POLYTECHNIQUE MONTRÉAL
affiliée à l'Université de Montréal

Infrastructure de test pour la cybersécurité des systèmes maritimes

JEAN-GUILLAUME LANGLOIS
Département de génie informatique et génie logiciel

Mémoire présenté en vue de l'obtention du diplôme de *Maîtrise ès sciences appliquées*
Génie informatique

Décembre 2021

© Jean-Guillaume Langlois, 2021.

POLYTECHNIQUE MONTRÉAL
affiliée à l'Université de Montréal

Ce mémoire intitulé :

Infrastructure de test pour la cybersécurité des systèmes maritimes

présenté par **Jean-Guillaume LANGLOIS**
en vue de l'obtention du diplôme de *Maîtrise ès sciences appliquées*
a été dûment accepté par le jury d'examen constitué de :

Alejandro QUINTERO, président
Nora BOULAHIA **CUPPENS**, membre et directrice de recherche
Pierre LANGLOIS, membre et codirecteur de recherche
Martine BELLAÏCHE, membre

DÉDICACE

À ma famille et mes proches

REMERCIEMENTS

Je tiens à remercier mes parents, mon frère et tous mes proches pour leur support tout au long de ma maîtrise. Ce support a été essentiel à ma réussite.

Je remercie ma directrice de recherche Nora Cuppens pour son travail et son support tout au long de ma maîtrise. Je remercie mon co-directeur de recherche Pierre Langlois pour son support et ses judicieux conseils, ceux-ci ayant rendu beaucoup plus aisée l'écriture du présent mémoire. Je remercie également José Fernandez de m'avoir fait joindre le laboratoire de cybersécurité.

Je tiens à remercier mes collègues au laboratoire. Tout d'abord, je remercie Axel Rousselot, avec qui j'ai eu beaucoup de plaisir à travailler, particulièrement dans le contexte de la pandémie. Ensuite, je remercie Shubh Arya, avec qui j'ai eu la chance de collaborer lors de l'été 2021, dont les compétences en cybersécurité ont énormément enrichi mon expérience. Finalement, je remercie Nuno et Itzael, avec qui j'ai eu la chance de partager une belle amitié au laboratoire.

Je remercie les membres de jury d'avoir accepté d'évaluer ce travail.

RÉSUMÉ

La montée de l'utilisation de systèmes informatiques sur les navires vient avec son lot de vulnérabilités, et ainsi de menaces. Effectivement, de multiples systèmes maritimes comportent des failles sécuritaires permettant à des attaquants potentiels de les exploiter, comme le montrent plusieurs études de risques et cyberattaques sur des systèmes maritimes. Ces vulnérabilités peuvent avoir des impacts majeurs sur les systèmes maritimes, tels que des dommages physiques à un navire, ou encore des pertes humaines parmi l'équipage du navire. Par rapport à cette problématique, nous émettons trois constats. Tout d'abord, des attaques de multiples sortes sont possibles sur une grande quantité de systèmes maritimes. Ensuite, l'unicité de chaque navire fait en sorte que tous les navires ne partagent pas les mêmes systèmes ni architectures. Finalement, le facteur humain joue un grand rôle dans la sécurité des systèmes maritimes.

À la lumière de ces observations, nous constatons que les solutions proposées dans la littérature scientifique ne permettent pas de résoudre la problématique de façon appropriée. Effectivement, les solutions trop spécifiques ne considèrent pas l'étendue des types de vulnérabilités, et les solutions générales n'entrent pas assez en profondeur. Conséquemment, nous postulons qu'une solution considérant la complexité de la problématique est la mise en place d'une infrastructure de test simulant divers systèmes maritimes. En effet, les infrastructures de test appliquées à des domaines particuliers ont permis des avancées considérables dans le domaine de la cybersécurité. Pour cette infrastructure, nous avons choisi d'inclure le système *Electronic Chart Display Information System* (ECDIS), puis de produire un flot de données maritimes simulant les données générées par différents capteurs présents sur un navire, tel que les données de positionnement et le cap. Ensuite, nous avons modélisé et implémenté trois scénarios d'attaque pour cette infrastructure.

