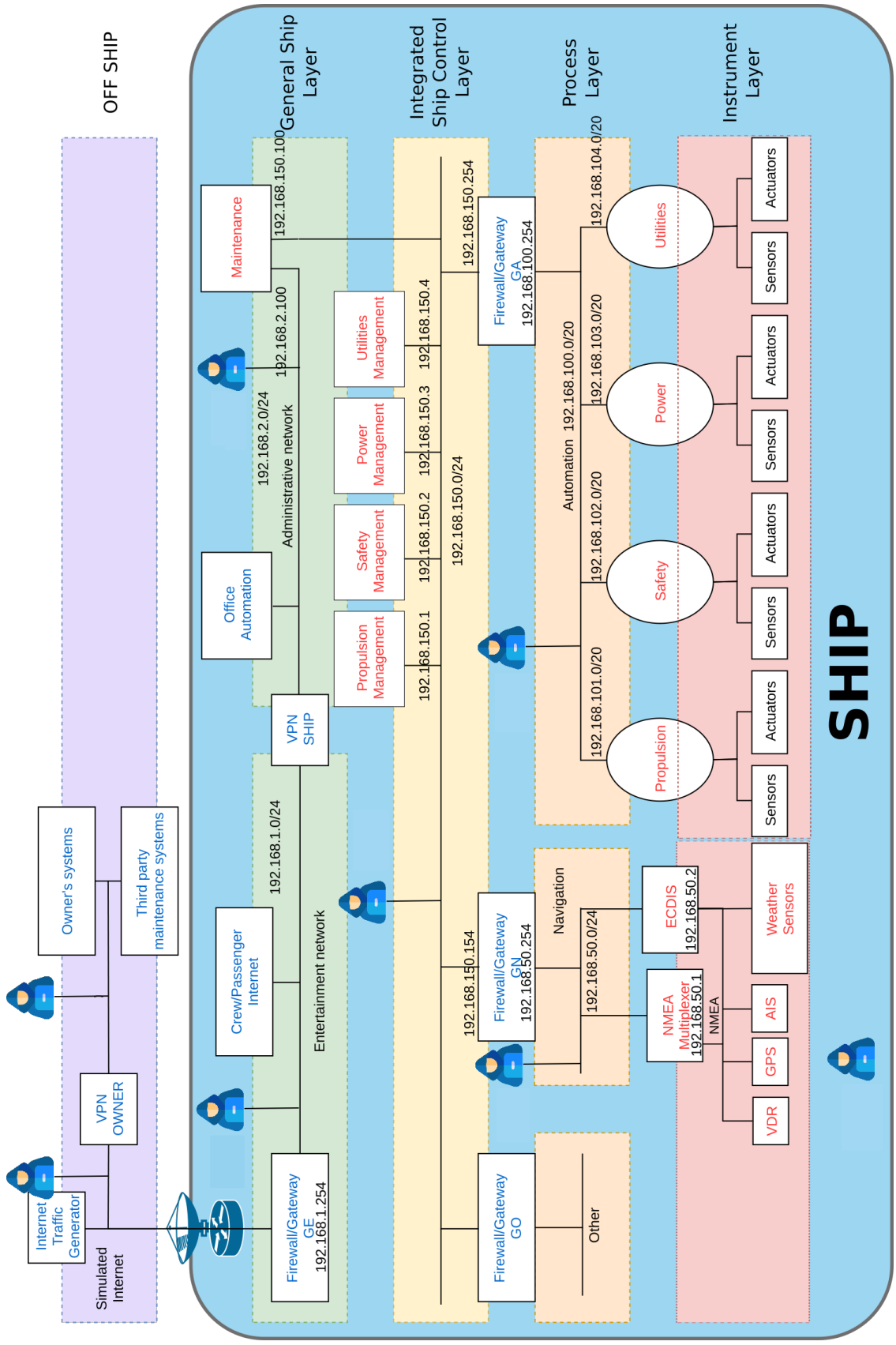


FIGURE I.10 – Architecture réseau du cyberrange

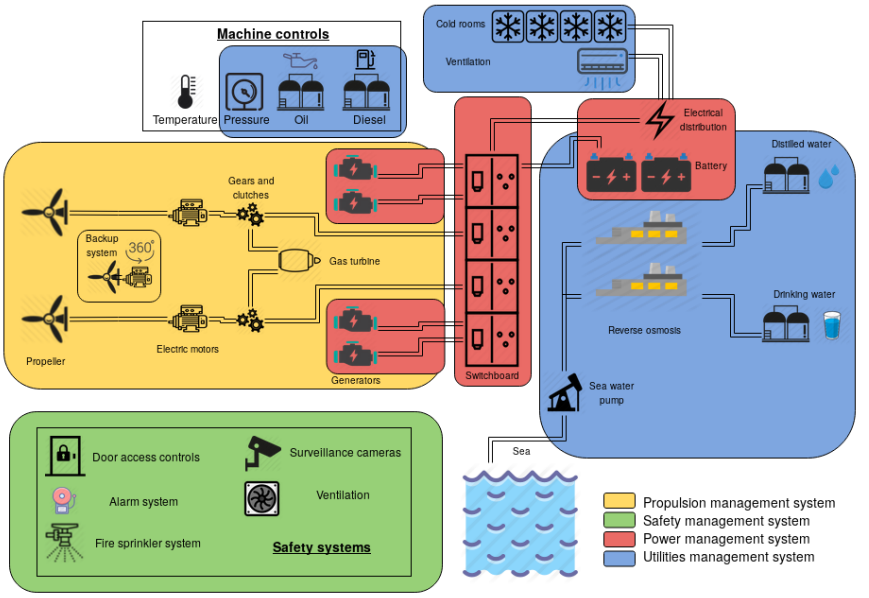


FIGURE I.11 – Boucles de gestion du cyber range

— HP5 : réseau des interfaces de contrôle des automates ;
— HP6 : réseau des équipements de navigation (NMEA, ECDIS, GNSS, AIS et capteurs météo) ;
— HP7 : réseau des automates. La plateforme contient plus d'une vingtaine d'automates connectés à des capteurs et actionneurs réels ou simulés ;
— HP8 : accès aux capteurs pour simuler des anomalies, du brouillage et du leurrage.

Les systèmes de gestion représentés dans le cyberrange sont au nombre de quatre : le système de gestion de la navigation, les systèmes de sécurité, le système de production d'énergie et le système auxiliaire (Figure I.11).

I.4.2 Simulation

La plateforme simule un navire de passagers qui peut naviguer. Le simulateur de passerelle *Bridge Command* (`https://www.bridgecommand.co.uk/`) est relié aux différents systèmes de gestion du bateau et permet ainsi de visualiser la navigation et de piloter le navire. Son interface est en permanence affichée sur grand écran. Les ordres passés par le logiciel sont exécutés par les automates qui renvoient les informations des capteurs et des actionneurs.

Pour augmenter l'immersion, un logiciel de cartographie (*OpenCPN*) est utilisé comme

Electronical Chart Display (ECS). Il est interfacé avec le logiciel *Bridge Command* ce qui permet de visualiser la position du bateau simulé en permanence. Un backbone NMEA auquel sont reliés un GPS et un receveur AIS complète la partie maritime du simulateur. Ces deux équipements injectent des données respectivement sur la position du bateau et sur l'identification des navires proches du bateau sous le format de trames NMEA (National Marine & Electronics Association). Pour que le bateau simulé bouge, une valise d'acquisition de signal GPS et AIS a été mise au point. Cette valise, installée à bord de vrais bateaux, capte le GPS et l'AIS et transmet ces signaux au cyberrange par 4G (ABL+22). Ainsi, le bateau simulé possède une position qui évolue dans le temps comme une vraie navigation. Deux modes de fonctionnement sont ainsi possibles : un mode interactif et un mode automatique dans lequel le bateau simulé suit la trajectoire d'un véritable navire.

I.4.3 Expérimentation

Afin d'acquérir des données réseau du cyberrange, une expérience a été conduite en simulant l'activité de l'ensemble des systèmes de la plateforme. Plusieurs points de collecte ont été implantés au sein de la plateforme. Ces points de collecte sont des *network tap* ou des ports miroirs sur les switches. La figure I.12 montre les différents points de collecte sur les 4 systèmes de gestion ainsi que sur la partie NMEA.

Pour la partie simulation des machines des passagers et des membres d'équipage, les travaux présentés dans la section I.2.2 ont été utilisés. La capture de données a généré 18Gb pour 7 heures de simulation (Figure I.13).

Un type de données difficile à obtenir est l'enregistrement contenu dans le *Vessel Data Recorder* (VDR). Ce système s'apparente à la boite noire se trouvant à bord des avions. Les données stockées dans le VDR doivent permettre en cas d'accident de comprendre les causes lors d'une enquête. Il est obligatoire sur la plupart des navires et doit contenir au minimum 12 heures d'enregistrement et avoir une autonomie énergétique d'au moins 2 heures. De nombreuses caractéristiques dépendent des modèles et des constructeurs de VDR. Le format d'enregistrement des données est propriétaire et nécessite les logiciels spécifiques du constructeur pour pouvoir analyser les données. Néanmoins, les VDR partagent à notre connaissance, une architecture commune composée d'un cœur de collecte de données et d'une capsule étanche conçue pour résister aux accidents.

Il existe deux types de VDR : les systèmes VDR dits standard constitués d'un concen-

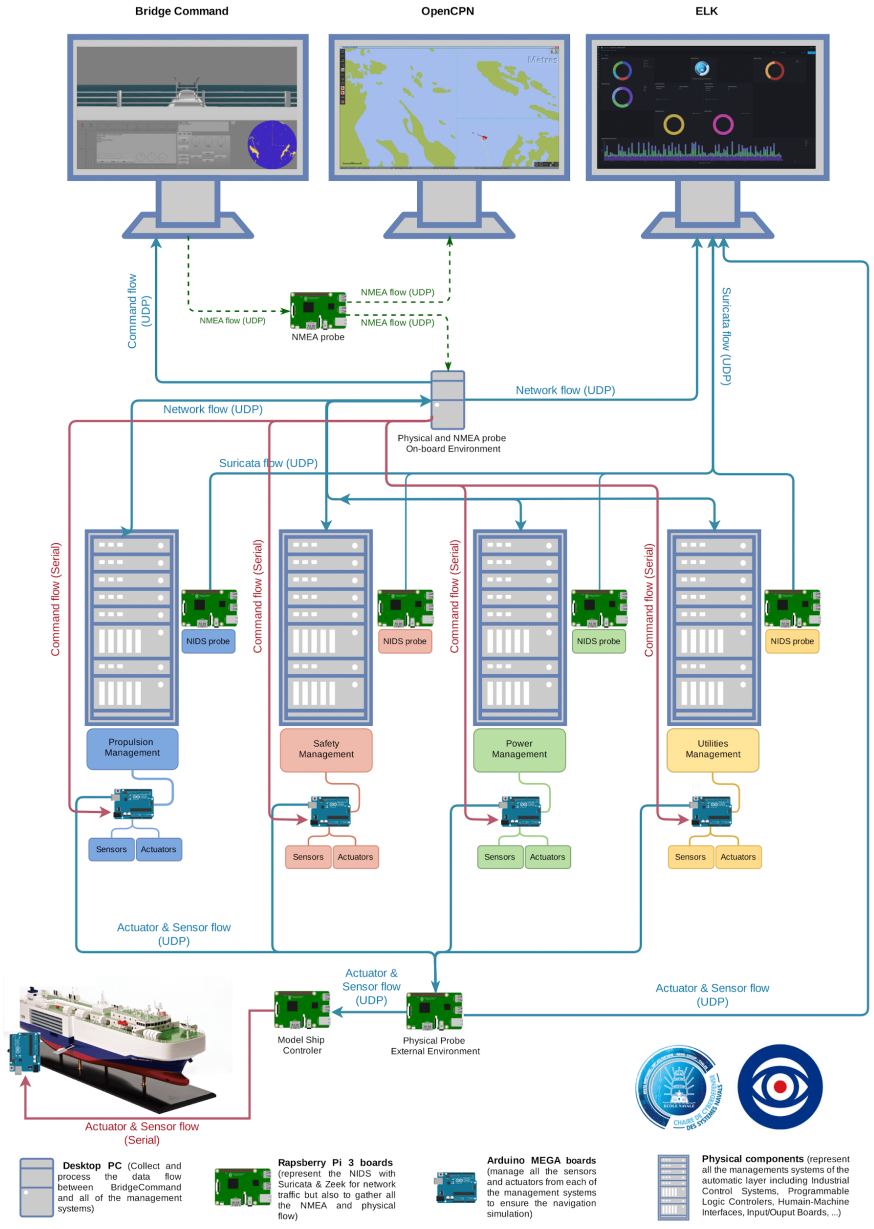


FIGURE I.12 – Architecture physique du cyberrange

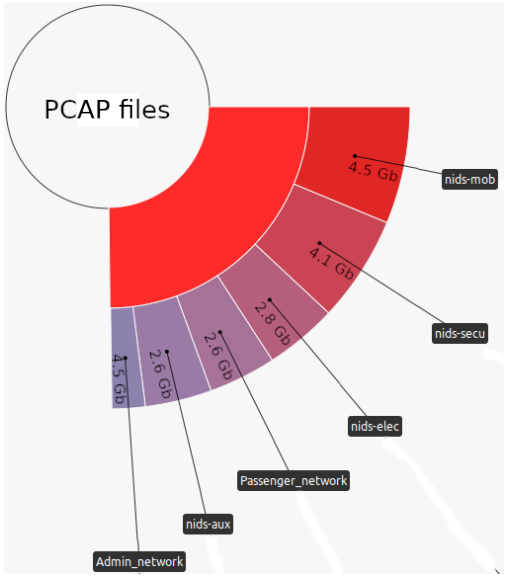


FIGURE I.13 – Capture des données

trateur, d'un module de contrôle et d'une ou deux capsules ; les systèmes VDR dit simples (S-VDR) équipant les navires ne pouvant pas accueillir un système VDR standard. Les données collectées par un S-VDR sont les informations de position, de mouvements et de situations du bateau. Plus concrètement les données capturées sont :

- des captures d'écran de l'ECDIS/RADAR ;
- l'enregistrement vocal de la passerelle ;
- les communications VHF ;
- GPS ;
- la profondeur ;
- la position du gouvernail ;
- les informations du compas ;
- la vitesse de giration ;
- les données des capteurs disponibles au format NMEA.

Pour compléter le cyberrange, un S-VDR a été développé sur la base d'un nano-ordinateur, d'une impression 3D pour la capsule et le développement d'une librairie Python (`https://pypi.org/project/vdr/`). La figure I.14 détaille le fonctionnement du S-VDR du cyberrange.

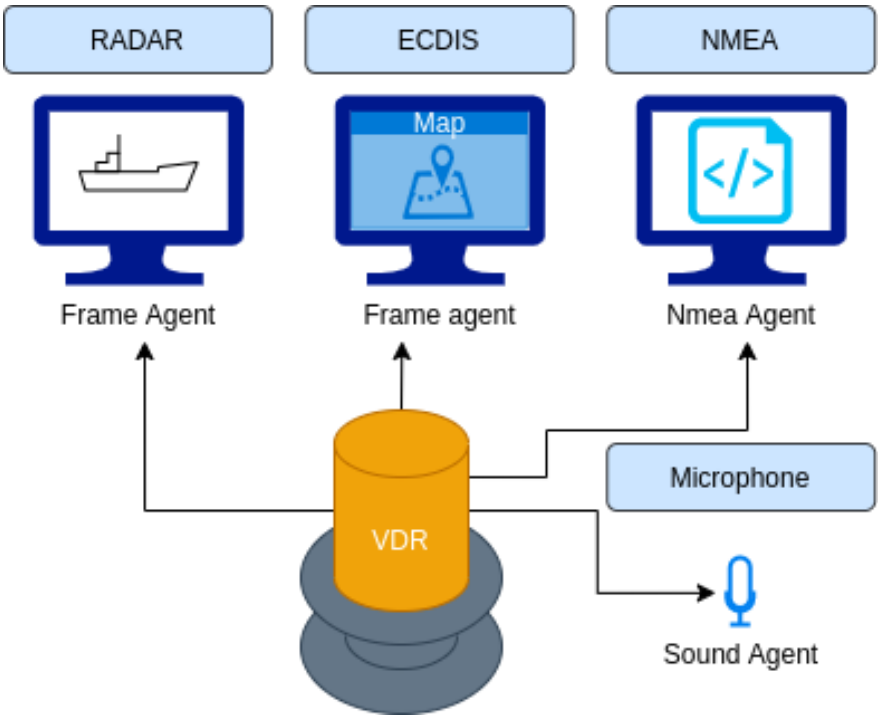


FIGURE I.14 – Architecture du S-VDR développé

La conception d'un cyberrange maritime reproduisant de manière réaliste les systèmes à bord d'un bateau a permis d'acquérir des données réseau de qualité. Cette approche bénéficie de la présence de systèmes industriels réels comme la plateforme pour la génération d'anomalies et utilise la virtualisation et la simulation de comportements proche de la génération de traces. L'équilibre entre réalisme pour être au plus près de données réelles et la maîtrise des biais est un défi important. La plateforme a entièrement été conçue et développée au sein du laboratoire en bénéficiant de l'expertise et de l'expérience des marins impliqués dans ce projet. Elle fait partie des rares plateformes de simulation dédiées au monde maritime pour la recherche et l'entraînement en cybersécurité.

I.5 Conclusion

Dans ce chapitre dédié à l'acquisition de données, nous avons présenté quatre méthodes différentes, de l'enregistrement de descriptions d'itinéraire à la conception d'un cyberrange maritime.

La première approche s'est intéressée à la collecte de descriptions verbales d'itinéraires. Cette collecte a été réalisée en réalisant une expérience dans le cadre d'une course d'orientation. Ce type de données n'était pas disponible et le seul moyen d'en obtenir était de faire une expérimentation spécifique. Plusieurs points pourraient être améliorés comme une plus grande maîtrise des profils des participants, le choix d'un terrain plus varié et le choix des conditions météorologiques qui influencent la perception humaine de l'environnement et de la navigation pédestre. Mais ce genre d'expérience nécessite des moyens financiers et humains conséquents pour l'obtention d'un nombre important de descriptions.

Nos recherches se sont ensuite tournées vers les traces réseau avec deux méthodes différentes : la configuration et la mise en place d'honeypots et la simulation de réseaux virtuels. La première approche, plus facile à mettre en place, permet d'avoir des quantités de données intéressantes. Ces données sont par contre moins riches, car il y a beaucoup de scans automatiques, mais elles permettent de faire des analyses utiles pour le renseignement sur la menace cyber. La deuxième méthode utilisait un ensemble de machines virtuelles configurées en réseau avec des simulations de comportements. Les données produites sont plus variées et l'ensemble de la simulation est maîtrisé. Cependant, la simulation de comportement est difficile, car elle peut être trop simpliste ou bien au contraire trop spécifique en ajoutant des biais. De plus, les machines virtuelles ne génèrent pas exactement les mêmes échanges réseau que des systèmes physiques et des différences existent également en fonction de la virtualisation choisie.

L'analyse d'anomalies sur un système cyberphysique a été réalisée sur un système industriel réel, mais de petite taille. Les données provenant des capteurs et des actionneurs ont été considérées. Si les problèmes de réalisme, de simulation, ne sont pas présents dans cette étude, le nombre de composants est la faible complexité de la plateforme ont constitué un frein à des analyses plus poussées.

Le chapitre s'est terminé par la description du cyberrange maritime développé depuis 2015. Cette plateforme permet d'obtenir des données plus riches, plus complexes et surtout plus réalistes. Si une partie simulation est toujours présente pour l'IT (passagers et membres d'équipages), la vingtaine d'automates, les capteurs, les actionneurs ainsi que les équipements spécifiques à la navigation (systèmes GPS, AIS, protocole NMEA, ...) augmentent le réalisme ainsi que la confiance dans les données produites par le cyberrange.