Nous avons développé l'infrastructure de test en nous appuyant sur diverses caractéristiques corrélées avec la crédibilité d'une infrastructure. De plus, son évolutivité et sa flexibilité permettront à notre infrastructure d'être utilisée et modifiée à des fins de recherche. Ensuite, les cyberattaques que nous avons développées nous ont permis d'évaluer les compétences nécessaires à un attaquant pour arriver à exploiter des vulnérabilités informatiques à bord d'un navire. Cette infrastructure est un projet à développer à long terme et dont les systèmes simulés seront amenés à évoluer au fil du temps selon les besoins et les menaces. Pour les travaux futurs, nous croyons que l'inclusion de simulations semi-physiques, telles qu'un pilote automatique, augmenterait la fiabilité, et donc la crédibilité de notre infrastructure de test.

ABSTRACT

The rise in the use of computer systems on ships comes with its share of vulnerabilities, and therefore with threats. Indeed, multiple maritime systems contain security vulnerabilities allowing potential attackers to exploit them, as shown by several studies of risk analysis and by cyberattacks on maritime systems. These vulnerabilities could have major impacts on maritime systems, such as physical damage to a ship, or even loss of life among the ship's crew. With regard to this problem, we make three observations. Firstly, attacks of multiple kinds are possible on a large number of maritime systems. Secondly, the uniqueness of each ship implies that all ships do not share the same systems or architectures. Finally, the human factor plays a big role in the security of maritime systems.

Looking at these observations, we note that the solutions proposed in the scientific literature do not make it possible to address the problem in an appropriate manner. Indeed, solutions that are too specific do not consider the big picture, and general solutions usually do not go into enough depth. Consequently, we postulate that a solution that is addressing the complexity of the problem is the implementation of a test infrastructure simulating various maritime systems. Indeed, test infrastructures applied to certain fields have enabled considerable advances, particularly in the field of cybersecurity. For this infrastructure, we have chosen to include the ECDIS, then to simulate a ship's data flow. Next, we modelled and implemented three attack scenarios for this infrastructure.

We have developed this test infrastructure based on various characteristics correlated with the credibility of a test infrastructure. In addition, its scalability and flexibility will allow our infrastructure to be used and modified for research purposes. Furthermore, the cyber attacks that we developed allowed us to assess the necessary skills for an attacker to exploit a ship's vulnerabilities. This infrastructure is a project to be developed in the long term, and its simulated systems will have to evolve over time according to needs and threats. For future work, we believe that the inclusion of semi-physical simulations, such as an autopilot, would increase the reliability, and therefore the credibility of our test infrastructure.

TABLE DES MATIÈRES

DÉDICACE iii

REMERCIEMENTS iv

RÉSUMÉ v

ABSTRACT vi

TABLE DES MATIÈRES vii

LISTE DES TABLEAUX xi

LISTE DES FIGURES xii

LISTE DES SIGLES ET ABRÉVIATIONS xiv

LISTE DES ANNEXES xvi

CHAPITRE 1 INTRODUCTION 1

1.1 Montée de la menace envers les systèmes maritimes 1

1.2 Analyse de risques des systèmes maritimes 2

1.2.1 Types d'attaquants sur des systèmes maritimes 2

1.2.2 Motifs d'attaque sur des systèmes maritimes 2

1.2.3 Vulnérabilités et menaces 3

1.3 Cas d'attaque sur des systèmes maritimes 3

1.3.1 Cas d'attaque sur des organisations/compagnies maritimes 3

1.3.2 Cas d'attaque sur des ports 4

1.3.3 Cas d'attaque sur des navires ou autres bâtiments se déplaçant sur l'eau 4

1.4 Problématique 5

1.5 Partenariat avec l'industrie (Neptune-Cyber) 6

1.6 Objectifs de recherche 6

1.6.1 Développement d'une infrastructure de simulation d'un système d'affichage numérique de cartes et la génération de données simulant différents capteurs d'un navire 7