Une fois les données collectées ou générées, l'étape suivante est leur transformation/-traduction en une forme permettant de les manipuler, comparer, analyser, visualiser pour

produire de nouvelles informations/connaissances pouvant être utilisées pour de la prise de décision. Cette étape est la modélisation, objet du prochain chapitre. Les étapes d'acquisition de données et leur modélisation ne sont pas si disjointes que leur présentation dans ce manuscrit. Le protocole expérimental de la phase d'acquisition est conçu en prenant en compte la modélisation ainsi que les analyses possibles et le type de modélisation choisie dépend évidemment des caractéristiques des données à disposition.

Chapitre II

Modélisation d'activités humaines

Sommaire

Ce chapitre explique les différentes modélisations développées à partir des données obtenues dans chapitre I. Tout d'abord, une étude des descriptions verbales d'itinéraires a été entreprise. Le but était de faire ressortir les principaux composants d'une description verbale d'itinéraire en milieu naturel et comparer ces résultats avec ceux obtenus dans la littérature pour le milieu urbain. À partir de ces observations, une approche de modélisation de description d'itinéraire a émergé.

La deuxième partie du chapitre s'intéresse à la modélisation d'activités humaines dans la ville. Les activités étudiées concernent celles engendrant des déplacements. La modélisation

proposée prend en compte la multimodalité des déplacements urbains.

Les troisième et quatrième parties concernent la modélisation d'activités sur les réseaux informatiques et plus particulièrement la modélisation de cyberattaques en lien avec les données de la section I.2.

II.1 Étude de descriptions verbales d'itinéraires en milieu naturel

Tablette, téléphone, montre connectée, de nombreux dispositifs électroniques sont utilisés pour se repérer dans l'espace pour les activités de loisirs ou pour les déplacements professionnels. Le positionnement par satellite permet de connaître sa position avec précision et plusieurs services de positionnement existent comme GPS, Galileo, GLONASS ou Beidou 3 qui couvrent le territoire français. Ces GNSS peuvent être couplés afin d'améliorer la précision du positionnement. C'est le cas de certaines montres de sport qui permettent d'utiliser GLONASS+GPS par exemple. Mais pour être utilisable il faut d'une par que le signal du satellite soit bien reçu et d'autre part que l'application de géolocalisation soit connectée à Internet pour recevoir des cartes et autres informations actualisées. Si la couverture des GNSS et de la téléphonie mobile est excellente en France, il existe tout de même des zones blanches. Celles-ci sont concentrées dans les zones montagneuses ainsi que dans les forêts denses. Ces lieux sont propices aux activités nature comme la randonnée pouvant être à l'origine d'accidents. Pouvoir communiquer un itinéraire autrement qu'en utilisant un système numérique est ainsi important.

Une description d'itinéraire a pour but de transmettre un ensemble d'informations en quantité et en qualité suffisantes afin de guider une personne d'un point de départ à un point d'arrivée. Les applications vont des loisirs avec les guides de randonnées par exemple aux opérations de secours pour la localisation de personnes après un accident.

L'analyse de descriptions d'itinéraires est une méthode intéressante pour comprendre la perception humaine d'une navigation. De nombreux travaux ont été réalisés en milieu urbain dans des buts touristiques, de sécurité ou simplement pour développer des outils visant à faciliter la navigation dans des villes toujours plus grandes et complexes.

II.1.1 Comparaison entre milieu naturel et urbain

Aucune expérience en milieu naturel n'étant disponible, les descriptions de l'expérience décrite dans la section I.1 ont été comparées à celles obtenues en milieu urbain. Parmi les travaux réalisés en urbain ceux de Denis (1997) définissent une catégorisation des éléments contenus dans une description d'itinéraire en cinq classes :

- Classe 1 : les actions exprimées sans repère ;
- Classe 2 : les actions exprimées avec références à un repère ;
- Classe 3 : les repères autres que ceux mentionnés avec une action ;
- Classe 4 : description d'un repère sans mentionner sa localisation ;
- Classe 5 : classe des commentaires, en d'autres termes tout ce qui ne rentre pas dans les autres classes.

Nous avons utilisé cette classification pour comparer les résultats obtenus lors de l'expérience de course d'orientation avec les travaux de (Den97) et (PM04) réalisés en urbain.

La différence principale entre nos résultats et ceux de Denis (1997) concernent le nombre d'occurrences des classes 3 et 4. Rehrl (2009) obtiennent des résultats semblables aux nôtres avec une expérimentation en milieu urbain (cf. figure II.1). Ils avancent l'hypothèse que cette différence est due au protocole expérimental, car l'expérimentation de Denis (1997) n'était pas faite "in situ" contrairement aux deux autres. Cette différence pourrait être liée aux deux environnements de navigation. En milieu naturel, les repères doivent être davantage décrits pour être identifiés.

II.1.2 Modélisation à base de repères

Ainsi, la modélisation de descriptions verbales d'itinéraires proposée repose sur l'interaction avec les repères décrits. La modélisation est basée sur la théorie des graphes. Une description verbale d'itinéraire peut être modélisée comme un chemin où les nœuds représentent les positions et les arcs, les actions. L'hypothèse principale de la modélisation est qu'une position peut contenir un repère et, de façon similaire, une action peut également interagir avec un repère.

Cette modélisation est composée de triplets, origine/action/destination, chaque élément pouvant être en interaction avec un repère. Au total, 8 différents triplets sont possibles (cf. Tableau II.1). En associant aux actions, *i.e* les arcs du graphe, des orientations et des élévations et aux nœuds des types de repères selon la classification de la course d'orientation,

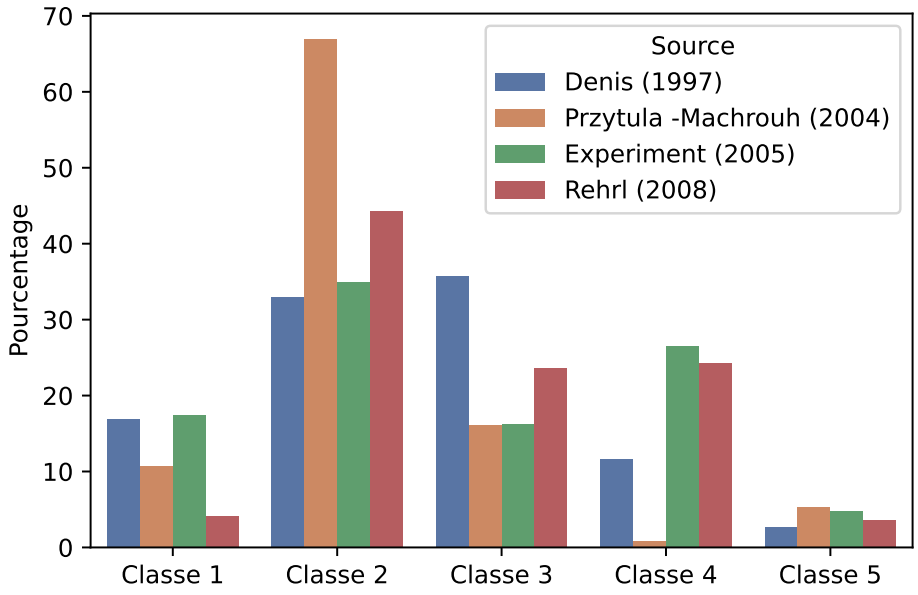


FIGURE II.1 – Analyse de plusieurs expériences selon la catégorisation de (Den97)

nous obtenons une modélisation permettant d'extraire l'essentiel des informations contenues dans une description d'itinéraire (Figure II.2). Les orientations peuvent être relatives (droite, gauche, devant derrière) ou cardinales (8 possibilités *e.g* nord-ouest) tandis que l'information sur l'élévation indique le relief entre les deux points décrits (montée, descente, plat).

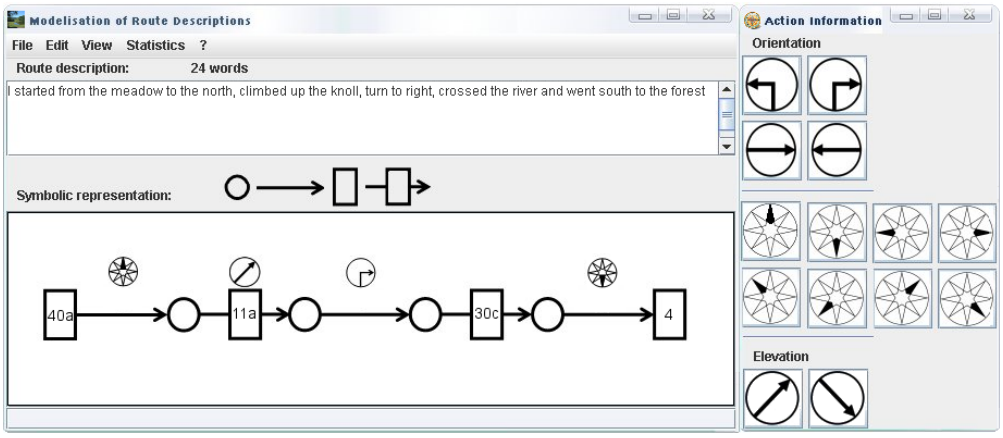


FIGURE II.2 – Modélisation d'itinéraires pédestres en milieu naturel

TABLE II.1 – Ensemble des segments d'itinéraire élémentaires

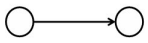
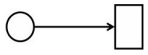
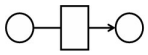
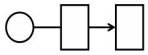
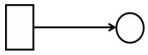
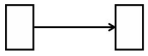
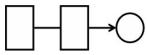
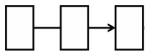
ID	**Définition**	**Représentation booléenne**	**Représentation graphique**
α_0	Une action qui commence par une position et qui se termine par une position	$[0, 0, 0]$	
α_1	Une action qui commence par une position et qui se termine par un repère ou une entité spatiale	$[0, 0, 1]$	
α_2	Une action, qualifiée par un repère ou une entité spatiale, qui commence par une position et qui se termine par une position	$[0, 1, 0]$	
α_3	Une action qui commence par une position, qualifiée par un repère ou une entité spatiale et qui se termine par un repère ou une entité spatiale	$[0, 1, 1]$	
α_4	Une action qui commence par un repère ou une entité spatiale et qui se termine par une position	$[1, 0, 0]$	
α_5	Une action qui commence par un repère ou une entité spatiale et qui se termine par un repère ou une entité spatiale	$[1, 0, 1]$	
α_6	Une action, qualifiée par un repère ou une entité spatiale, qui commence par un repère ou une entité spatiale et qui se termine par une position	$[1, 1, 0]$	
α_7	Une action, qualifiée par un repère ou une entité spatiale, qui commence par un repère ou une entité spatiale et qui se termine par un repère ou une entité spatiale	$[1, 1, 1]$	

TABLE II.2 – Corrélation entre les différentes mesures appliquées aux descriptions d'itinéraire en course d'orientation

	Richesse	**Longueur**	**Entropie**
Richesse	1.0	-0.1400366697680603	-0.3099038571374949
Longueur	-0.1400366697680603	1.0	0.8979890214051617
Entropie	-0.3099038571374949	0.8979890214051617	1.0

II.1.3 Mesures et opérateurs

Ce langage de description d'itinéraire facilite la définition d'opérateurs et de mesures pour analyser les descriptions verbales d'itinéraires. Acte de communication, une description d'itinéraire peut être utilisée pour mesurer la quantité et la qualité des informations contenues avec la théorie de l'information (SW49).

Trois mesures principales ont été appliquées :
— l'entropie ;
— la richesse structurelle ;
— la longueur logique.
L'entropie illustre la diversité d'une description d'itinéraire en prenant en compte l'alphabet utilisé pour la modélisation (Figure II.1).

La mesure de richesse s'intéresse au nombre d'orientations et d'élévations utilisées ainsi que le nombre de descriptions de repères présents dans la description. Ces valeurs sont ramenées entre 0 et 1 en utilisant la longueur logique correspondant au nombre de segments de la description. La figure II.3 illustre les relations entre les différentes mesures appliquées aux descriptions de course d'orientation.

Une seule corrélation peut être observée entre l'entropie et la longueur logique ce qui est normal (Tableau II.2). Cependant, une description plus longue ne veut pas dire une description qui a une richesse structurelle plus élevée. Une hypothèse est que longueur de description et richesse structurelle peuvent se compenser l'une l'autre. Une description plus courte aurait tendance à utiliser plus d'éléments pour décrire les actions et les repères.

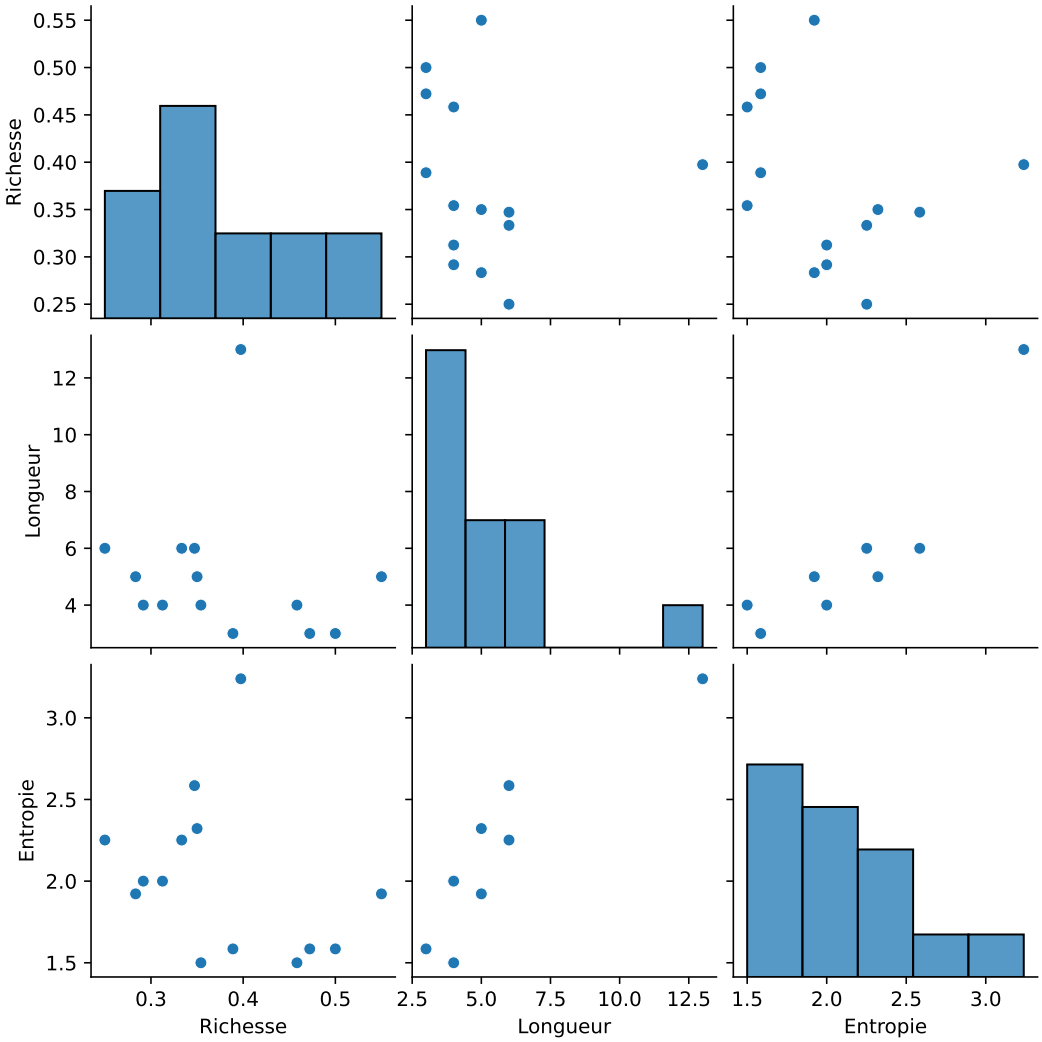


FIGURE II.3 – Relations entre les mesures appliquées aux descriptions d'itinéraires

Cette première modélisation a utilisé la théorie des graphes et plus particulièrement la notion de chemin. Après avoir comparé les résultats de deux autres études concernant des itinéraires en milieu urbain, nous nous sommes intéressés à la relation entre actions et repères c'est-à-dire comment les actions de déplacements interagissent avec des repères spatiaux dans une description d'itinéraire. Un alphabet et plusieurs opérateurs permettent de manipuler et comparer des descriptions d'itinéraires après transformation en chemins étiquetés en précisant l'interaction entre actions et repères.

II.2 Modélisation d'activités dans la ville

La modélisation d'itinéraires présentée dans la section précédente considère exclusivement les expériences de navigation pédestre en milieu naturel. Elle a servi d'inspiration à la modélisation d'activité dans la ville. L'aménagement des différents réseaux de déplacement urbains est un enjeu important pour l'optimisation des déplacements, l'utilisation des services, la lutte contre la pollution ...Mieux comprendre comment les déplacements en ville sont effectués est ainsi essentiel.

II.2.1 Modélisation de la ville

Nous avons proposé une modélisation de la ville, d'un point de vue réalisation d'activités, à l'aide de trois couches de réseau superposées (Figure II.4) :

— le réseau routier ;
— un réseau de transport public ;
— un ensemble de points d'intérêts (POI) pouvant offrir des services.

La ville est ainsi modélisée comme un ensemble de services accessibles par un réseau de transport multimodal. Cette représentation permet de prendre en compte à la fois la structure et l'usage de la ville.

Tout comme la modélisation d'itinéraires en milieu naturel, la théorie des graphes est la base de la modélisation de la ville. Les graphes sont utilisés fréquemment pour des problématiques de modélisation urbaine et des réseaux de transport.

Le réseau routier définit le support de la ville et la structure des activités possibles. Le réseau urbain est utilisé par des moyens de transport individuels tels que les voitures et les vélos, les piétons pouvant également l'utiliser en partie et sous certaines conditions. Le réseau de transport urbain est modélisé par un graphe orienté et pondéré avec l'ensemble des intersections entre les rues et l'ensemble des segments qui les relient. En première approximation chaque segment est pondéré par la vitesse maximale autorisée pour les automobiles, car cette impédance est liée à la structure routière de l'espace urbain. Les autres modalités ont une vitesse considérée comme fixe, mais qui dépend du profil du participant à l'activité considérée.

Le réseau de transport public est un réseau multimodal qui se connecte directement au réseau routier. En effet, la partie de réseau réservée pour les bus et les navettes routières se

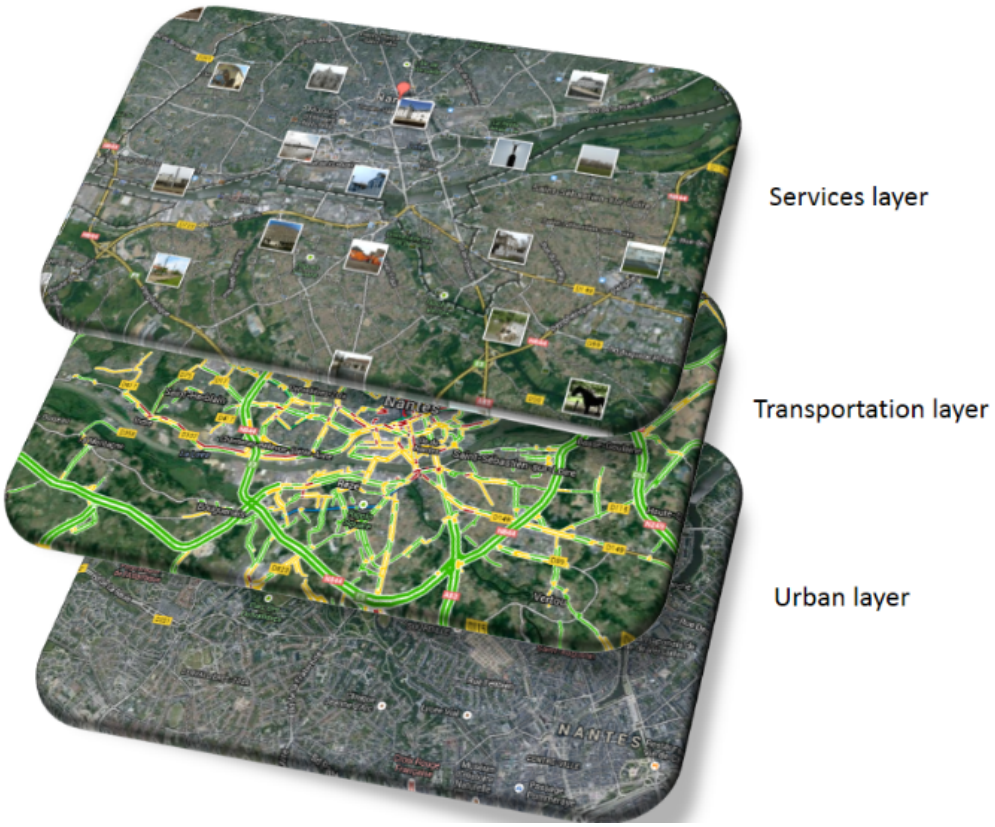


FIGURE II.4 – Les trois couches de la ville(JBC14)

basent sur le réseau routier de la ville. Cependant, le transport ferroviaire est accessible par les arrêts qui sont connectés au réseau routier. Le réseau de transport public est modélisé par une séquence de stations utilisées par différents moyens de transport présents dans la ville tels que : le bus, le tramway, le métro et le train. Chaque moyen de transport possède un ensemble de stations et d'itinéraires prédéfinis. Pour prendre en compte cette multimodalité avec une modélisation à base de graphes, deux concepts peuvent être utilisés :

— les hypergraphes qui étendent les graphes conceptuels en considérant un ensemble de sous-graphes comme noeuds.
— les super-réseaux qui sont organisés en couches de réseaux avec des noeuds spéciaux permettant de connecter les différentes couches entre elles.