1.6.2 Développement de cyberattaques contre l'infrastructure de test 7

1.7 Structure du mémoire 7

CHAPITRE 2 REVUE DE LA LITTÉRATURE 9
2.1 Normes et réglementations maritimes 9
2.2 Vulnérabilités de systèmes informatiques maritimes 9
2.2.1 Réseaux de technologie de l'information 9
2.2.2 Systèmes de contrôle industriels (SCI) 10
2.2.3 Systèmes de visualisation des cartes de navigation électroniques . . . 10
2.2.4 GNSS 11
2.2.5 Les communications satellitaires 11
2.2.6 VDR, radar et GMDSS 11
2.3 Vulnérabilités des protocoles de communication maritime 12
2.3.1 NMEA-0183 12
2.3.2 NMEA-2000 12
2.3.3 NMEA OneNET 13
2.3.4 Système d'échanges automatisés de messages 13
2.4 Solutions de protection pour les systèmes maritimes 14
2.4.1 Méthodes d'analyse de risque 14
2.4.2 Solutions de protection spécifiques 15
2.5 Solutions de détection d'anomalies pour les systèmes maritimes 16
2.5.1 Systèmes d'échanges automatisés de messages 16
2.5.2 Utilisation d'ontologies 17
2.6 Infrastructures de tests et laboratoires de recherche pour la cybersécurité maritime 18
2.6.1 Cyber Ranges 18
2.6.2 Cyber-MAR 19
2.6.3 Grace Maritime Cyber Testbed 19
2.6.4 Laboratoire dédié à la cybersécurité maritime 20
2.7 Discussion 20

CHAPITRE 3 MÉTHODOLOGIE DE CONCEPTION DE L'INFRASTRUCTURE DE TEST 22
3.1 Objectifs de conception 22
3.2 Caractéristiques des infrastructures de test 24
3.2.1 Options de caractéristiques 24
3.2.2 Choix des caractéristiques 27
3.3 Approches de simulation 31
3.4 Synthèse 31

CHAPITRE 4 MODÉLISATION DE L'INFRASTRUCTURE DE TEST 33
4.1 Choix de conception de l'infrastructure de test 33
4.1.1 Options de systèmes à inclure 33
4.1.2 Choix des systèmes à inclure 35
4.1.3 Données à générer 36
4.1.4 Protocoles à simuler 37
4.1.5 Architecture de l'infrastructure de simulation 38
4.2 Préparation de la modélisation d'attaques 38
4.2.1 Vulnérabilités des systèmes et protocoles choisis 39
4.2.2 Motivation de l'attaquant et victime ciblée 39
4.2.3 Hypothèses et environnement de travail 40
4.3 Modélisation de trois scénarios d'attaques 40
4.3.1 Chaîne de frappe commune aux trois scénarios 41
4.3.2 Scénario 1 : Attaque par déni de service sur l'ECDIS 42
4.3.3 Scénario 2 : Attaques par usurpation de paquets et par l'homme du milieu sur l'ECDIS 43
4.3.4 Scénario 3 : Attaque sophistiquée sur l'ECDIS 44
4.3.5 Synthèse 45

CHAPITRE 5 EXPÉRIMENTATION ET RÉSULTATS 47
5.1 Mise en place de l'infrastructure de test 47
5.1.1 Choix de l'environnement d'implémentation 47
5.1.2 Étude comparative des générateurs de données 47
5.1.3 Choix de simulation de la communication 50
5.1.4 Étude comparative de logiciels d'ECDIS 52
5.1.5 Infrastructure de test 55
5.2 Mise en place des étapes 1 à 6 de la chaîne de frappe 56
5.2.1 Reconnaissance 56
5.2.2 Armement 56
5.2.3 Livraison 57
5.2.4 Exploitation 58
5.2.5 Installation / Commandement et contrôle 59
5.3 Mise en place de l'étape #7 pour chacun des scénarios 59
5.3.1 Scénario 1 : Déni de service sur l'ECDIS 59
5.3.2 Scénario 2 : Usurpation de paquets et attaque par l'homme du milieu sur l'ECDIS 60

5.3.3 Scénario 3 : Attaque sophistiquée sur l'ECDIS 64
5.4 Résultats/Analyse 72
5.4.1 Résultats et analyse de la mise en place de l'infrastructure de test . . 73
5.4.2 Résultats et analyse de la mise en place des attaques 74

CHAPITRE 6 CONCLUSION 78
6.1 Synthèse des travaux 78
6.1.1 Développement d'une infrastructure de simulation 78
6.1.2 Développement de cyberattaques contre l'infrastructure 79
6.2 Limites de la solution présentée et perspectives 79
6.2.1 Approche de simulation 79
6.2.2 Expérimentation 80
6.2.3 Implémentation de solutions de détection d'anomalies 80
6.3 Sommaire 81

RÉFÉRENCES 82

ANNEXES 93

LISTE DES TABLEAUX

Tableau 3.1 Caractéristiques et leur proportion d'impact sur la crédibilité d'une infrastructure de test 27
Tableau 3.2 Impacts des caractéristiques de conception d'une infrastructure de test sur les objectifs de conception choisis 30
Tableau 4.1 Synthèse de la modélisation de trois scénarios d'attaques . . 46
Tableau 5.1 Comparaison de logiciels générateurs de données NMEA-0183 48
Tableau 5.2 Comparaison des instruments NMEA-0183 simulés pour chacun des logiciels 48
Tableau 5.3 Comparaison des formats de phrases GPS NMEA-0183 pour chacun des logiciels 49
Tableau 5.4 Synthèse de l'analyse des scénarios d'attaques implémentés . 77

LISTE DES FIGURES

Figure 4.1 Relations entre l'ECDIS et les autres systèmes 34
Figure 4.2 Architecture de l'infrastructure de simulation 38
Figure 4.3 Architecture de l'environnement de travail 40
Figure 4.4 Injection de phrases GPS NMEA-0183 localisées au milieu de l'Afrique 44
Figure 5.1 Écran de présentation du logiciel de génération de données NMEA-0183 NEMAStudio (Sailsoft) 50
Figure 5.2 Création d'une connexion série virtuelle avec le logiciel com0com 51
Figure 5.3 Flux de données GPS, de cap, d'écho sondeur et de vent envoyé à OpenCPN 52
Figure 5.4 Écran d'OpenCPN affichant la position et le cap du navire . . 53
Figure 5.5 Écran de TimeZero Navigator affichant la position et le cap du navire, puis les données d'écho sondeur et de vent 54
Figure 5.6 Configuration du tableau de bord de TimeZero Navigator . . . 54
Figure 5.7 Implémentation de l'infrastructure de test 55
Figure 5.8 Écoute des données transmises sur un port série par ENLYZE PortSniffer 61
Figure 5.9 Architecture informatique pour l'implémentation du scénario 2 62
Figure 5.10 Trajectoire d'un navire dans TimeZero avant l'attaque par l'homme du milieu 63
Figure 5.11 Trajectoire d'un navire dans TimeZero après l'attaque par l'homme du milieu 63
Figure 5.12 Fenêtre de redémarrage 64
Figure 5.13 Flux de données générées pour le scénario 3 65
Figure 5.14 Architecture informatique pour l'implémentation du scénario 3 67
Figure 5.15 Trajectoire d'un navire dans TimeZero Navigator avant l'attaque sophistiquée 68
Figure 5.16 Lancement de l'application Python 69
Figure 5.17 Trajectoire d'un navire dans TimeZero Navigator après le lancement de l'attaque sophistiquée (1) 69
Figure 5.18 Trajectoire d'un navire dans TimeZero Navigator après le lancement de l'attaque sophistiquée (2) 70

Figure 5.19 Trajectoire d'un navire dans TimeZero Navigator après le lancement de l'attaque sophistiquée (3) 70
Figure 5.20 Script Python pour la modification du port série sur lequel écoute TimeZero Navigator 72

LISTE DES SIGLES ET ABRÉVIATIONS

AIS	Automatic Identification System
ARPA	Automatic radar plotting aids
BeEF	Browser Exploitation Framework
BIMCO	Baltic and International Maritime Council
CAN	Controller Area Network
CTF	Capture the Flag
DCNS	Direction des constructions navales
ECDIS	Electronic Chart Display Information System
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HID	Human Interface Device
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IMO	International Maritime Organization
IPMS	Integrated Platform Management System
IPv6	Internet Protocol version 6
ISPS	International Ship and Port Facility Security
Lite-CA	Lite Certification Authority
MaCRA	ModelBased Framework for Maritime Cyber-Risk Assessment
NMEA	National Marine Electronics Association
PD	Positionnement dynamique
PDF	Portable Document Format
SCI	Systèmes de contrôle industriels
SPI	Système du pont intégré
SQ	Sequence Number
S-VDR	Simplified Voyage Data Recorder
TCP	Transmission Control Protocol
TI	Technologies de l'information
TO	Technologies d'opération
UDP	User Datagram Protocol
USB	Universal Serial Bus

VDR	Voyage Data Recorder
VSAT	Very Small Aperture Terminal
VTS	Vessel Traffic Services
XML	Extensible Markup Language