L'organisation des données des différents réseaux de transport nous a fait choisir le concept de super-réseau pour la modélisation d'activités urbaines (Jgu16). La figure II.5 illustre les connexions entre pistes cyclables, réseau piéton et ligne de tramway.

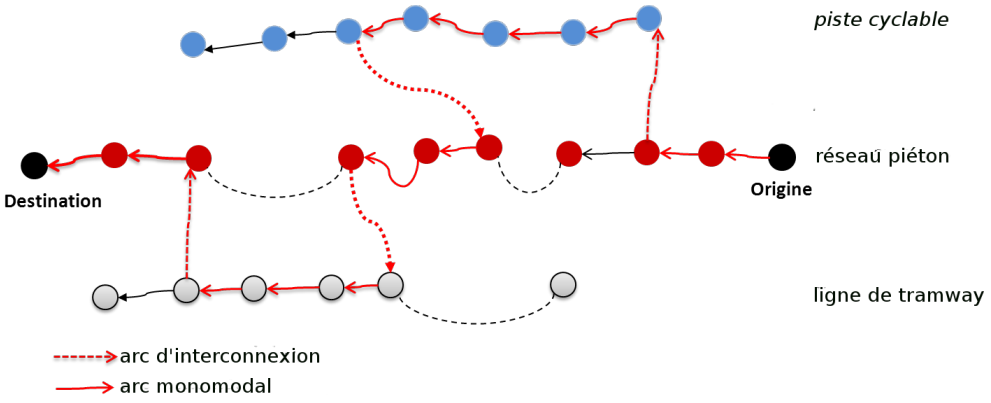


FIGURE II.5 – Un réseau de transport multimodal(Jgu16)

II.2.2 Modélisation des activités

Une activité urbaine est modélisée comme un ensemble de POI à visiter. Un POint d'Intérêt est défini par sa position dans l'espace et le type de service qu'il met à disposition (p. ex., restaurant, magasin). Pour faire correspondre les activités avec les POI, les travaux de (LOY05) ainsi que les bases de données d'OpenStreetMap [1] et Factual [2] ont été utilisés. Il en résulte une classification des points d'intérêt pour les activités urbaines (Figure II.6).

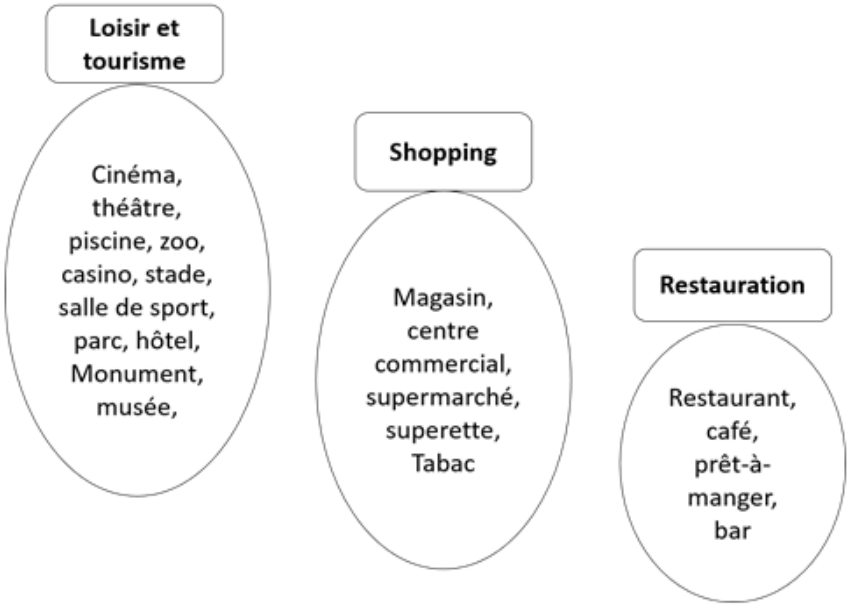


FIGURE II.6 – Typologie des POIs proposée (Jgu16)

1. http ://wiki.openstreetmap.org/wiki/Key :amenity
2. http ://developer.factual.com/working-with-categories/

Dans notre cas l'étude de la structure de l'espace exige de prendre en compte les fonctionnalités offertes par une ville. Nous proposons un modèle qui décrit les activités urbaines en prenant en compte le cadre spatio-temporel ainsi que différents profils d'utilisateurs. Une activité est définie comme un ensemble d'actions à accomplir par des individus dans un objectif précis. Une activité est modélisée comme un ensemble de nœuds qui peuvent être des POI fournissant des services particuliers (Figure II.7).

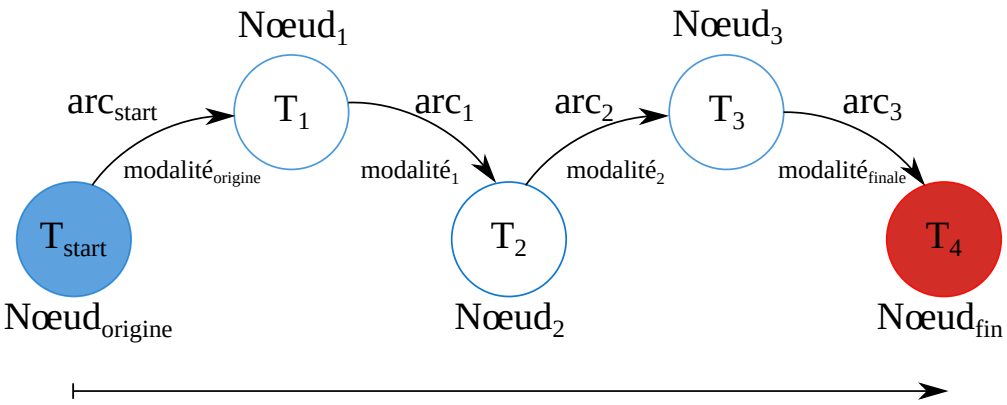


FIGURE II.7 – Graphe d'une activité (Jgu16)

La description d'une activité repose sur des étapes séparées par des déplacements avec une modalité précise. Nous modélisons donc une instance d'activité par une chaîne connectée :

$$act = N_{origine}, a_S^{m_S}, [N_i T_i, a_i^{m_i}]^n, N_{fin} \tag{II.1}$$

La manière de réaliser une activité dépend en grande partie du profil de la personne la réalisant. Nous définissons un profil selon plusieurs caractéristiques : la mobilité réduite de la personne qui devra prise en compte pour l'accessibilité des trajets, la vitesse de marche et une liste des différents moyens de transport utilisables. À ces critères s'ajoute également une durée minimale et maximale de temps d'activité.

$$profil = PMR, vitesse_{marche}, [modalité_i], durée_{min}, durée_{max} \tag{II.2}$$

Pour cette approche de modélisation, nous avons travaillé sur les activités urbaines impliquant des déplacements. Ces déplacements peuvent être multimodaux et utiliser différents réseaux de transports. L'originalité de la modélisation vient de l'utilisation du concept de super-réseaux, de l'ajout de nœuds particuliers représentant des points d'intérêt ainsi que la définition d'activités et de profils d'utilisateurs qui manquait à la modélisation précédente. Cette modélisation est adaptée à la génération automatique d'itinéraires d'activité en utilisant les données spatiales communautaires de plus en plus précises.

II.3 Modélisation de cyberitinéraires

À l'instar des itinéraires en milieu naturel et des activités urbaines, les cyberattaques peuvent être modélisées par une approche à base de graphes. En effet, les attaques cyber peuvent être spatialisées par les adresses IP de l'attaquant (dernier rebond, car l'attribution d'une cyberattaque est difficile/impossible) et de la victime et elles possèdent également une estampille temporelle. Les itinéraires parcourus dans le cyberespace par ces attaques sont autant de chemins qu'il est possible d'analyser afin de faire émerger des motifs. Ces itinéraires permettent à la fois de mieux comprendre l'état du cyberespace à un instant donné, mais également d'étudier la dynamique afin d'adapter les stratégies de cyberdéfense.

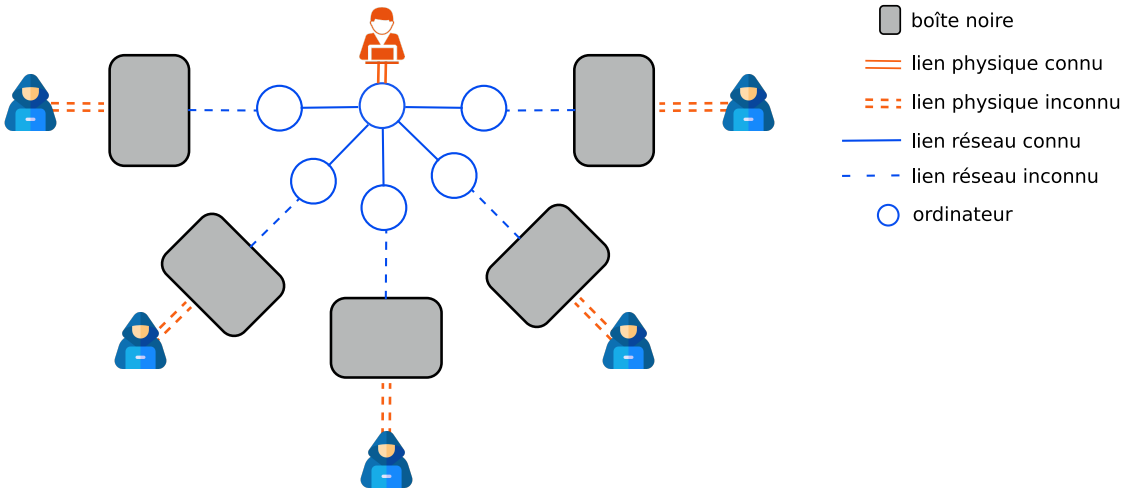


FIGURE II.8 – Chemins de cyberattaques

Les itinéraires des cyberattaques sont réduits à une source et une cible du fait des

difficultés de l'attribution et que seul le dernier rebond est facilement connu (le modèle utilise la couche 3 du modèle OSI). Néanmoins, la modélisation proposée va plus loin en considérant l'ensemble des points de passages (rebonds) même si ceux-ci ne sont pas connus. La figure II.8 illustre l'ensemble des itinéraires des cyberattaques pour une cible donnée située au centre du schéma. Dans ce schéma sont distinguées les données connues (IP et liens) et les informations manquantes (chemins réels jusqu'aux vrais attaquants).

Le concept de "boîte noire" entre le vrai attaquant et le dernier rebond connu est intégré à la modélisation et permet de traiter les informations manquantes. La figure II.9 détaille le chemin d'une cyberattaque avec le contenu de cette "boîte noire".

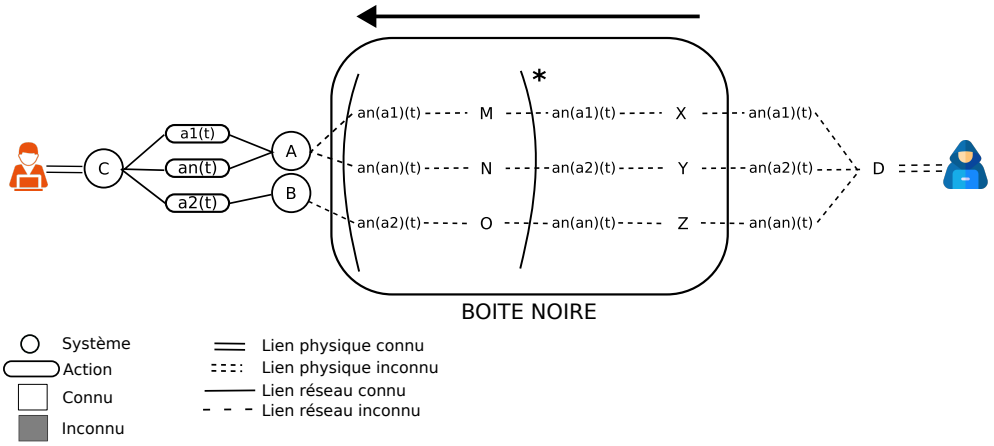


FIGURE II.9 – Modélisation de chemins de cyberattaques

L'hypothèse principale de cette étude est la persistance de l'intention de l'attaquant, quelle que soit la méthode d'attaque utilisée.

II.3.1 Le concept d'intention

Nous définissons l'intention comme une action permettant d'aboutir à un objectif particulier. Le concept d'intention s'appuie sur la *Cyber Kill Chain*, concept inventé par la société américaine Lockheed Martin en 2011. Il s'agit d'une modélisation permettant d'analyser les actions offensives lors d'une attaque. Cette modélisation permet aux enquêteurs et aux analystes d'affecter un nom à l'étape de l'attaque étudiée (YR15). La figure II.10 montre l'enchaînement des 7 étapes.

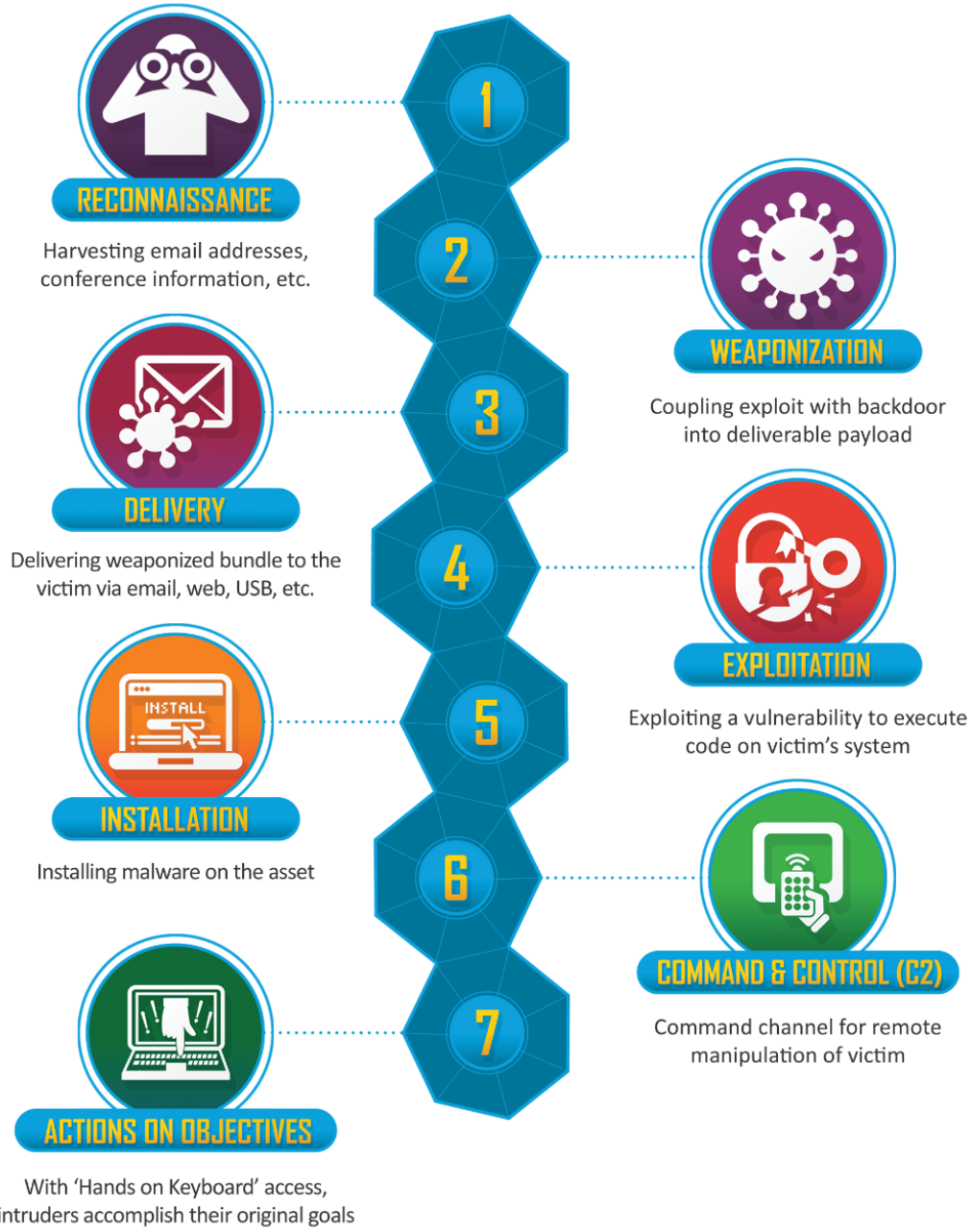


FIGURE II.10 – Différentes phases de la Cyber Kill Chain Source : `https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html`

En 2015, le MITRE, agence à but non lucratif dont les objectifs sont d'améliorer la sécurité dans l'intérêt public, a conçu le framework ATT&CK (Adversarial Tactics and Technics & Common Knowledge). Ce framework a pour but de mieux connaître les cyberattaques en adoptant le point de vue de l'attaquant. Ce modèle dynamique permet de qualifier les

étapes d'une cyberattaque en détaillant les tactiques et les techniques utilisées. De 7 étapes dans la Cyber Kill Chain, ATT&CK passe à 12 catégories :

— Accès initial ;
— Exécution ;
— Persistance ;
— Escalade des privilèges ;
— Évasion de la défense ;
— Accès aux justificatifs ;
— Découverte ;
— Mouvement latéral ;
— Collecte ;
— Commande et contrôle ;
— Exfiltration ;
— Impact.

Cette classification est de plus en plus utilisée dans le domaine du renseignement sur la menace et la lutte contre les menaces (Threat Intelligence et Threat Hunting) comme le montre la figure II.11.

Jusqu'en octobre 2020, la première étape considérée est l'accès initial aux systèmes victimes. Les phases de reconnaissance et d'armement que l'on retrouve dans la Cyber Kill Chain n'était pas traitées par le framework du MITRE qui était principalement dédié à l'étude des attaques lorsque celles-ci sont en cours.

Une autre partie, PRE ATT&CK, permet de prendre en compte les phases de préparation des attaques. Cette partie a été intégrée à partir de la version 8. La dernière version à l'écriture de ce manuscrit est la version 9. Elle comporte 14 catégories (tactics) avec les deux premières, la reconnaissance et le développement de ressources, qui permettent d'englober toutes les phases d'une cyberattaque. Le nombre de techniques répertoriées est de 215 sans compter les sous-techniques.

II.3.2 Modélisation formelle

Afin de pouvoir manipuler les tentatives d'intrusion, une modélisation formelle a été définie. Une cyberattaque est constituée de l'attaquant (h_{atq}) et la victime (h_{cbl}) (Figure II.12). Le point important est la relation entre ces deux entités. L'attaquant souhaite compromettre la cible et a une intention précise du moyen à utiliser pour ses fins. Ainsi, cette

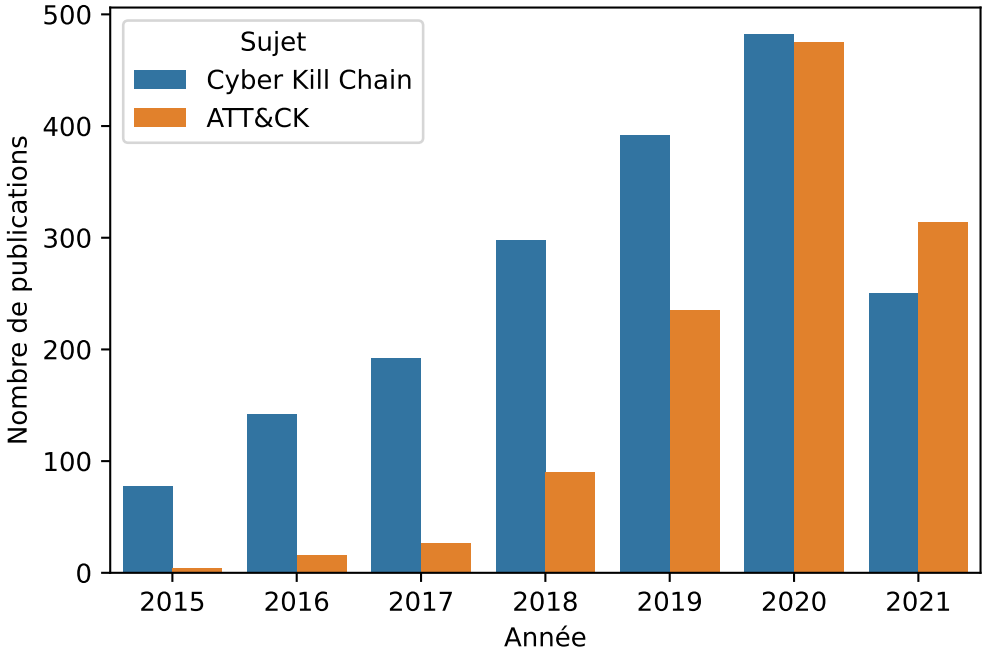


FIGURE II.11 – Évolution du nombre de publications sur la Cyber Kill Chain et le framework ATT&CK à partir des données de `scholar.google.com`

intention relie l'attaquant et la cible.

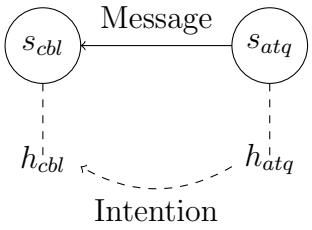


FIGURE II.12 – Modélisation réseau avec intentions

Comment connaître l'intention de l'attaquant en n'ayant seulement les résultats de ces actions dans les messages réseau ? L'hypothèse de notre modèle est que l'intention de l'attaquant peut être inférée en partie par les messages transitant sur le réseau, notamment à l'aide des protocoles réseau utilisés (MBBC18b). En effet, les protocoles réseau ainsi que la durée des échanges permettent de déduire à un niveau macro les actions des utilisateurs.

Le tableau II.3 montre une proposition de relation entre protocoles et intentions.

TABLE II.3 – Attributions des intentions en fonctions des protocoles

	Intention	**Protocoles**
Collecte	Écoute du réseau	ICMP ; SIP ; SNMP ; SSDP
	DNS	DNS ; LLMNR ; MDNS ; NBNS
	ICS	BACnet ; DNP3.0 ; IPMI ; XDMCP ; ...
	Web	HTTP ; HTTPS
Action	Contrôle	SSH ; SSHv2
	Partage de fichiers	FTP ; TFTP

TABLE II.4 – Les différents paramètres permettant de qualifier les intentions

	États possibles
Légitimité	Légitime / Illégitime
Protocole	Écoute du réseau / DNS / ICS / Web / Contrôle / Partage de fichiers
Contenu	Normal / Malveillant
Pression	Nominale / Faible / Élevée

Plusieurs critères peuvent nous éclairer sur l'intention de l'attaquant :

— la légitimité de la source ;

— les protocoles utilisés ;

— le contenu des messages ;

— la fréquence des messages ;

— et bien d'autres paramètres.

Nous définissons 4 ensembles L, $Prot$, C et Fre respectivement pour la légitimité, le protocole, le contenu du message et la fréquence de messages. Le tableau II.4 donne les valeurs possibles pour chaque ensemble.

L'attribution des attaques est généralement impossible. L'utilisation de multiples rebonds, de machines compromises, de serveurs anonymes ou du réseau TOR permet aux attaquants de préserver leur anonymat. Cet enchaînement de systèmes entre l'attaquant et la cible ne peut être connu, mais peut être représenté comme une boîte noire.

La figure II.13 montre comment nous modélisons le lien entre attaquant h_{atq} et victime h_{cbl} qui est qualifié par l'intention $i(t)$ à l'instant t. Les données enregistrées avec l'expérience décrite dans la sous-section I.2.1 ne contiennent seulement les messages $m_0(t_0)$ entre le dernier rebond utilisé s_0 et la machine de la victime s_{cbl}. L'ajout du concept de boîte noire permet de modéliser deux messages supplémentaires qui respectivement en parte et en arrive ($m_1(t_{X0})$ et $m_n(t_{Xn})$) ainsi que le système de l'attaquant s_{atq}.

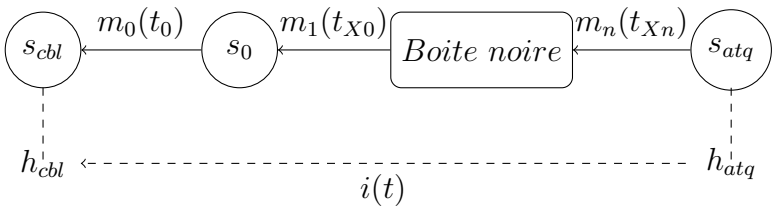


FIGURE II.13 – Modèle réseau intégrant l'humain

À partir des données des Honeypots nous avons modélisé les chemins entre attaquants et victimes en utilisant le concept d'intention que nous avons défini. Similaire à l'interaction action/repère pour les descriptions d'itinéraire, l'intention repose sur la cyberkill chain pour utiliser la phase de reconnaissance de l'attaquant. Il conviendrait à présent de se baser sur le modèle ATT&CK qui est plus précis et plus complet. Les différents rebonds entre attaquants et honeypots sont inconnus, mais nous les avons modélisés par une boîte noire pour être capables de manipuler des données d'attaques réseau incomplètes. Plusieurs opérateurs définis sur cette modélisation peuvent permettre d'identifier des comportements d'attaquants.

II.4 Modélisation d'activités réseau

Les cyberattaques étudiées dans la section précédente étaient considérées comme des messages unidirectionnels de l'attaquant vers la cible. Les réponses de la machine cible n'étaient pas prises en compte. Dans cette section nous intéressons à l'ensemble des échanges effectués dans un réseau informatique par des machines. Il ne s'agit plus seulement de cyberattaques, mais de l'ensemble des comportements qui peuvent être extraits d'un enregistrement réseau.

L'objectif de cette modélisation est d'une part la qualification des enregistrements réseau et d'autre part la reproduction d'échanges réseau ayant des caractéristiques spécifiques dans le but de générer des traces réseau ayant des propriétés similaires. Ces traces générées, reproduisant des caractéristiques de traces originales, pourront être utilisées pour l'apprentissage de sondes de détection d'intrusion comportementales. L'intérêt est double : multiplier les ensembles d'apprentissage et utiliser des traces "similaires" à des ensembles ne pouvant être rendus publics (pour des raisons de confidentialité).

Dans cette partie nous abordons en premier les caractéristiques des datasets puis la modélisation des échanges réseau qu'ils contiennent.

II.4.1 Enregistrements réseau

Nous nous intéressons tout d'abord à l'enregistrement de traces réseau. Plusieurs formats d'enregistrement existent. Les deux types les plus fréquemment utilisés sont des enregistrements simples au format texte et formatés en fichiers CSV et des captures de paquets au format PCAP (Packet CAPture). Les enregistrements en données texte sont généralement issus de l'extraction de données de fichiers PCAP. Ce format est le plus reconnu, mais plusieurs déclinaisons existent. Le format original développé dans les années 80 est limité à une seule interface réseau et a une précision de l'ordre de la milliseconde. Le format nsecpcap partage les mêmes caractéristiques, mais avec une précision à la nanoseconde. Le format PCAPNG, apparu en 2013, reprend la précision à la nanoseconde, mais permet d'avoir des paquets réseau de plusieurs interfaces réseau et l'ajout de champs dans l'entête du fichier.

De nombreux datasets de traces réseau sont disponibles en téléchargement pour tester différentes méthodes de détection d'intrusion ou pour l'investigation numérique (HBB+18). Les datasets sont toutefois très différents les uns des autres et évaluer leur adéquation pour

l'usage voulu est difficile.

Plusieurs critères permettent de qualifier un dataset de données réseau. Le premier permet de connaître la nature (*nature of data*) de l'expérimentation c'est-à-dire si les données proviennent d'un enregistrement réel ou bien si les données ont été générées (HBB+20). La génération de données peut être faite à partir d'un enregistrement réel (sous-section I.2.1) avec de l'injection de paquets (des attaques généralement) ou bien être issue de simulations et l'utilisation de virtualisation comme les données présentées dans la sous-section I.2.2.

De nombreux travaux ce sont intéressés à l'évaluation des datasets disponibles sur Internet et l'identification de caractéristiques (CVM+15 ; VSO17 ; SGLG18 ; HBB+20 ; CVW+21).

D'après ces études, un enregistrement réseau doit être :
— réel ;
— étiqueté ;
— valide ;
— correct ;
— varié ;
— documenté ;
— facile à mettre à jour ;
— reproductible ;
— distribuable ;
— pourvu de données "normales" de qualité ;
— issues de systèmes réalistes.

Une information importante à connaître sur un jeu de données réseau est de savoir pourquoi et dans quel objectif il a été enregistré. Cela peut être lors d'un challenge, comme c'est le cas des datasets KDD, pour l'entraînement de sondes d'intrusion, la construction de jumeaux numériques et pour bien d'autres objectifs.

Nous allons discuter les caractéristiques retenues, leur pertinence et leur utilité pour comparer des jeux de données entre eux et en indiquant les valeurs possibles, l'ensemble vide représentant le manque d'information sur le critère concerné.

Tout d'abord, le critère *réel* identifié dans la littérature peut avoir plusieurs sens. Il peut s'agir du type de systèmes utilisés (virtuel ou bien réel) ou bien si le trafic a été généré ou injecté dans des données existantes. Nous définissons l'ensemble $Nature\_of\_data$ tel que :

$Nature\_of\_data = \emptyset, real, virtual, simulated, mixed.$

Le paramètre *etiqueté* permet de savoir si les échanges réseau sont identifiés pour que le jeu de données puisse servir à l'apprentissage supervisé par exemple. L'ensemble $Labels$ est constitué de l'ensemble vide, indiquant l'absence d'étiquettes, du sous-ensemble $AttackLabels$ et du sous-ensemble $NormalLabels$. Ces deux sous-ensembles permettent de connaître les types identifiés dans le jeu de données à la fois pour les attaques et les actions "normales" du réseau. Ce dernier peut être utilisé pour évaluer le critère *pourvu de données "normales" de qualité*.

Les deux paramètres *valide* et *correct* sont difficiles à formaliser. En effet, la validité est difficile à évaluer. Il peut s'agir d'avoir l'ensemble des échanges complets entre systèmes ainsi que les réponses et accusés de réception de chaque paquet (flux TCP complets par exemple). Le caractère correct est redondant par certains aspects avec la validité de l'enregistrement. Ces deux paramètres sont néanmoins clairement issus de l'analyse des échanges réseau et restent toutefois dépendants de l'utilisation souhaitée des données.

Le critère *varié* sera déduit des différentes caractéristiques des échanges réseau comme le nombre d'adresses réseau ou le nombre de protocoles.

Les critères *facile à mettre à jour*, *reproductible*, *distribuable*, *issu de systèmes réalistes* sont à apprécier par la description faite dans la documentation.

Nous définissons un enregistrement de communications réseau par *capture* tel que :

$$capture = \Big(\{échanges\_réseau\}, \{propriétés\}\Big)$$

$\{échanges\_réseau\}$ représente l'ensemble des échanges réseau enregistrés dans la capture et $\{propriétés\}$ rassemble les critères caractérisant la capture vus précédemment.

II.4.2 Échanges réseau

De nombreuses modélisations des échanges réseaux sont possibles. Le type de modélisation est comme la caractérisation de jeux de données réseau dépendant des objectifs/usages souhaités. L'élément atomique manipulé est le Protocole Data Unit (PDU) qui permet de regrouper l'ensemble des paquets, messages et objets sous la même appellation, quelle que soit la couche réseau d'origine (KRF11).

Nous définissons un ensemble d'échanges réseau comme un ensemble de PDU : $\{PDU\}$

Un enregistrement réseau est donc une série temporelle de PDU. Pour analyser les échanges réseau, les PDU sont agrégés en fonction de certains attributs. Le concept de "packet train" est défini comme un agrégat de paquets avec la même source et même destination, mais avec une durée maximale entre deux paquets appelée "inter-train gap" (JR86).

Un flux réseau (Network Flow) est quant à lui défini par une séquence de paquets ayant les mêmes valeurs pour les attributs suivants : Source IP, Destination IP, Source Port, Destination Port and Protocol (TCP or UDP) (LDGMG17). L'importance étant généralement mise sur la machine source et la machine cible, le terme Origine-Destination exchange est parfois utilisé notamment pour l'étude de réseau de grande taille en regroupant les échanges entre leur origine initiale et leur destination finale (LPC+04). Cisco définit formellement un NetFlow avec 5 à 7 attributs parmi :

- une adresse IP source ;
- une adresse IP cible ;
- une adresse matérielle source ;
- une adresse matérielle cible ;
- un port source ;
- un port cible ;
- un protocole d'échange ;
- une taille d'échange en octets ;
- une estampille temporelle ;
- une durée.

D'autres caractéristiques peuvent être utilisées, mais celles-ci représentent les informations les plus importantes. Certains commutateurs permettent d'obtenir les NetFlow directement. Le type *sFlow* (Sampled Flow) ne permet pas d'obtenir des données précises sur les échanges réseau et notamment les comportements anormaux dû à l'échantillonnage appliqué qui supprime de nombreuses informations.

En fonction, du temps maximum entre deux paquets, le nombre de "trains"/flows est complètement différent ce qui entraîne des analyses différentes (CBP95).

Plusieurs modélisations agrégeant les PDU peuvent être extraites d'un enregistrement réseau en fonction du choix de certains critères comme la durée maximale entre deux PDU pour appartenir au même flux ainsi que la durée maximale d'un flux.

Nous définissons la fonction $PDU_{aggregation}$ la transformation d'une capture réseau en

un ensemble d'objets ayant un nombre d'attributs variable :

$$PDU_{aggregation}\Big(capture, \{attributes\}, time\_out, T\Big)$$

capture représente l'enregistrement réseau tel que défini auparavant, $\{attributes\}$ est l'ensemble des critères utilisés pour l'agrégation, *time_out* est le temps maximum entre deux PDU pour faire partie du même agrégat et T est la durée maximale d'un agrégat.

Par exemple :

$$PDU_{aggregation}\Big(capture, \{ip\_src, ip\_dest, port\_src, port\_dest, proto\}, 500ms, 5min\Big)$$

permet l'obtention des flux TCP/IP en agrégeant les paquets ayant les mêmes adresses IP d'origine et de destination, les mêmes numéros de port en origine et en destination ainsi que le même protocole, séparés de moins de 500ms avec une durée inférieure à 5 minutes.

L'intérêt de cette modélisation est de pouvoir analyser des captures en faisant varier les différents paramètres. Il est possible de s'intéresser au flux réseau comme l'exemple précédent, mais aussi aux applications exécutées sur les machines en agrégeant seulement les adresses d'origine, les ports source et les protocoles :

$$PDU_{aggregation}\Big(capture, \{ip\_src, port\_src, proto\}, 500ms, 5min\Big)$$

De nombreuses recherches concernent les échanges réseau ou plus précisément utilisent des ensembles de données réseau. Nous avons modélisé tout d'abord les ensembles d'échanges réseau en utilisant les critères identifiés dans la littérature et plusieurs autres provenant des expériences d'acquisition de données que nous avons réalisées. Il en résulte un ensemble de propriétés qui caractérise les ensembles d'échanges réseau. Nous avons ensuite étudié les échanges réseau à partir des flux TCP/IP qui sont les plus utilisés pour caractériser des communications réseau. La construction des flux peut être faite de différentes manières avec des précisions et des attributs qui peuvent varier. La modélisation des échanges que nous proposons précise comment la construction des flux a été réalisée pour connaître précisément la nature des flux manipulés. Ces deux modélisations caractérisent de manière précise les échanges réseau pour pouvoir comparer les méthodes les utilisant de manière plus fiable qu'auparavant en utilisant différents jeux de données et en évitant d'utiliser des jeux de données anciennes du type de KDD.

II.5 Conclusion

Ce chapitre a décrit les différentes approches de modélisation développées au cours de notre recherche. Des travaux sur les itinéraires pédestres aux échanges réseau, les points communs sont des points de départ et d'arrivée ainsi qu'un moyen d'interaction avec l'environnement qu'il soit physique ou numérique. Ce mode d'interaction peut se traduire par un moyen de locomotion spécifique pour les travaux sur la modélisation des déplacements urbains ou le protocole utilisé entre deux systèmes informatiques.

La notion de chemin est omniprésente que ce soit pour des itinéraires pédestres ou des chemins d'attaques. L'étude des déplacements dans la ville se rapproche des travaux sur les échanges réseau. Les modalités de transport du monde physique se transformant en protocole réseau entre deux systèmes et la vitesse entre ces deux applications jouent un rôle important (vitesse de déplacement *vs.* débit réseau).

Qu'il s'agisse d'activités dans le monde réel ou bien d'activités numériques, l'étape de la modélisation est essentielle afin de permettre différentes analyses. L'objectif de la modélisation est à prendre en considération. En fonction des analyses et des hypothèses à étudier, les propriétés du modèle, sa précision et les attributs manipulés devront être adaptés. L'approche proposée pour les échanges réseau permet de faire varier les informations modélisées ainsi que la précision du modèle (temps minimum et temps maximum entre échanges) afin de tester la robustesse des analyses et également pour caractériser les données en entrée.

Chapitre III

Analyses d'activités

Sommaire

Les modélisations présentées ont été instanciées par des données réelles ou simulées dont plusieurs protocoles expérimentaux sont présentés dans le chapitre I. À partir de ces données, plusieurs analyses et traitements ont pu être réalisés. Le premier traitement présenté dans ce document concerne les itinéraires en milieu naturel. Les graphes décrivant les navigations pédestres sont utilisés pour géolocaliser les différents points de passage. Les itinéraires modélisés peuvent également être utilisés pour la génération de schémas représentant l'environnement. Deux autres analyses sont décrites pour des activités numériques avec l'analyse des données collectées par les honeypots et le concept d'intention et l'utilisation de la qualité pour la détection d'anomalies.

III.1 Géolocalisation de descriptions d'itinéraires

La géolocalisation d'une description verbale d'itinéraire consiste à proposer pour chaque étape de l'itinéraire un ensemble de points possibles dans l'espace géographique. Pour cela un algorithme basé sur les principes des algorithmes de colonies de fourmis a été développé en utilisant l'approche de modélisation d'itinéraires mentionnée dans le chapitre précédent (BCS08b ; BCS08a ; BC11).

Les algorithmes de colonies de fourmis sont inspirés de l'observation du monde vivant :

les colonies de fourmis et de termites. Une forme de communication indirecte chez certains insectes a été observée : la stigmergie. Grâce à cette forme de communication utilisant l'environnement comme support, une colonie de fourmis est capable de résoudre des problèmes complexes comme déterminer le plus court chemin dans un réseau.

L'algorithme de géolocalisation défini s'appuie sur ces principes. Le but n'est pas de trouver le plus court chemin, c'est-à-dire minimiser la distance, mais trouver des solutions satisfaisant le plus possible les contraintes de la description d'itinéraire, c'est-à-dire maximiser la satisfaction avec la description.