LISTE DES ANNEXES

Annexe A Notions maritimes et de cybersécurité 93

CHAPITRE 1 INTRODUCTION

Plus on ouvre à un système informatique des portes vers l'extérieur, plus les attaquants auront d'opportunités pour l'attaquer [1]. Or, depuis plusieurs années, les systèmes maritimes subissent une informatisation et une automatisation grandissantes [2, 3]. Ces avancées technologiques profèrent à ces systèmes de meilleures performances, ou encore une plus grande efficacité. Cependant, l'informatisation et l'automatisation de ces systèmes ont ouvert la porte à des attaques de toutes formes dont les impacts sur le domaine maritime sont énormes [4]. En outre, les navires équipés de systèmes de technologies de l'information (TI) et de technologies d'opération (TO) sont connectés à des réseaux externes, ce qui ouvre également la porte à des intrusions et attaques potentielles [5, 6].

1.1 Montée de la menace envers les systèmes maritimes

En réaction à ces menaces grandissantes, la *Baltic and International Maritime Council* (BIMCO) a émis pour 2020 des lignes directrices en matière de cybersécurité maritime [7]. Ces dernières visent à aider l'industrie maritime à mieux se protéger contre les attaques potentielles. De pair avec ces lignes directrices, l'*International Maritime Organization* (IMO) a émis en 2021 des lignes directrices forçant désormais les entreprises à adopter des mesures cybersécuritaires [8].

Cette ruée vers la sécurité informatique est une réaction au manque de mesures dont l'industrie maritime a fait preuve dans les dernières années [9]. En effet, les mesures prises contre les cyberattaques sont trop peu nombreuses et le nombre d'attaques ne cesse d'augmenter. De 2017 à 2020, les cyberattaques menées contre des systèmes de technologie opérationnelle maritimes ont augmenté de 900% [4]. En outre, selon le spécialiste en cybersécurité Naval Dome, entre février et juin 2020, les tentatives de cyberattaques dans l'industrie maritime ont augmenté de 400% [10]. Si ces chiffres semblent énormes par rapport à ce qui est rapporté dans les médias, il faut savoir qu'en matière de cybersécurité, les incidents connus sous souvent sous-représentés par rapport à la réalité, et ce pour deux raisons. Tout d'abord, les victimes de cyberattaques ne sont généralement pas favorables à l'idée de partager ces informations avec le public, celles-ci pouvant avoir des impacts négatifs sur leur sécurité et leur réputation, lorsque mises au grand jour. Ensuite, certaines victimes de cyberattaques ne sont même pas au courant qu'elles en sont victimes, dans les cas par exemple de vol de données sensibles, où l'attaque laissera peu de traces auprès de la victime [11].

1.2 Analyse de risques des systèmes maritimes

Dans cette section, nous commencerons par décrire les quatre différents types d'attaquants que nous distinguons pour les systèmes maritimes. Ensuite, nous présenterons les quatre motifs d'attaque sur des systèmes maritimes que nous distinguons. Finalement, nous définirons les concepts de vulnérabilité et de menace pour ce mémoire.

1.2.1 Types d'attaquants sur des systèmes maritimes

Nous distinguons quatre types d'attaquants sur des systèmes maritimes, que nous présentons sans ordre particulier. Tout d'abord, nous avons les criminels sans connaissance particulière en matière de cyberattaques. Si ces acteurs ne sont pas dangereux en soit, ils sont tout de même capables d'engager des gens ayant les compétences nécessaires pour mener des cyberattaques. Ensuite, nous avons les criminels dotés des compétences nécessaires pour mener des cyberattaques. Ces acteurs peuvent être amenés à travailler pour leur propre cause, ou encore à travailler pour les criminels sans compétences pour mener des cyberattaques. Pour continuer, nous avons les hacktivistes, dont la cause politique sera la principale motivation pour perturber des systèmes maritimes. Finalement, nous avons les États-nations, tels que des pays, qui peuvent engager les gens ayant les compétences nécessaires pour mener des attaques contre différents systèmes maritimes.