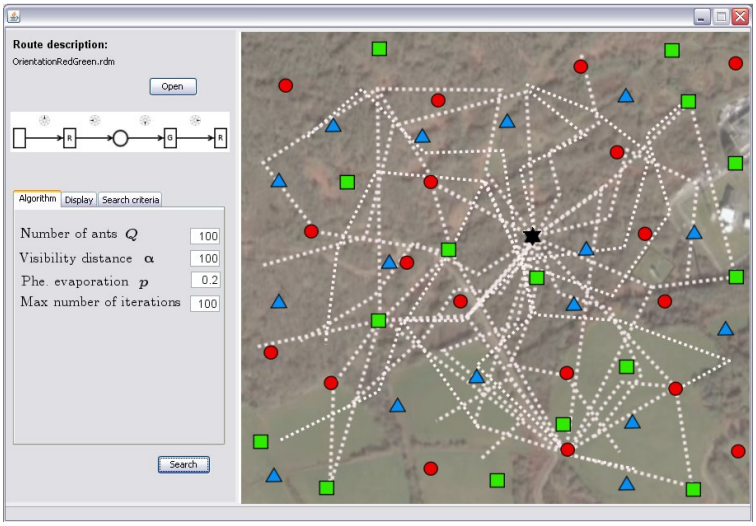


FIGURE III.1 – Géolocalisation d'un itinéraire à partir de sa description (Bro08)

L'environnement étudié ne possède pas une structure limitant la navigation comme un réseau de rues et de chemins. La première étape de la géolocalisation a été de créer une méthode permettant d'obtenir un réseau d'itinéraires possibles. Cette méthode se base sur la proximité des repères décrits dans la description donnée en entrée. Le résultat est un ensemble de couches de nœuds pouvant correspondre aux étapes de l'itinéraire recherché. Le nombre de nœuds est important, plus de deux cent par couche, et justifie l'utilisation d'une technique d'approximation telle que les algorithmes par colonies de fourmis. Une fois le réseau constitué, la phase d'exécution génère des itinéraires de façon probabiliste, évalue ces solutions et met à jour le réseau pour favoriser les étapes qui produisent des solutions satisfaisantes. La Figure III.1 montre l'interface permettant d'exécuter l'algorithme de géolocalisation d'un itinéraire à partir de sa description.

À partir des descriptions d'itinéraires modélisées, nous avons pu recréer des itinéraires possibles en utilisant les repères décrits ainsi que les différentes interactions entre actions et repères. Cette génération d'itinéraires a été possible par l'utilisation d'algorithmes d'approximation de type colonie de fourmis qui ont la capacité de trouver des solutions même s'il manque des informations ou qu'il y a des erreurs dans les descriptions. Le logiciel développé a permis d'identifier les itinéraires réellement décrits. Des erreurs de descriptions faites par les participants ont également été détectées. Ce travail peut être utilisé pour construire des itinéraires à partir de récits et aussi pour vérifier que des descriptions d'itinéraires (pour la randonnée par exemple) sont suffisamment précises pour être utilisées.

III.2 Génération de cartes schématiques

Les travaux réalisés sur les descriptions d'itinéraires ont abouti au développement d'un algorithme permettant de réaliser des représentations de l'environnement dans lesquels les expériences de navigation ont eu lieues. Ces représentations sont considérées comme des schémas et non comme des cartes de par leur manque des propriétés d'alignement et de distance. L'environnement est ainsi représenté selon les différentes navigations faites par différents utilisateurs et les représentations obtenues sont plus proches de cartes cognitives ou de collages cognitifs.

Les différences entre environnement réel, représenté par une carte, et les schémas générés peuvent permettre d'identifier les éléments les plus saillants pour générer de nouvelles descriptions d'itinéraires et également connaître les éléments qui ne sont pas à considérer pour celles-ci.

La modélisation d'itinéraires développée a été couplée à l'ontologie spatiale SpaceOntology ((BBM10 ; BBC13)). Le processus de fusion de descriptions d'itinéraire a engendré un réseau dont les nœuds représentent les points de passage et les liens les relations spatiales entre ces points (Figure III.2).

Ce réseau a été utilisé comme entrée à un algorithme génétique pour produire une représentation spatiale de l'environnement (BBC16). La Figure III.3 montre une carte schématique générée à partir d'une vingtaine de descriptions d'itinéraires lors d'une course d'orientation.

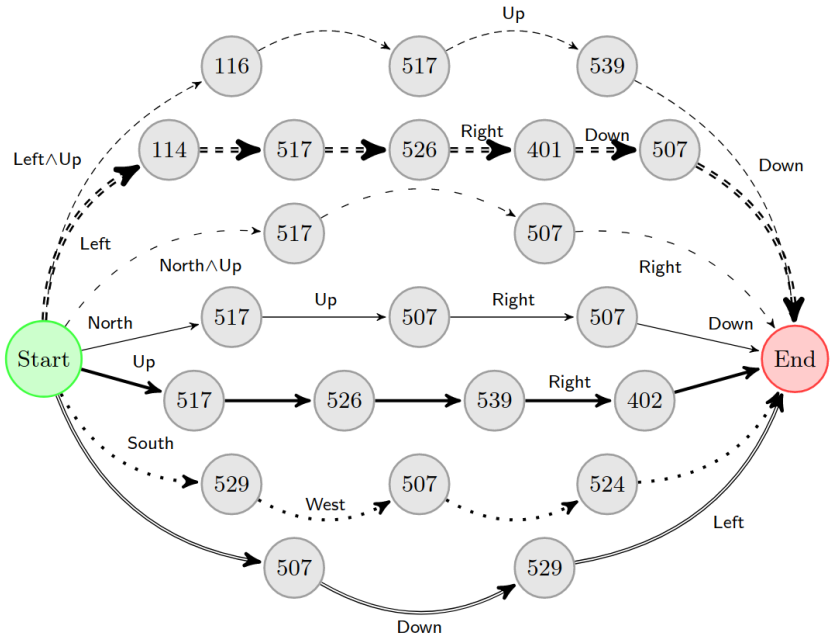


FIGURE III.2 – Fusion de descriptions d'itinéraire (BBC13)

La génération d'itinéraires à partir de descriptions a montré que les repères utilisés étaient différents d'une personne à l'autre et que certains participants avaient suivi des itinéraires plus ou moins directs ou s'étaient trompés dans leur description. Il nous est apparu intéressant de travailler sur l'ensemble des informations contenues dans ces mêmes itinéraires pour en faire une description de l'environnement. À partir d'une ontologie spatiale et de règles de fusion permettant d'identifier les repères décrits identiques, nous avons généré une carte schématique. Le schéma produit à partir des descriptions d'itinéraire permet de vérifier si les descriptions sont correctes et surtout de pouvoir analyser la diversité des itinéraires qui partagent pourtant les mêmes points de départ et d'arrivée et de nombreux points intermédiaires. Les participants ont planifié leur itinéraire en utilisant une carte de course d'orientation, ont parcouru cet itinéraire planifié avec plus ou moins de précision, puis ont décrit l'itinéraire avec encore une fois des biais et des imprécisions. Le résultat de ce travail donne une carte schématique que l'on peut comparer à la carte originale pour améliorer celle-ci et identifier les repères les plus utiles.

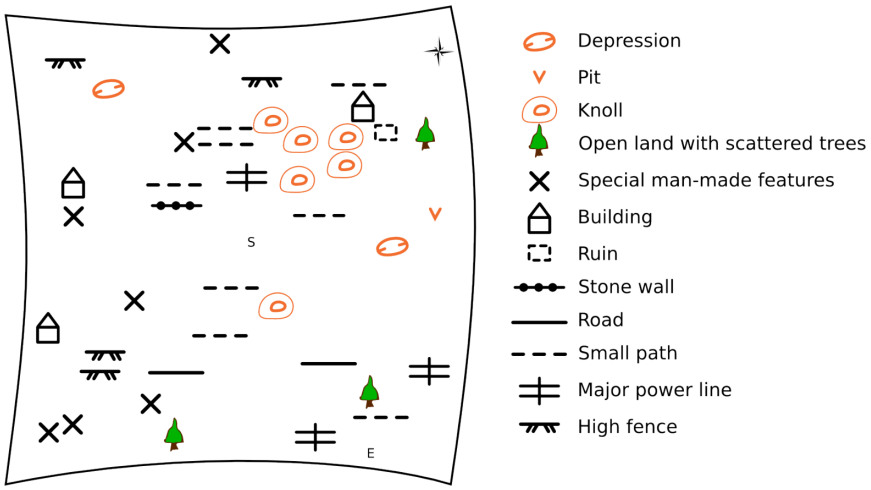


FIGURE III.3 – Carte schématique produite à partir de descriptions verbales d'itinéraires (BBC16)

III.3 Analyse de cyber attaques

L'activité sur les réseaux informatiques est de plus importante en raison de la multiplication des utilisateurs d'Internet (Figure III.4) et du nombre de systèmes connectés dépassant largement le nombre d'habitants sur la planète (4,9 milliards d'utilisateurs d'Internet en 2021 et certaines estimations vont jusqu'à plusieurs dizaines de milliards d'équipements connectés à Internet).

Le nombre d'actes malveillants est en proportion de ce nombre d'équipements. Estimer et qualifier la pression des cyberattaques sur Internet est particulièrement difficile, car les attaques sont peu reportées soit par crainte de mauvaise publicité ou plus probablement, car elles ne sont pas détectées. Deux situations sont seulement possibles de nos jours : nos systèmes sont attaqués et nous avons conscience ; nos systèmes sont attaqués et nous l'ignorons. Il n'est plus possible de connecter un équipement au réseau Internet sans subir un flot continu de cyberattaques (qui sont en grande majorité des tests d'ouverture de ports).

Dans l'optique d'étudier la pression des cyberattaques subies par les équipements reliés à Internet, nous avons développé un ensemble d'opérateurs à partir de la modélisation à base de graphe. Une collecte de données à partir de l'installation de plusieurs serveurs vulnérables (honeypots) dans le monde nous sert de jeux de données (cf. section I.2.1). Les résultats montrent des comportements proches quelque soit le serveur victime considéré, mais permettent de produire des cartes caractérisant les derniers rebonds utilisés (MBBC18a).

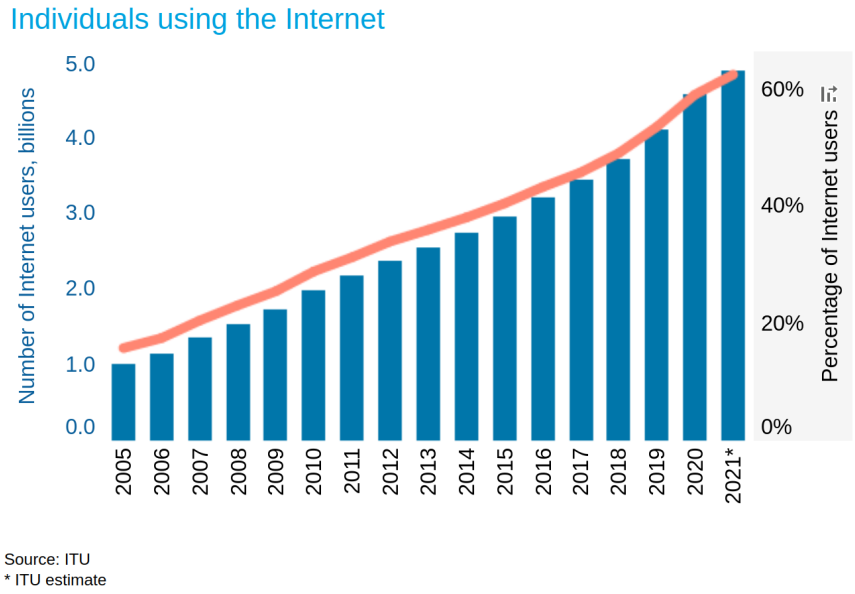


FIGURE III.4 – Évolution du nombre d'utilisateurs d'Internet (source : `https://www.itu.int`)

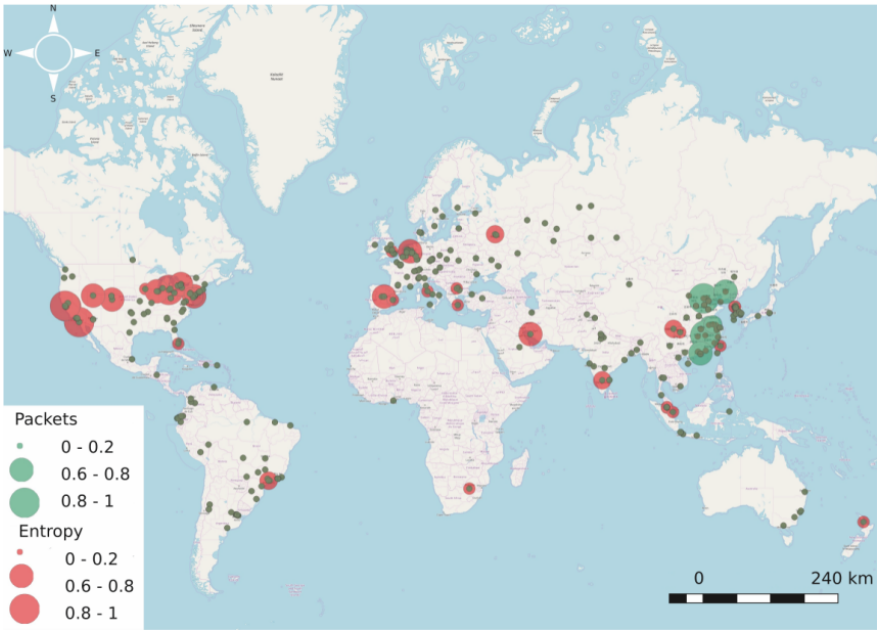


FIGURE III.5 – Répartition de cyberattaques (MBBC18a)

Nous avons calculé l'entropie des intentions pour chaque adresse IP source géolocalisée pour l'ensemble des honeypots. Pour produire des analyses rapidement un plugin a été développé pour le logiciel QGIS permettant de calculer différentes mesures et produire des cartes à partir de capture réseau sous forme de PCAP ou de fichiers CSV.

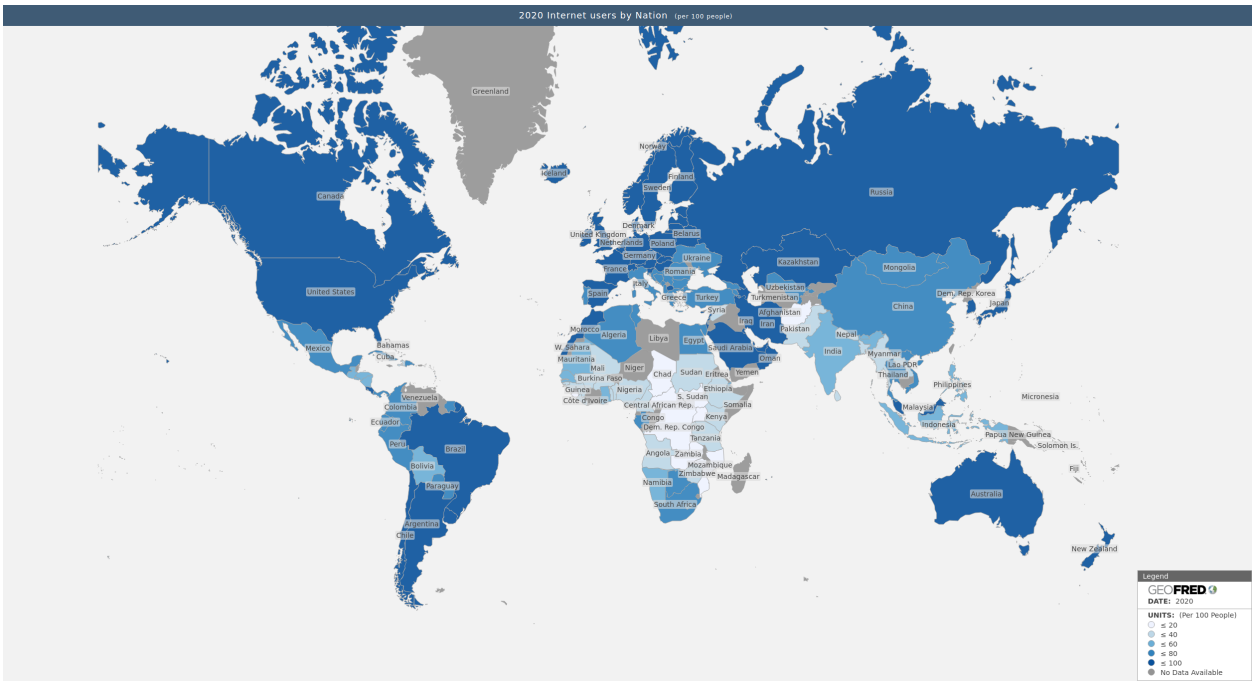


FIGURE III.6 – Répartition des utilisateurs dans le monde en 2020 (source : GEOFRED `https://geofred.stlouisfed.org`)

Nous avons observé une certaine régularité dans les échanges réseau enregistrés avec une périodicité journalière. Cette régularité s'explique en partie par l'enregistrement d'actions automatiques réalisées par des programmes comme les scanneurs de vulnérabilités qui parcourent l'ensemble des adresses IPV4 en permanence.

La Figure III.5 montre le nombre de paquets réseau enregistrés ainsi que le calcul d'entropie sur les intentions. La diversité des attaques est différente selon l'endroit où se trouve le dernier système utilisé pour perpétrer l'attaque. Il faut évidemment prendre en considération que toutes les régions du monde ne possèdent pas un nombre de machines connectées à Internet identique. La figure III.6 montre que le pourcentage d'internautes varie beaucoup d'une région à l'autre. Si le positionnement des hotspots est directement relié à la répartition des systèmes connectés dans le monde, trois régions apparaissent comme particulièrement actives : L'Asie du Sud-Est, les États-Unis et l'Europe de l'Ouest.

L'Asie du Sud-Est apparaît comme la région ayant émis le plus de paquets et possédant le plus d'adresses IP ayant contacté les honeypots. L'entropie des intentions est par contre faible avec une prédominance de l'intention de type contrôle. L'inverse est observé aux États-Unis avec un nombre de paquets reçus plus faible, mais une entropie d'intention importante.

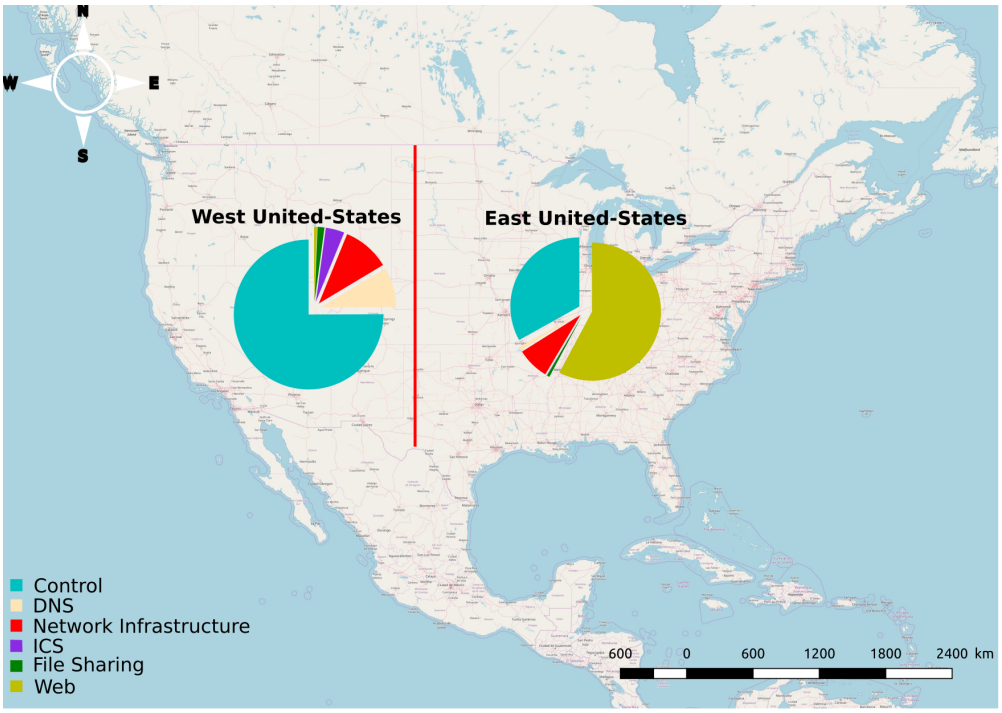


FIGURE III.7 – Différences entre Est et Ouest des États-Unis (MBBC18a)

Au niveau régional, il apparaît que l'entropie d'intention aux États-Unis n'est pas homogène avec une dichotomie marquée entre Est et Ouest (Figure III.7). Le nombre de paquets reste par contre similaire pour l'ensemble du pays. Plus d'intentions de type contrôle sont enregistrées à l'Ouest tandis que c'est l'intention de type Web qui prédomine dans l'Est du pays.