1.2.2 Motifs d'attaque sur des systèmes maritimes

Nous distinguons quatre motifs d'attaque sur des systèmes maritimes, que nous présentons sans ordre particulier. Le premier est l'espionnage. En effet, les navires, les ports, et surtout les compagnies maritimes ont à leur disposition de multiples données sensibles pour lesquelles plusieurs seraient prêts à attaquer des systèmes pour y avoir accès, par exemple pour obtenir un avantage concurrentiel. Le prochain motif d'attaque sur des systèmes maritimes est le vol monétaire. Effectivement, on observe depuis plusieurs années le cas de logiciels de rançon utilisés sur des navires, les empêchant ainsi de quitter le port avant que l'on ne verse une somme monétaire à l'attaquant [12]. Un autre motif d'attaque sur des systèmes maritimes est le déplacement illégal de cargaison. En effet, certains acteurs, voulant faire passer de la cargaison illégalement par une voie maritime, tenteront de compromettre les systèmes présents dans les ports navals. De cette façon, ils peuvent désactiver les mesures de sécurité mises en place et faire passer leur cargaison sous le radar. Le dernier motif d'attaque que nous distinguons est de causer des perturbations ou des pertes, sans en retirer quelque chose de positif. Effectivement, nous observons des cas d'attaque où l'attaquant ne retirait autre

chose de son attaque que des pertes chez la victime, dans des cas où par exemple la victime est un concurrent de l'attaquant. On dénote aussi le cas des hacktivistes, voulant causer du tort à des organisations à des fins partisanes ou politiques.

1.2.3 Vulnérabilités et menaces

Dans ce mémoire, nous abordons le concept de vulnérabilité pour les systèmes maritimes. Par vulnérabilité, nous entendons une faille dans le système pouvant être exploitée par un attaquant pour mener une cyberattaque. Ces vulnérabilités peuvent être matérielles, logicielles, ou encore humaines. Lorsqu'un attaquant a un motif pour attaquer un système, que ce système comporte une vulnérabilité et que cet attaquant a la capacité d'exploiter cette vulnérabilité, ce système fait face à une menace, et donc à un risque.

1.3 Cas d'attaque sur des systèmes maritimes

Pour les cas d'attaque sur des systèmes maritimes, nous distinguons trois catégories de cibles. Tout d'abord, nous avons les organisations ou compagnies maritimes. Cette catégorie de cible regroupe les organisations ou autorités maritimes, ou encore les compagnies et consultants oeuvrant dans le domaine maritime. La seconde catégorie regroupe les ports navals, dans laquelle nous incluons les compagnies de livraison navale. La dernière catégorie regroupe les navires. Elle inclut également les autres bâtiments se déplaçant sur l'eau, telle que les foreuses marines.

1.3.1 Cas d'attaque sur des organisations/compagnies maritimes

Les organisations et compagnies maritimes font souvent le cas d'infiltration par des logiciels malveillants. En effet, en 2013, un logiciel malveillant appelé *icefog* s'en est pris à un ensemble de compagnies coréennes, dont deux constructeurs de navires, soit *Daewoo Shipbuilding & Marine Engineering Tech* et *Hanjin Heavy Industries* [13]. D'autres compagnies font plutôt l'objet de vol de données sensibles. C'est le cas de la direction des constructions navales (DCNS), compagnie de construction navale française, qui a été victime en 2016 d'un vol de données confidentielles, soit des plans de construction de nouveaux sous-marins [14]. La fuite consistait en 22 000 pages détaillant les plans de six sous-marins que la DCNS avait conçus pour les forces marines indiennes. Les sous-marins étant déjà en construction lorsque l'attaque a eu lieu, la sécurité de ce projet de construction a été mise en doute. Même si les coupables et la nature de l'attaque n'ont pas été découverts, les soupçons semblent pointer vers de l'espionnage industriel. L'action de Thales, propriétaire partiel de la compagnie, a à

l'époque chuté de 3%. Finalement, en 2017, le courtier maritime Clarksons a été victime d'une intrusion dans ses systèmes informatiques [15]. Les attaquants se seraient introduits dans le réseau informatique à l'aide d'un compte utilisateur compromis. Leur but était de soutirer des informations sensibles pour ensuite demander une rançon, sans quoi ils allaient diffuser les informations. Les données volées consistaient entre autres en des données personnelles de clients. Même si les investigateurs forensiques de Clarksons ont réussi à restituer les données volées sans avoir à payer de rançon, l'action de Clarksons a tout de même subi une baisse de 2% suite à cet incident.