La modélisation des données collectées par les Honeypots mis en place a été complétée par la définition d'opérateurs dont l'entropie d'intention, pour analyser ces données. L'hypothèse initiale était que des différences géographiques peuvent exister. Cette hypothèse a été confirmée notamment par la séparation Est/Ouest aux États-Unis. Cette observation peut s'expliquer par des spécificités entre datacenters à l'Ouest et à l'Est du pays servant de rebond à des scan de vulnérabilités.

III.4 Détection d'anomalies dans les systèmes cyber physiques

L'histoire de l'industrialisation est communément considérée comme ayant quatre grandes phases. La première est l'arrivée des machines à vapeur qui a réellement permis d'atteindre la fabrication de type industriel. Puis les phases d'électrification et d'automatisation ont inséré des composants électronique et de l'informatique dans les processus de fabrication. Enfin, dans la dernière phase, appelée industrie 4.0, l'interconnexion des systèmes et l'utilisation importante d'Internet a transformée l'industrie.

Ainsi les systèmes contrôlant des processus industriels et des équipements physiques sont de plus en plus reliés à Internet. Ces systèmes sont appelés systèmes cyberphysiques (CPS) du fait qu'ils agissent sur l'environnement avec des actionneurs et prennent des décisions grâce à des capteurs. Les conséquences de cyberattaques sur ce type de systèmes peuvent être catastrophiques et mettre en danger l'intégrité physique des opérateurs voire des personnes aux alentours (barrage hydraulique, transport en commun ...).

L'analyse des activités de ce genre de systèmes est particulièrement importante pour la détection d'anomalies dont les cyberattaques font partie. Les systèmes industriels sont de plus en plus impactés par les cyberattaques. Si le vers STUXNET ayant provoqué des dégâts importansL'approche développée s'est basée sur le concept de qualité d'information. La qualité d'information peut être décrite par plusieurs dizaines de paramètres différents pour les CPS. L'idée principale est que le changement des indicateurs de qualité d'information provenant des capteurs de systèmes cyberphysiques peut être le signe d'une cyberattaque en cours.

À partir des expériences menées sur le système industriel composé de deux cuves et décrit dans le chapitre I, plusieurs analyses ont été effectuées. Les données collectées ont été transformées en informations pour être utilisées pour détecter des anomalies. L'imperfection des données et la qualité d'information ont été prises en compte. Données et informations sont souvent confondues. Ces travaux s'appuient sur la pyramide de la connaissance ou hiérarchie du savoir, DIKW (Data Information Knowledge Wisdom) qui permet de bien différencier les deux. Cette pyramide a plusieurs formes dans la littérature et est souvent remise en question, car elle permet d'expliquer et structurer un concept complexe à partir d'une représentation graphique simpliste (Fri09). Elle peut avoir plus de niveaux ou bien être représentée à l'envers pour mettre en avant l'importance des couches hautes ou leur

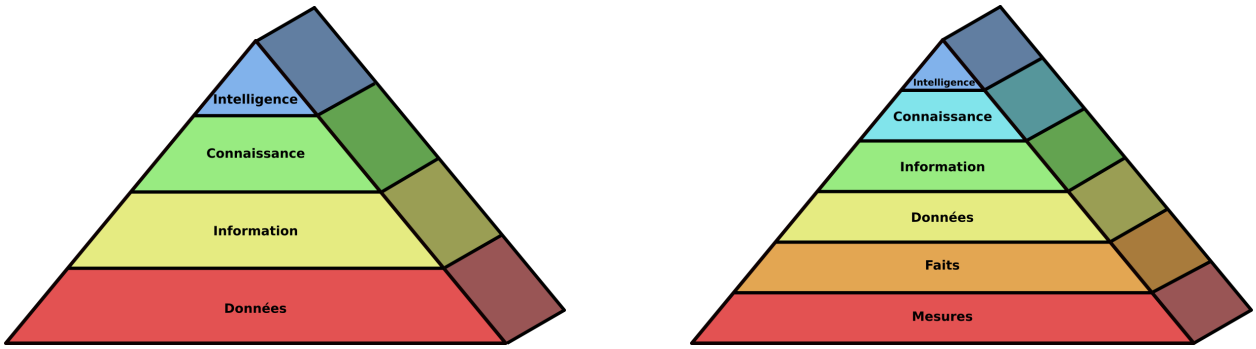


FIGURE III.8 – Pyramide de la connaissance

complexité (Figure III.8).

L'adaptation de la pyramide DIKW à l'étude des systèmes cyberphysiques se fait par la prise en compte du contexte (MLBP17a) :

$$Information = Data + Contexte_{sous-système} + Contexte_{système}$$

À partir des informations provenant des systèmes cyberphysiques, l'imperfection des données et la qualité d'information ont été formalisées. Les vecteurs DQV et IQV représentent respectivement la qualité des données et la qualité des informations :

$$DQV = \{I_1, ..., I_N\}$$

tel que I_k représente la kième imperfection parmi les N possibles

$$IQV = \{D_1, ..., D_M\}$$

tel que D_k représente la kième dimension parmi les M possibles

Les imperfections de la donnée et les dimensions de la qualité d'information sont nombreuses, mais doivent être adaptées pour chaque application. Dans (MLBP17a) 2 imperfections de données et 8 dimensions de qualité d'information ont été utilisées pour détecter des anomalies enregistrées lors de l'expérience de la section I.3 :

— des données erronées I_{err} ;
— des données incomplètes I_{inc} ;
— la précision de la source (le bruit produit par le capteur) D_{sp} ;
— la précision réelle de l'information (le bruit produit par la mesure) D_{rp} ;
— la confiance dans l'information D_{con} ;

— l'erreur de l'information D_{err} ;
— la rapidité de transmission D_{tim} ;
— la cohérence de l'information D_{coh} ;
— la complétude de l'information D_{inc} ;
— l'unicité de l'information (pour savoir si une information est répétée) D_{uni}.

La qualité de la connaissance et la qualité de l'intelligence (algorithmes pour les systèmes cyberphysiques) extraites peuvent également être utilisées pour la détection d'anomalies (ML17).

À partir de ces 8 critères, des niveaux d'acceptation ont été définis permettant de détecter des anomalies sur le système cyberphysique lorsque les valeurs dépassent ces seuils. Les anomalies peuvent être des pannes de capteurs ou de sous-systèmes, des perturbations naturelles ou bien des actes de malveillance intentionnés (actes de sabotage ou cyberattaques). La Figure III.9 illustre l'utilisation des dimensions D_{sp} et D_{rp} pour détecter un acte de sabotage consistant à bloquer physiquement un capteur.

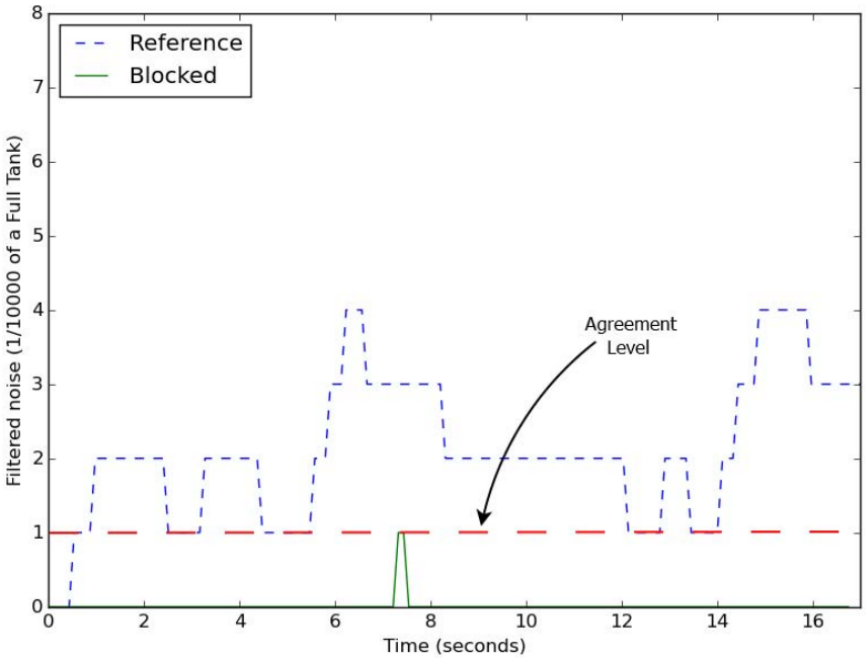


FIGURE III.9 – Exemple de détection d'anomalie en utilisant un niveau d'acceptation (MLBP17a)

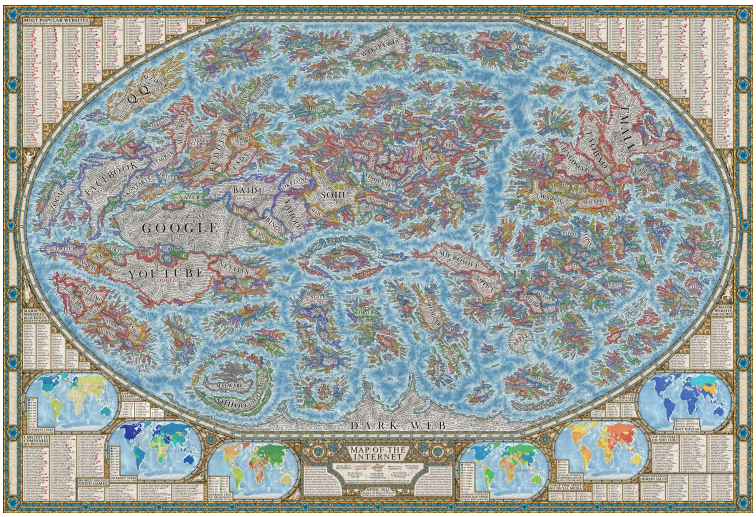


FIGURE III.10 – Représentation cartographie d'Internet (Source : `https://www.halcyonmaps.com/#/map-of-the-internet-2021/`)

Des données issues de l'expérimentation présentée dans la section I.3 sur le système industriel des cuves plusieurs dimensions de qualité de données et d'information ont été définies. Elles ont permis d'identifier des seuils d'acceptation au-dessus (ou en dessous en fonction des dimensions) desquels une anomalie est probable. Cette méthode de détection vient en plus des méthodes de détection de cyberattaques, car elle est particulièrement efficace pour les systèmes cyberphysiques notamment sur les cyberattaques par rejeu.

III.5 Conclusion

L'analyse des activités qu'elles soient réelles ou bien numériques permet de mieux comprendre les interactions entre individus et avec l'environnement. Les résultats obtenus peuvent permettre de développer des politiques de gestion ou bien des moyens de protection plus performants.

La phase de modélisation des données permet de traiter les applications de la même manière sans avoir de spécificités dues au caractère numérique des comportements à analyser. Ainsi, le traitement de descriptions d'itinéraire et celui des attaques sur honeypots sont très proches. La relation de proximité spatiale est remplacée par le lien de communication dans les réseaux numériques.

Cette similarité va jusqu'à représenter des activités numériques sous la forme de cartes pour mieux appréhender les relations entre entités. La Figure III.10 est la génération d'une carte des sites web en fonction du trafic enregistré en 2021.

La pertinence des analyses est directement reliée à la qualité des données en entrée et à la justesse de la modélisation. Mais il faut ajouter à cela la cohérence entre les 3 étapes : Acquisition, Modélisation et Analyse/Représentation. Ces phases doivent partager des granularités (spatiale, temporelle, sémantique) compatibles et surtout avoir été développées dans un objectif commun.

Une dernière étape, qui n'a pas été suffisamment traitée pour l'instant, est la représentation des résultats. Il s'agit d'adapter la visualisation des informations selon le contexte et le profil des utilisateurs et proposer de nouvelles représentations.

Chapitre IV

Conclusions et perspectives

Si les activités humaines sont le point commun de notre recherche les types des activités étudiées sont variés. Les premiers travaux se sont intéressés aux activités de navigation en milieu naturel et en milieu urbain. Dans ce premier cas, la difficulté est d'identifier comment l'humain se déplace et quels sont les repères importants dans l'environnement permettant de construire une représentation mentale de celui-ci. Pour les déplacements multimodaux dans la ville, le profil des acteurs est essentiel pour construire des itinéraires urbains adaptés. Cette importance du profil d'utilisateur est également valable pour la détection d'anomalies dans les systèmes cyberphysiques avec l'identification de la catégorie d'utilisateurs en lien avec le type d'anomalie détectée (panne, cyberattaque ou sabotage). L'analyse d'interaction avec des honeypots a utilisé le concept d'intention pour comprendre les traces réseau enregistrées. L'objectif des intentions manipulées est la compromission de systèmes numériques. Enfin, ces intentions ont été élargies pour prendre en compte l'ensemble des comportements utilisateur pouvant être extraits de traces réseau.

IV.1 Conclusions

Les contributions de la recherche présentée concernent trois grands thèmes : la conception de protocoles expérimentaux pour l'acquisition de données sur les activités humaines ; le développement de modèles pour la représentation et la manipulation des données ; la conception d'approches et algorithmes pour analyser les activités humaines.

L'acquisition de données est ainsi apparue déterminante au cours du temps, car elle conditionne la pertinence de la modélisation et de l'analyse. Ainsi, plusieurs méthodes ont

été utilisées en commençant par des entretiens et aboutissant à la conception d'un cyber-range maritime. L'objectif est d'obtenir des données/mesures adaptées à la modélisation envisagée pour répondre aux questions de recherche fixées. Cette première étape doit garantir l'obtention de la matière première en qualité et quantité suffisante et avec un protocole expérimental reproductible et maîtrisé. Nous nous sommes orientés vers la génération de données afin d'avoir plus de contrôle sur cette phase d'acquisition.

À partir des données acquises, différentes approches de modélisation ont été appliquées en utilisant principalement des graphes. Ce choix s'explique par l'omniprésence d'entités reliées entre elles soit par des relations spatiales, comme les descriptions d'itinéraire ou les déplacements urbains multimodaux, soit par des interactions entre systèmes numériques dans le cas des honeypots.

Les analyses réalisées ont démontré la difficulté d'identifier un caractère "normal" dans les données à disposition. En effet, pour l'analyse de trafic réseau ou la détection d'anomalies dans les systèmes cyberphysiques, il s'agit de mesurer l'écart à un comportement nominal des individus ou des systèmes. Dans le cas du trafic réseau, il faut identifier le "network baseline" qui émerge alors que pour l'identification d'anomalies il est important de définir des niveaux d'acceptation d'écart à la normale.

IV.2 Perspectives

Les travaux futurs concernent exclusivement les activités numériques dans le domaine de la cybersécurité. En effet, depuis 6 ans, nos travaux se sont orientés vers la modélisation et la détection de cyberattaques.

Quatre thématiques différentes sont considérées dans les prochaines années :

1. L'aide à la décision en cas de cyberattaques avec une approche de représentation visuelle multidécideurs ;
2. L'amélioration de la détection des cyberattaques en prenant l'angle de la création de données d'entraînement spécifiques pour les sondes comportementales utilisant l'apprentissage automatique ;
3. L'analyse des comportements dans le cyberespace couplée aux méthodes de détection pour une meilleure appréhension des cyberattaques ;
4. La sécurisation des réseaux en environnements industriels.

IV.2.1 Visualisation de situation cyber

L'ensemble des travaux de recherche présentés concernent les activités humaines. Ces activités peuvent avoir lieu dans le monde réel ou bien dans le monde numérique. Une des perspectives de travail concerne une meilleure prise en compte de l'humain dans les analyses faites à partir de traces numériques, notamment dans le cas de cyberattaques.

Le rôle de l'humain en cybersécurité est souvent considéré comme négatif, car de nombreux incidents sont imputables à des erreurs humaines, les systèmes numériques étant plus fiables pour la prise de décisions dans des situations connues. Néanmoins, pour certains scénarios rares ou dans le cas de défaillances de systèmes, l'humain peut être vu comme le dernier rempart.

L'équilibre entre réponse automatique par un système numérique ou d'aide à la décision est un problème complexe et fortement contextuel. Une réponse automatique n'est pas toujours une solution satisfaisante, mais une aide à la décision apportée par un système numérique, sans explication du processus qui a amené le système à choisir l'action préconisée, n'est pas non plus toujours acceptable.

Le travail dans cette thématique visera à coupler des méthodes d'aide à la décision avec les travaux réalisés sur la visualisation d'incidents cyber. L'amélioration de la cybersituationnal awareness peut être faite par des représentations visuelles adaptées à la fois au contexte, notion dont les limites sont difficiles à cerner, et aux opérateurs et décideurs. L'idée principale est de générer des graphiques dynamiquement en fonction de la situation et de l'utilisateur. Les verrous scientifiques concernent en premier lieu la définition de la notion de contexte et l'identification de ces différents contextes dans le cadre de cyberattaques. Un deuxième verrou qui devra être traité est la définition des différents types de visualisations graphiques possibles des données utilisées et des formes de graphiques. La méthode d'apprentissage comme le processus d'aide à la décision sont confrontés à plusieurs limites. Accéder à des ensembles de données d'apprentissage étiquetées et cohérent pour l'application voulue est toujours difficile. L'échantillon d'apprentissage sera constitué des choix de visualisations d'opérateurs en fonction de la situation cyber. Afin d'être le mieux acceptée possible, l'aide à la décision devra pouvoir cohabiter avec des personnalisations utilisateurs. Les choix des visualisations proposées devront également être expliqués un minimum afin que l'opérateur ait confiance dans le système.

IV.2.2 Entraînement des sondes de détection de cyberattaques

Si une meilleure visualisation de la situation cyber améliore la prise de décision en cas de cyberattaques, la détection d'incidents cyber reste encore un défi. Avec l'augmentation des communications numériques et du nombre de périphériques, deux uniques cas de figure existent aujourd'hui : les systèmes numériques subissent des cyberattaques et les opérateurs sont ("bien") au courant de la situation ; et les systèmes numériques sont sous le feu de cyberattaques et les opérateurs l'ignorent. Le cas de figure où les systèmes ne sont pas attaqués n'existe pas.

En outre, les attaques deviennent de plus en plus sophistiquées et les outils des attaquants sont de plus en plus performants et accessibles et les surfaces d'attaques sont de plus en plus importantes avec l'IOT (Internet Of Things), IIOT (Industrial Internet of Things) et finalement l'IOE (Internet Of Everything). La détection d'attaques se fait à partir de signatures ou bien de comportements. Les attaques sont de plus en plus originales et sont souvent des zéros-day, c'est-à-dire des vulnérabilités qui n'ont pas encore été identifiées ni résolues.

Ainsi, les systèmes de détection de cyberattaques basés sur la détection de comportements anormaux sont porteurs de beaucoup d'espoir avec leur capacité à détecter des attaques avec des méthodes qui n'ont pas encore été découvertes. Ces sondes de détection de cyberattaques reposent pour la plupart sur des algorithmes d'apprentissage automatique nécessitant donc une phase d'apprentissage avec des données étiquetées. Un point dur pour les méthodes d'intelligence artificielle pour la classification est d'avoir à disposition un ensemble de données étiquetées suffisamment important pour apprendre les caractéristiques des données.

En effet, si l'entraînement de ces sondes est crucial pour obtenir de bonnes performances de détection, les jeux d'entraînements disponibles sont insuffisants et souvent inadaptés au contexte d'emploi. Le développement d'une méthodologie de production de jeux de données d'apprentissage en commençant par la définition formelle du contexte applicatif, permettra d'améliorer l'efficacité de détection des cyberattaques.

Les travaux de génération de trafic réseau ont montré qu'il était possible de produire des jeux de données de réseau spécifiques. Ces traces sont issues de réseaux virtuels afin de produire des données en quantité avec les mêmes propriétés. Les jeux de données contenant de réelles attaques sont rares, voire inexistants. C'est particulièrement le cas pour certains

domaines comme les systèmes industriels maritimes, la production de données intégrant ces anomalies est donc essentielle. De plus, en ce qui concerne les systèmes critiques, et particulièrement les systèmes cyberphysiques des industries, les jeux de données ne sont pas publics et il est difficile (impossible) d'obtenir un compromis entre anonymisation et précision des données.

L'analyse précise des traces réseau sur les systèmes complexes de type industriels permet d'extraire les caractéristiques pour la génération de traces réseau similaires. La modélisation présentée dans la section II.4 fournit la méthodologie d'analyse.

L'approche retenue est celle d'utiliser des techniques d'intelligence artificielle et plus spécifiquement de simulation multiagent pour la production de comportements légitimes ou des cyberattaques. Ce mécanisme de génération de comportements est probabiliste et permettra d'obtenir des données plus réalistes. Cela ne permet pourtant pas d'avoir des informations sur le réalisme, la pertinence et la qualité des enregistrements produits.

Afin de répondre à ce défi méthodologique, nous prévoyons d'utiliser des réseaux antagonistes génératifs ou GANs (Generative Adversarial Network). L'idée principale est de mettre en confrontation deux algorithmes d'IA, un générateur et un discriminateur jusqu'à ce que le discriminateur n'arrive plus à déterminer les traces artificielles des traces réelles. Outre le problème fréquent de convergence de ces méthodes, elles manipulent des données continues ce qui pose problème pour utiliser des données réseau dont les valeurs, bien que numériques, ne sont pas des nombres comme les numéros de ports de communication. (RSLH19) ont montré l'intérêt des GAN sur la génération de flux réseau. Notre approche consisterait à manipuler les données de la simulation multiagent afin de produire des traces réseau de qualité et identifier comment manipuler des attributs de traces réseau.

IV.2.3 Détection d'événements à partir de traces numériques

La spatialisation des événements comme des infrastructures supportant le réseau internet est une clé de compréhension déterminante de la modélisation conceptuelle et spatiale du cyberespace. Elle permet également d'identifier comment les menaces cyber se propagent. Les communications qui parcourent l'espace numérique laissent des traces qui génèrent des opportunités d'étude par analyse automatisée afin de décrire le caractère réticulaire et protéiforme du cyberespace.

Ce travail commencé par l'analyse de la dynamique d'humeurs sur Twitter (WBB15a ;

WBB+15b) et l'approche honeypots réseau présentée, s'élargira par la prise en compte de données mises à dispositions ou captées par le déploiement de filtres (serveurs répartis géographiquement). La représentativité de ces données est en soi une question déterminante tant les opérateurs d'internet et les agences nationales bornent de manière floue les processus de filtrage. C'est là un objectif secondaire de cette étude : tester l'hypothèse de la mise à disposition d'un échantillon fiable des données proposées par les grands opérateurs mondiaux d'internet, avec pour but de connaître la façon d'opérer et le degré de complétude des échantillons analysés. Il s'agit de tenter d'évaluer les biais d'acquisition de données hétérogènes et leurs impacts d'un point de vue source, temporalité et nature.

IV.2.4 Sécurisation des réseaux en environnements industriels : prototype de switch intelligent

À l'heure actuelle, il n'existe pas ou très peu de normes ou certifications en cybersécurité au niveau des équipements réseau (Com17). Il existe surtout un ensemble de bonnes pratiques pour les sécuriser. De plus en plus d'entreprises commencent à se pencher sur la question pour leurs systèmes toujours plus connectés et par conséquent exposés aux attaques.

L'objectif de cette étude est de proposer des solutions pour améliorer la sécurité des équipements réseau dans le but de prévenir certaines attaques et comportements malveillants. Par exemple, un pare-feu procure un premier filtre de sécurité, mais reste tout de même plus ou moins contournable une fois une source autorisée identifiée, surtout si l'attaque vient d'un employé ou directement de l'intérieur. L'ajout d'un ou plusieurs contrôles supplémentaires sur un switch permettrait de mieux anticiper et bloquer les attaques, ou a minima la contenir pour éviter toute propagation. Une analyse du trafic, même chiffré, permettrait de prévenir certains comportements malveillants.

L'idée principale est bien de faire une première analyse du trafic afin de délester les éléments réseau chargés de protéger le réseau comme les pare-feu et les sondes de détection d'intrusion réseau (NIDS). En aucun cas, il ne s'agira de se substituer aux différentes barrières de cybersécurité, mais d'améliorer la défense en profondeur des réseaux de type industriel.

Ce type de défense provient du domaine militaire et a pour principe de multiplier les obstacles afin d'empêcher et freiner la progression d'agresseurs. Le principe de ce modèle de défense a été formalisé dans les années 60 pour la sûreté du nucléaire civil. Trois niveaux de protection ont ainsi été définis. L'accident de Three mile island en 1979 a mis à mal les

trois premiers niveaux de défense et un 4e niveau a été défini à la suite de cet accident. Puis un 5e niveau a été ajouté afin de limiter la contamination de la population et de l'environnement. La catastrophe de Fukishima en 2011, n'a pas remis en cause les principes de la défense en profondeur à 5 niveaux, mais a généré des progrès technologiques au sein des premières couches et a montré l'importance des aspects humains et organisationnels face à de tels accidents. Il s'agit ainsi d'un modèle qui évolue et s'adapte en fonction des retours d'expériences et des progrès technologiques. Notre but est ainsi de contribuer à son amélioration dans le domaine de la cybersécurité.

Le concept de défense en profondeur a été adapté à la sécurité des systèmes d'information dans les années 2000 (DCS04) et formalisé plus récemment par l'Agence Nationale de la Sécurité (NSA) américaine (Nat10). Elle s'oppose au modèle de défense en largeur (Cle13) qui est le renforcement d'un seul niveau de défense. Ces deux approches sont à combiner pour sécuriser un système complexe. Trois niveaux sont généralement considérés dans la défense en profondeur :

— Les opérateurs ;
— Les procédures ;
— Les technologies.

C'est sur ce dernier niveau que nos travaux vont porter en ajoutant de nouvelles capacités d'identification de trafic réseau dans les éléments réseau. Ce concept peut être remis en question, car un des points importants de la défense en profondeur dans le monde militaire est l'augmentation de la vulnérabilité de l'attaquant au fur et à mesure qu'il franchit les couches de protection. Or, un cyberattaquant ne reste pas piégé lorsqu'il a franchi plusieurs couches ni ne devient plus vulnérable à notre connaissance. C'est un point intéressant à étudier avec des actions proportionnelles à la profondeur du niveau concerné dans le réseau.

L'originalité de la méthode reposera sur une modélisation de classification/identification de trafic réseau robuste. Ce modèle sera ensuite transformé en algorithmes pour être implémenté pour deux objectifs distincts :

— L'identification de trafic réseau légitime et illégitime afin d'alléger les mécanismes de défense des infrastructures ;
— la génération de trafic réseau permettant de renforcer la protection du réseau contre les cyberattaques (DCRS12).

La classification de trafic réseau est un thème de recherche très actif dont le but est d'identifier le trafic légitime et illégitime (AY20 ; ID19 ; RL20 ; UQQAF19). Ces méthodes fonctionnent également sur du trafic réseau chiffré comme celui produit par le réseau TOR

(BFE+20 ; KA18 ; CMMV17 ; LDGMG17). Dans la même thématique, de recherches sont menées pour lutter contre les méthodes d'analyse statistique de trafic réseau (DCRS12 ; WCM09).

Les tests des nouveaux matériels et programmes informatiques seront faits sur le cyberrange maritime permettant d'évaluer au plus près les conséquences des cyberattaques sur des systèmes réels, les méthodes de détection ainsi que les méthodes de remédiation.

Bibliographie

[ABL+22] Ramla Abdelkader, Clet Boudehenn, Maxence Lannuzel, Jean-Christophe Cexus, and David Brosset. Hollistic approach of integrated navigationequipment for cybersecurity at sea. *Under Review*, 2022. I.4.2

[ADD+05] E Alata, M Dacier, Y Deswarte, M Kaâniche, K Kortchinsky, V Nicomette, VH Pham, and F Pouget. Leurré. com : retour d'expérience sur plusieurs mois d'utilisation d'un pot de miel distribué mondialement. In *Proceedings of the Symposium Sur La Sécurité des Technologies de l'Information et des Communications, June*, pages 1–3, 2005. I.2.1

[ANK+06] Eric Alata, Vincent Nicomette, Mohamed Kaâniche, Marc Dacier, and Matthieu Herrb. Lessons learned from the deployment of a high-interaction honeypot. In *2006 Sixth European Dependable Computing Conference*, pages 39–46. IEEE, 2006. I.2.1

[AY20] Nour Alqudah and Qussai Yaseen. Machine learning for traffic analysis : a review. *Procedia Computer Science*, 170 :911–916, 2020. IV.2.4

[BBB+17] Thomas Becmeur, Xavier Boudvin, David Brosset, Gaël Héno, Benjamin Coste, Yvon Kermarrec, and Pedro Merino Laso. Generating data sets as inputs of reference for cyber security issues and industrial control systems. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, pages 453–454. IEEE, 2017. I.4

[BBC13] Lamia Belouaer, David Brosset, and Christophe Claramunt. Modeling spatial knowledge from verbal descriptions. In *International Conference on Spatial Information Theory*, pages 338–357. Springer, 2013. (document), III.2, III.2

[BBC16] Lamia Belouaer, David Brosset, and Christophe Claramunt. From verbal route descriptions to sketch maps in natural environments. In *Proceedings of the 24th acm sigspatial international conference on advances in geographic information systems*, pages 1–10, 2016. (document), III.2, III.3

[BBM10] Lamia Belouaer, Maroua Bouzid, and Abdel-Illah Mouaddib. Ontology based spatial planning for human-robot interaction. In *2010 17th International Symposium on Temporal Representation and Reasoning*, pages 103–110. IEEE, 2010. III.2

[BC11] David Brosset and Christophe Claramunt. An experimental ant colony approach for the geolocation of verbal route descriptions. *Knowledge-Based Systems*, 24(4) :484–491, 2011. III.1

[BCS08a] David Brosset, Christophe Claramunt, and Eric Saux. An acs cooperative learning approach for route finding in natural environment. In *Proceedings of the 16th ACM SIGSPATIAL international conference on Advances in geographic information systems*, pages 1–8, 2008. III.1

[BCS08b] David Brosset, Christophe Claramunt, and Eric Saux. An experimental ant colony approach for the spatialization of verbal route descriptions. In *International Workshop on Computational Models of Place PLACE'08*, page 45, 2008. III.1

[BFE+20] Lamiaa Basyoni, Noora Fetais, Aiman Erbad, Amr Mohamed, and Mohsen Guizani. Traffic analysis attacks on tor : a survey. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pages 183–188. IEEE, 2020. IV.2.4

[BJH+19] Xavier Bellekens, Gayan Jayasekara, Hanan Hindy, Miroslav Bures, David Brosset, Christos Tachtatzis, and Robert Atkinson. From cyber-security deception to manipulation and gratification through gamification. In *International Conference on Human-Computer Interaction*, pages 99–114. Springer, 2019. I.2.1

[Bla19] Todd JB Blayone. Theorising effective uses of digital technology with activity theory. *Technology, Pedagogy and Education*, 28(4) :447–462, 2019. (document), 3

[Bro08] D Brosset. *Description d'itinéraire en milieu naturel : modèle intégré de description verbale et de représentation spatiale au sein des systèmes d'information géographique*. PhD thesis, Arts et Métiers Paritech, 2008. (document), I.1, I.1, III.1

[Bur18] Matt Burgess. Strava's data lets anyone see the names (and heart rates) of people exercising on military bases. *Wired UK*, 30, 2018. (document)

[CBP95] Kimberly C. Claffy, H-W Braun, and George C. Polyzos. A parameterizable methodology for internet traffic flow profiling. 13(8) :1481–1494, 1995. II.4.2

[Cle13] Lance Cleghorn. Network defense methodology : A comparison of defense in depth and defense in breadth. 2013. IV.2.4

[CMMV17] Alfredo Cuzzocrea, Fabio Martinelli, Francesco Mercaldo, and Gianni Vercelli. Tor traffic analysis and detection via machine learning techniques. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 4474–4480. IEEE, 2017. IV.2.4

[Com17] Common criteria for information technology security evaluation, cc v3.1. release 5. https ://www.commoncriteriaportal.org/cc/, 2017. IV.2.4

[CVM+15] Carlos Garcia Cordero, Emmanouil Vasilomanolakis, Nikolay Milanov, Christian Koch, David Hausheer, and Max Mühlhäuser. Id2t : A diy dataset creation toolkit for intrusion detection systems. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pages 739–740. IEEE, 2015. II.4.1

[CVW+21] Carlos Garcia Cordero, Emmanouil Vasilomanolakis, Aidmar Wainakh, Max Mühlhäuser, and Simin Nadjm-Tehrani. On generating network traffic datasets with synthetic attacks for intrusion detection. *ACM Transactions on Privacy and Security (TOPS)*, 24(2) :1–39, 2021. II.4.1

[DCRS12] Kevin P Dyer, Scott E Coull, Thomas Ristenpart, and Thomas Shrimpton. Peek-a-boo, i still see you : Why efficient traffic analysis countermeasures fail. In *2012 IEEE symposium on security and privacy*, pages 332–346. IEEE, 2012. IV.2.4

[DCS04] DCSSI. Mémento sur le concept de la défense en profondeur appliqué aux si. Technical report, Secrétariat général de la défense nationale, 2004. IV.2.4

[Den97] Michel Denis. The description of routes : A cognitive approach to the production of spatial discourse. *Current Psychology of Cognition*, 16 :409–458, 1997. (document), I.1, I.1, I.1, II.1.1, II.1

[DH12] Sherri Davidoff and Jonathan Ham. *Network forensics : tracking hackers through cyberspace*, volume 2014. Prentice hall Upper Saddle River, 2012. I.2

[Eng87] Y Engestrom. Learning by expanding : An activity-theoretical approach to developmental research. helsinki : Orienta-konsultit, 1987. (document), 2

[Eng01] Yrjö Engeström. Expansive learning at work : Toward an activity theoretical reconceptualization. *Journal of education and work*, 14(1) :133–156, 2001. (document)

[Fer17] Stênio Fernandes. Internet traffic profiling. In *Performance Evaluation for Network Services, Systems and Protocols*, pages 113–152. Springer, 2017. I.2

[FP01] Sally Floyd and Vern Paxson. Difficulties in simulating the internet. *IEEE/ACm Transactions on Networking*, 9(4) :392–403, 2001. I.2

[Fri09] Martin Frické. The knowledge pyramid : a critique of the dikw hierarchy. *Journal of information science*, 35(2) :131–142, 2009. III.4

[GK12] Ashish Girdhar and Sanmeet Kaur. Comparative study of different honeypots system. *International Journal of Engineering Research and Development e-ISSN*, pages 23–27, 2012. I.2.1

[Häg70] Torsten Hägerstrand. What about people in regional science ? In *Papers of the Regional Science Association*, volume 24, pages 6–21. Springer, 1970. (document), 4

[HBB+18] Hanan Hindy, David Brosset, Ethan Bayne, Amar Seeam, Christos Tachtatzis, R Atkinson, and X Bellekens. A taxonomy and survey of intrusion detection system design techniques. *Netw. Threats Datasets*, 2018. II.4.1

[HBB+20] Hanan Hindy, David Brosset, Ethan Bayne, Amar Kumar 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*, 8 :104650–104675, 2020. II.4.1

[ID19] Auwal Sani Iliyasu and Huifang Deng. Semi-supervised encrypted traffic classification with deep convolutional generative adversarial networks. *IEEE Access*, 8 :118–126, 2019. IV.2.4

[Jac21] Olivier Jacq. *Détection, analyse contextuelle et visualisation de cyber-attaques en temps réel : élaboration de la Cyber Situational Awareness du monde maritime.* Theses, Ecole nationale supérieure Mines-Télécom Atlantique, January 2021. I

[JBC14] Ines Jguirim, David Brosset, and Christophe Claramunt. Functional and structural analysis of an urban space extended from space syntax. In *8th International Conference on Geographic Information Science,Vienna, Austria*, 2014. (document), II.4

[Jgu16] Ines Jguirim. *Modélisation et génération d'itinéraires contextuels d'activités urbaines dans la ville.* PhD thesis, 2016. (document), II.2.1, II.5, II.6, II.7

[JR86] Raj Jain and Shawn Routhier. Packet trains–measurements and a new model for computer network traffic. 4(6) :986–995, 1986. II.4.2

[KA18] Minsu Kim and Alagan Anpalagan. Tor traffic classification from raw packet header using convolutional neural network. In *2018 1st IEEE International Conference on Knowledge Innovation and Invention (ICKII)*, pages 187–190. IEEE, 2018. IV.2.4

[KNSM21] Stan Karanasios, Bonnie Nardi, Clay Spinuzzi, and Julien Malaurent. Moving forward with activity theory in a digital world. *Mind, Culture, and Activity*, pages 1–20, 2021. (document)

[KRF11] W Richard Stevens Kevin R Fall. *TCP/IP Illustrated, Volume 1 : The Protocols.* Professional Computing. Addison-Wesley Professional, 2 edition, 2011. II.4.2

[LDGMG17] Arash Habibi Lashkari, Gerard Draper-Gil, Mohammad Saiful Islam Mamun, and Ali A Ghorbani. Characterization of tor traffic using time based features. In *ICISSp*, pages 253–262, 2017. II.4.2, IV.2.4

[Leo78] A. N. Leont'ev. *Activity, Consciousness, and Personality.* Prentice-Hall Englewood Cliffs, Nj, 1978. (document)

[LOY05] Bernhard Lorenz, Hans Jürgen Ohlbach, and Laibing Yang. Ontology of transportation networks. 2005. II.2.2

[LPC+04] Anukool Lakhina, Konstantina Papagiannaki, Mark Crovella, Christophe Diot, Eric D. Kolaczyk, and Nina Taft. Structural analysis of network traffic flows. In *Proceedings of the joint international conference on Measurement and modeling of computer systems*, SIGMETRICS '04/Performance '04, pages 61–72, New York, NY, USA, #jun# 2004. Association for Computing Machinery. II.4.2

[MBBC18a] Thibaud Mérien, Xavier Bellekens, David Brosset, and Christophe Claramunt. A spatio-temporal entropy-based approach for the analysis of cyber attacks (demo paper). In *Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pages 564–567, 2018. (document), III.3, III.5, III.7

[MBBC18b] Thibaud Merien, David Brosset, Xavier Bellekens, and Christophe Claramunt. A human-centred model for network flow analysis. In *2018 2nd Cyber Security in Networking Conference (CSNet)*, pages 1–6. IEEE, 2018. II.3.2

[Mil08] Harvey J. Miller. *Time Geography*, pages 1151–1156. Springer US, Boston, MA, 2008. (document)

[ML17] Pedro Merino Laso. *Détection de dysfonctionements et d'actes malveillants basée sur des modèles de qualité de données multi-capteurs*. PhD thesis, Chaire de cyberdéfense des systèmes navals, 2017. Thèse de doctorat dirigée par Puentes, John Informatique Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire 2017. (document), I, I.3, I.7, III.4

[MLBP17a] Pedro Merino Laso, David Brosset, and John Puentes. Analysis of quality measurements to categorize anomalies in sensor systems. In *2017 Computing Conference*, pages 1330–1338. IEEE, 2017. (document), I.3, III.4, III.9

[MLBP17b] Pedro Merino Laso, David Brosset, and John Puentes. Dataset of anomalies and malicious acts in a cyber-physical subsystem. *Data in brief*, 14 :186–191, 2017. I.3

[Nat10] National Security Agency. Defense in depth : A practical strategy for achieving information assurance in today's highly networked environments. Technical report, 2010. IV.2.4

[NBH+19] Maël Nogues, David Brosset, Hanan Hindy, Xavier Bellekens, and Yvon Kermarrec. Labelled network capture generation for anomaly detection. In *International Symposium on Foundations and Practice of Security*, pages 98–113. Springer, 2019. (document), I.4, I.5, I.6

[NWS+16] Marcin Nawrocki, Matthias Wählisch, Thomas C Schmidt, Christian Keil, and Jochen Schönfelder. A survey on honeypot software and data analysis. *arXiv preprint arXiv :1608.06249*, 2016. I.2.1

[OP13] Martin Oliver and Caroline Pelletier. Activity theory and learning from digital games : developing an analytical methodology. pages 79–100, 2013. (document)

[PM04] Edyta Przytula-Machrouh. *Information verbale et information graphique pour la description d'itinéraires*. Unpublished PhD report, Université René Descartes, France, 2004. I.1, I.1, I.1, II.1.1

[PMLB18] John Puentes, Pedro Merino Laso, and David Brosset. The challenge of quality evaluation in fraud detection. *Journal of Data and Information Quality (JDIQ)*, 10(2) :1–4, 2018. I.3

[RL20] Shahbaz Rezaei and Xin Liu. Multitask learning for network traffic classification. In *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, pages 1–9. IEEE, 2020. IV.2.4

[RSLH19] Markus Ring, Daniel Schlör, Dieter Landes, and Andreas Hotho. Flow-based network traffic generation using generative adversarial networks. *Computers & Security*, 82 :156–172, 2019. IV.2.2

[SGLG18] Iman Sharafaldin, Amirhossein Gharib, Arash Habibi Lashkari, and Ali A Ghorbani. Towards a reliable intrusion detection benchmark dataset. *Software Networking*, 2018(1) :177–200, 2018. II.4.1

[Sha20] Faisal Shaman. *User profiling based on network application traffic monitoring*. PhD thesis, University of Plymouth, 2020. I.2

[Sto05] Cliff Stoll. *The cuckoo's egg : tracking a spy through the maze of computer espionage*. Simon and Schuster, 2005. I.2.1

[SW49] C.E. Shanon and W. Weaver. *The Mathematical Theory of Communication*. University of Illinois, 1949. II.1.3

[UQQAF19] Muhammad Usama, Adnan Qayyum, Junaid Qadir, and Ala Al-Fuqaha. Black-box adversarial machine learning attack on network traffic classification. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 84–89. IEEE, 2019. IV.2.4

[VC78] Lev Semenovich Vygotsky and Michael Cole. *Mind in society : Development of higher psychological processes*. Harvard university press, 1978. (document)

[VSO17] Eduardo K Viegas, Altair O Santin, and Luiz S Oliveira. Toward a reliable anomaly-based intrusion detection in real-world environments. *Computer Networks*, 127 :200–216, 2017. II.4.1

[WBB15a] Shoko WAKAMIYA, Lamia BELOUAER, and David BROSSET. Exploring geographical crowd's emotions with twitter. *DBSJ journal*, 13(1) :77–82, 2015. IV.2.3

[WBB+15b] Shoko Wakamiya, Lamia Belouaer, David Brosset, Ryong Lee, Yukiko Kawai, Kazutoshi Sumiya, and Christophe Claramunt. Measuring crowd mood in city space through twitter. In *International Symposium on Web and Wireless Geographical Information Systems*, pages 37–49. Springer, 2015. IV.2.3

[WCM09] Charles V Wright, Scott E Coull, and Fabian Monrose. Traffic morphing : An efficient defense against statistical traffic analysis. In *NDSS*, volume 9. Citeseer, 2009. IV.2.4

[Wil94] Theodore J Williams. The purdue enterprise reference architecture. *Computers in industry*, 24(2-3) :141–158, 1994. I.4.1

[YR15] Tarun Yadav and Arvind Mallari Rao. Technical aspects of cyber kill chain. In *International Symposium on Security in Computing and Communication*, pages 438–452. Springer, 2015. II.3.1

Production Scientifique

Revues internationales

[1] Mohamed Amine Ben Farah, Elochukwu Ukwandu, Hanan Hindy, David Brosset, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. Cyber security in the maritime industry: a systematic survey of recent advances and future trends. *Information*, 13(1):22, 2022.

[2] 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.

[3] Iwan Le Berre and David Brosset. Aide à la décision par l'identification de formes d'urbanisation: application au littoral breton. *Cybergeo: European Journal of Geography*, 2020.

[4] Elochukwu Ukwandu, Mohamed Amine Ben Farah, Hanan Hindy, David Brosset, Dimitris Kavallieros, Robert Atkinson, Christos Tachtatzis, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, 20(24):7148, 2020.

[5] Hanan Hindy, David Brosset, Ethan Bayne, Amar Seeam, and Xavier Bellekens. Improving siem for critical scada water infrastructures using machine learning. In *Computer Security*, pages 3–19. Springer, Cham, 2018.

[6] Hanan Hindy, David Brosset, Ethan Bayne, Amar Seeam, Christos Tachtatzis, R Atkinson, and X Bellekens. A taxonomy and survey of intrusion detection system design techniques. *Network Threats Datasets*, 2018.

[7] John Puentes, Pedro Merino Laso, and David Brosset. The challenge of quality evaluation in fraud detection. *Journal of data and information quality*, 10(2):5–1, 2018.

[8] Pedro Merino Laso, David Brosset, and John Puentes. Dataset of anomalies and malicious acts in a cyber-physical subsystem. *Data in brief*, 14:186–191, 2017.

[9] Damien Le Guyader, Cyril Ray, and David Brosset. Identifying small-scale fishing zones in France using AIS data. *Advances in Shipping Data Analysis and Modeling: Tracking and Mapping Maritime Flows in the Age of Big Data*, 2017.

[10] Damien Le Guyader, Cyril Ray, Françoise Gourmelon, and David Brosset. Defining high-resolution dredge fishing grounds with automatic identification system (ais) data. *Aquatic Living Resources*, 30:39, 2017.

[11] Cecile Guegan, Cyril Tissot, Sebastien Kervern, David Brosset, Solenn Le Berre, and Louis Brigand. Monitoring and modeling visitors flows: application to the mont-saint-michel. *Cybergeo: European Journal of Geography*, 2015.

[12] Shoko Wakamiya, Lamia Belouaer, David Brosset, Yukiko Kawai, Christophe Claramunt, and Kazutoshi Sumiya. Exploring geographical crowd's emotions with twitter. *Information and Media Technologies*, 10(2):357–362, 2015.

[13] Didier G Leibovici, Christophe Claramunt, Damien Le Guyader, and David Brosset. Local and global spatio-temporal entropy indices based on distance-ratios and co-occurrences distributions. *International Journal of Geographical Information Science*, 28(5):1061–1084, 2014.

[14] Nicolas Maslov, David Brosset, Christophe Claramunt, and Jean-Frederic Charpentier. A flexible decision-aid system for sites selection and technology options for a marine energy system. 2014.

[15] Nicolas Maslov, David Brosset, Christophe Claramunt, and Jean-Frédéric Charpentier. A geographical-based multi-criteria approach for marine energy farm planning. *ISPRS International Journal of Geo-Information*, 3(2):781–799, 2014.

[16] Cyril Tissot, David Brosset, Laurent Barillé, Laurent Le Grel, Ion Tillier, Mathias Rouan, and Matthieu Le Tixerant. Modeling oyster farming activities in coastal areas: a generic framework and preliminary application to a case study. *Coastal Management*, 40(5):484–500, 2012.

[17] David Brosset and Christophe Claramunt. An experimental ant colony approach for the geolocation of verbal route descriptions. *Knowledge-Based Systems*, 24(4):484–491, 2011.

[18] Matthieu Le Tixerant, Françoise Gourmelon, Cyril Tissot, and David Brosset. Modelling of human activity development in coastal sea areas. *Journal of Coastal Conservation*, 15(4):407–416, 2011.

[19] Cyril Faucher, Cyril Tissot, Jean-Yves Lafaye, Frédéric Bertrand, David Brosset, and Mathias Rouan. Location-and temporal-based services for nature–society interaction regulation. *Journal of Location Based Services*, 4(3-4):147–165, 2010.

[20] David Brosset, Christophe Claramunt, and Eric Saux. Wayfinding in natural and urban environments: a comparative study. *Cartographica: The International Journal for Geographic Information and Geovisualization*, 43(1):21–30, 2008.

Revues nationales

[21] Cécile Guégan, Cyril Tissot, Sébastien Kervern, David Brosset, Solenn Le Berre, and Louis Brigand. Observation et modélisation des flux touristiques: application au mont-saint-michel. *Cybergeo: European Journal of Geography*, 2015.

[22] Damien Le Guyader, David Brosset, and Françoise Gourmelon. Exploitation de données ais pour la cartographie du transport maritime. *M@ ppemonde*, 104(2011.4):http–mappemonde, 2012.

Conférences internationales

[23] Xavier Bellekens, Gayan Jayasekara, Hanan Hindy, Miroslav Bures, David Brosset, Christos Tachtatzis, and Robert Atkinson. From cyber-security deception to manipulation and gratification through gamification. In *International Conference on Human-Computer Interaction*, pages 99–114. Springer, Cham, 2019.

[24] Olivier Jacq, David Brosset, Jacques Simonin, and Yvon Kermarrec. Use of suricata, elasticstack, neo4j and linkurious for network defence. In *SuriCon 2019, Amsterdam*, 2019.

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

[26] Pedro Merino Laso, David Brosset, and Marie-Annick Giraud. Defining role-based access control for a secure platform of unmanned surface vehicle fleets. In *OCEANS 2019-Marseille*, pages 1–4. IEEE, 2019.

[27] Pedro Merino Laso, David Brosset, and Marie-Annick Giraud. Monitor and control human-computer interface for unmanned surface vehicle fleets. In *OCEANS 2019-Marseille*, pages 1–5. IEEE, 2019.

[28] Maël Nogues, David Brosset, Hanan Hindy, Xavier Bellekens, and Yvon Kermarrec. Labelled network capture generation for anomaly detection. In *International Symposium on Foundations and Practice of Security*, pages 98–113. Springer, Cham, 2019.

[29] Xavier Bellekens, Gayan Jayasekera, Hanan Hindy, Miroslav Bureš, David Brosset, Christos Tachtatzis, and Robert Atkinson. From cyber-security deception to manipulation and gratification through gamification. In *21st International Conference on Human-Computer Interaction*, pages 1–3, 2018.

[30] Olivier Jacq, Xavier Boudvin, David Brosset, Yvon Kermarrec, and Jacques Simonin. 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.

[31] Pedro Merino Laso, David Brosset, and Marie-Annick Giraud. Secured architecture for unmanned surface vehicle fleets management and control. In *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*, pages 373–375. IEEE, 2018.

[32] Thibaud Mérien, Xavier Bellekens, David Brosset, and Christophe Claramunt. A spatio-temporal entropy-based approach for the analysis of cyber attacks (demo paper). In *Proceedings of the 26th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pages 564–567. ACM, 2018.

[33] Thibaud Merien, David Brosset, Xavier Bellekens, and Christophe Claramunt. A human-centred model for network flow analysis. In *2018 2nd Cyber Security in Networking Conference (CSNet)*, pages 1–6. IEEE, 2018.

[34] Arthur Valko, Alexandru Liviu Olteanu, David Brosset, and Patrick Meyer. Integrating a temporal component into multi-criteria majority-rule sorting models. In *DA2PL'2018: from Multiple Criteria Decision Aid to Preference Learning*, 2018.

[35] Arthur Valko, Alexandru Liviu Olteanu, David Brosset, and Patrick Meyer. Integrating time into majority-rule sorting models: application to the cyber-defense context. In *15th Decision Deck Workshop*, 2018.

[36] Damien Le Guyader, Cyril Ray, and David Brosset. Identifying small-scale fishing zones in France using AIS data. In *Advances in Shipping Data Analysis and Modeling: Tracking and Mapping Maritime Flows in the Age of Big Data*. November 2017.

[37] Thomas Becmeur, Xavier Boudvin, David Brosset, Gaël Héno, Benjamin Costé, Yvon Kermarrec, and Pedro Merino Laso. Generating data sets as inputs of reference for cyber security issues and industrial control systems. In *Research Challenges in Information Science (RCIS), 2017 11th International Conference on*, pages 453–454. IEEE, 2017.

[38] Thomas Becmeur, Xavier Boudvin, David Brosset, Gaël Héno, Thibaud Merien, Olivier Jacq, Yvon Kermarrec, and Bastien Sultan. A platform for raising awareness on cyber security in a maritime context. In *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 103–108. IEEE, 2017.

[39] David Brosset, Camille Cavelier, Benjamin Costé, Yvon Kermarrec, Joffrey Lartigaud, and Pedro Merino Laso. Cr@ ck3n: A cyber alerts visualization object. In *Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2017 International Conference On*, pages 1–2. IEEE, 2017.

[40] Pedro Merino Laso, David Brosset, and John Puentes. Analysis of quality measurements to categorize anomalies in sensor systems. In *Computing 2017: Science and Information Conference*, pages 1330–1338. IEEE, 2017.

[41] Lamia Belouaer, David Brosset, and Christophe Claramunt. From verbal route descriptions to sketch maps in natural environments. In *Proceedings of the 24th acm sigspatial international conference on advances in geographic information systems*, page 13. ACM, 2016.

[42] Clément Iphar, Aldo Napoli, Cyril Ray, Erwan Alincourt, and David Brosset. Risk analysis of falsified automatic identification system for the improvement of maritime traffic safety. In *ESREL 2016*, pages 606–613. Taylor & Francis, 2016.

[43] Pedro Merino Laso, David Brosset, and John Puentes. Monitoring approach of cyber-physical systems by quality measures. In *International Conference on Sensor Systems and Software*, pages 105–117. Springer, 2016.

[44] Damien Le Guyader, Cyril Ray, and David Brosset. Defining fishing grounds variability with automatic identification system (ais). In *2nd International Workshop on Maritime Flows and Networks (WIMAKS'16)*, page 96, 2016.

[45] Ines Jguirim, David Brosset, and Christophe Claramunt. An activity-based modeling approach for the representation of the city. In *ACM GIS*, 2015.

[46] Shoko Wakamiya, Lamia Belouaer, David Brosset, Ryong Lee, Yukiko Kawai, Kazutoshi Sumiya, and Christophe Claramunt. Measuring crowd mood in city space through twitter. In *International Symposium on Web and Wireless Geographical Information Systems*, pages 37–49. Springer, 2015.

[47] Ines Jguirim, David Brosset, and Christophe Claramunt. Functional and structural analysis of an urban space extended from space syntax. In *GISCIENCE, GeoVisual Analytics: Interactivity, Dynamics, and Scale Workshop*, 2014.

[48] Cyril Tissot, Mathias Rouan, Etienne Neethling, Hervé Quenol, and David Brosset. Modeling of vine agronomic practices in the context of climate change. In *BIO Web of Conferences*, volume 3, page 01015. EDP Sciences, 2014.

[49] Lamia Belouaer, David Brosset, and Christophe Claramunt. Modeling spatial knowledge from verbal descriptions. In *International Conference on Spatial Information Theory*, pages 338–357. Springer, 2013.

[50] Lamia Belouaer, David Brosset, and Christophe Claramunt. A rule-based genetic algorithm for mapping route descriptions towards map representations. In *COMP@ SIGSPATIAL*, pages 50–53, 2013.

[51] Cyril Tissot, David Brosset, Mathias Rouan, Etienne Neethling, and Hervé Quénol. Presentación de las posibles aplicaciones de utilización del sistema multi-agentes dahu a los viñedos de las costas de layon y de mendoza. In *Impacto del cambio climático a la escala de los terroirs vitícolas*, 2011.

[52] D Brosset and C Claramunt. A dynamic ants colony algorithm for geopositioning verbal route descriptions (dard) in natural and non constrained environments. In *META'10, International Conference on Metaheuristics and Nature Inspired Computing*, 2010.

[53] David Brosset, Christophe Claramunt, and Eric Saux. An acs cooperative learning approach for route finding in natural environment. In *Proceedings of the 16th ACM SIGSPATIAL international conference on Advances in geographic information systems*, page 13. ACM, 2008.

[54] David Brosset, Christophe Claramunt, and Eric Saux. An experimental ant colony approach for the spatialization of verbal route descriptions. In *International Workshop on Computational Models of Place (PLACE'08)*, 2008.

[55] David Brosset, Christophe Claramunt, and Eric Saux. A location and action-based model for route descriptions. In *International Conference on GeoSpatial Sematics*, pages 146–159. Springer, 2007.

Conférences nationales

[56] Ines Jguirim, David Brosset, and Christophe Claramunt. Un système de génération d'itinéraires des activités mobiles dans la ville. In *SAGEO*, 2015.

[57] Damien Le Guyader, Cyril Ray, and David Brosset. Caractérisation spatio-temporelle de l'activité de pêche à la drague en rade de brest par analyse de données ais. In *Merigéo: de la côte à l'océan, l'Information Géographique en mouvement*, page 210, 2015.

[58] Etienne Neethling, Cyril Tissot, Mathias Rouan, Sebastien Kervern, David Brosset, and Hervé Quénol. Modélisation des activités viticoles sous contraintes climatiques, 2014.

[59] Damien Le Guyader and David Brosset. L'ais: une donnée pour l'analyse des activités en mer. In *Conférence Internationale de Géomatique et d'Analyse spatiale (Spatial Analysis and GEOmatics)-SAGEO 2013*, page 53, 2013.

[60] Cyril Tissot, Mathias Rouan, David Brosset, and Damien Le Guyader. Modélisation des activités de pêche à la drague en rade de brest. In *SAGEO 2013*, page 12, 2013.

[61] Ion Tillier, Cyril Tissot, Mathias Rouan, Brice Trouillet, David Brosset, and Marc Robin. Modelisation du deroulement d'activites conchylicoles en zone cotiere par couplage sig/sma. In *MASHS*, page 12, 2009.

[62] David Brosset and Thomas Devogele. Algorithmes génétiques et généralisation de mnt marins. In *Actes des 7ièmes journées Cassini, Grenoble*, 2004.

DOCTORAT BRETAGNE LOIRE / MATHSTIC

UBO Université de Bretagne Occidentale

Titre : Etudes des Activités humaines : de l'expérimentation à l'analyse

Mots clés : réseau informatique, modélisation, graphe, cybersécurité

Résumé : Les travaux de recherche menés concernent les activités humaines, de leur modélisation à leur analyse en passant par leur modélisation. Ces activités sont des activités dans le monde physique comme la randonnée pédestre ou bien des activités numériques avec l'étude des échanges réseau dans des systèmes cyber physiques.
Le premier chapitre détaille les différents protocoles expérimentaux qui ont été développés pour obtenir des données sur les activités. De l'entretien à la conception d'un cyberrange maritime, les données collectées sont très différentes et possèdent des caractéristiques qui doivent être prises en compte dans la phase de modélisation.
La modélisation a utilisé préférentiellement les graphes particulièrement adaptés pour des entités localisées en interaction. Les modélisations ont mis l'accent sur les types de relations entre les entités avec l'interaction possible avec les repères spatiaux ou l'intention des cyberattaques.
Enfin, dans la troisième étape, les données modélisées ont été analysées avec des objectifs différents allant de la génération de cartes schématiques à la détection d'anomalies dans les systèmes industriels maritimes.
Le développement de représentations visuelles originales fait partie des perspectives des travaux ainsi que l'amélioration de l'analyse des traces réseau par détection de comportements catégorisés.

Title : Study of human behaviours: from data collection to data analysis

Keywords : IT/OT networks, data modelling, graph theory, maritime cybersecurity

Abstract :
This research focuses on human behaviour and how to capture, model and analyse data.

The human behaviours studied were physical world actions, such as hiking routes taken, as well as digital activities within cyber physical systems, such as network messages.

The first chapter details the different experimental protocols developed to collect unique raw data on human behaviours. From initial interviews through to the development of a maritime cyber range, the data collected was extremely varied with specific characteristics that had to be taken into account during the modelling phase.

Graph theory was the preferred modelling tool used as it is well adapted to represent interactions between different entities. Models focussed on the relationships between entities and their potential interactions within the physical or digital world, such as spatial landmarks as well as cyberattack intentions.

The third phase was the analysis of the modelled data with various objectives including the generation of sketch maps and the detection of anomalies within maritime industrial systems.

This study could play a major role in the development of new visual representations as well as improvements in the analysis of network footprints through network behavioural analysis methods.