1.3.2 Cas d'attaque sur des ports

Certains ports navals sont l'objet d'attaques par déni de service. Effectivement, en 2001, un adolescent américain nommé Aaron Caffrey a mené une attaque par déni de service sur les systèmes informatiques du port de Houston. L'attaque a rendu certains systèmes du port hors d'usage, alors que ces systèmes envoyaient des informations importantes aux officiers de navigation [16]. Ensuite, les ports navals font parfois l'objet d'attaques pour des motifs de déplacement illégal de cargaisons illicites. Par exemple, entre 2011 et 2013, le port d'Anvers a été victime de cyberattaques visant la manipulation de son système de contrôle [17]. Un groupe de trafiquants néerlandais aurait engagé un groupe de cyberattaquants basé en Belgique. Ils auraient réussi à faire passer des cargaisons d'héroïne et de cocaïne via le port d'Anvers pendant cette plage de deux ans [17]. Également, en 2016, le port d'Oakland a été victime d'une attaque par déni de service. L'attaque semblait, selon les soupçons, être d'origine russe [18]. Ensuite, en 2017, le grand armateur Dannois Maersk a été victime d'un logiciel de rançon nommé NotPetya. Ayant empêché la compagnie d'effectuer ses livraisons le temps que le système informatique soit remis sur pied, le logiciel de rançon a coûté entre 200 et 300 M de dollars ($) US à Maersk [19]. Finalement, en 2019, les ports israéliens de Haïfa et Ashdod ont été la cible d'attaque menant à l'interruption de grues. L'attaque ciblait plus spécifiquement le *Global Positioning System* (GPS) [20].

1.3.3 Cas d'attaque sur des navires ou autres bâtiments se déplaçant sur l'eau

Les navires sont également vulnérables à des cyberattaques. En 2013, Todd Humphreys a démontré la faisabilité et la facilité avec lesquelles on peut envoyer de fausses données GPS à un navire de croisière [21]. En outre, pendant l'année 2016, selon la Corée du Sud, des centaines de bateaux de pêcheurs sont revenus au port étant donné que leurs signaux GPS ont été compromis par des cyberattaquants de la Corée du Nord [22]. Pour poursuivre, en 2017, des cyberattaquants ont réussi à prendre le contrôle d'un porte-conteneurs faisant route

de Cyprus à Djibouti. L'attaque ayant duré dix heures, le capitaine du navire a indiqué qu'il ne pouvait subitement plus naviguer. Des experts en systèmes informatiques ont pu résoudre le problème en installant un logiciel conçu spécifiquement pour l'industrie maritime, permettant de bloquer toute attaque venant de l'extérieur [23]. De surcroit, en 2019, un logiciel malveillant appelé Emotet a infiltré le système informatique d'un navire marchand. Ce logiciel malveillant est réputé comme étant l'un des plus coûteux et des plus destructeurs, coûtant en moyenne un M$ US pour s'en défaire [24]. Selon les investigations, le navire n'était pas explicitement ciblé par un attaquant, le système informatique a donc été compromis dû à un manque de protections cybersécuritaires. Effectivement, tous les membres de l'équipage partageaient un profil de connexion unique, les disques durs étaient branchés de façon routinière sans mesure de sécurité, et aucun antivirus n'était installé sur les ordinateurs du navire.

Finalement, d'autres bâtiments se déplaçant sur l'eau courent tout autant le danger que les navires. Par exemple, en 2010, une foreuse marine en route de la Corée du Sud vers le Brésil a été prise d'attaque par un logiciel malveillant. Celui-ci a empêché la foreuse de fonctionner pendant 19 jours [25].

1.4 Problématique

En analysant différents cas de cyberattaques contre des systèmes maritimes ayant eu lieu dans les vingt dernières années, on constate que le spectre d'attaques sur les systèmes maritimes est très large. Effectivement, les motifs d'attaques, tout comme les systèmes à attaquer, sont très différents de cas en cas. Dans le cadre de ce mémoire, nous allons nous attarder plus précisément à des scénarios d'attaque sur des navires.

Par rapport aux cas d'attaque sur les navires, nous émettons deux constats témoignant de la complexité du problème. Le premier constat est que les systèmes informatique et opérationnel d'un navire comportent de multiples éléments interreliés. Conséquemment, les solutions cybersécuritaires à apporter pour pallier les menaces devront tenir compte de cette interdépendance de façon à mieux répondre au problème. Le second constat est que le facteur humain est un des éléments les plus importants dans cette problématique. En effet, comme démontré en 2019 par l'infiltration du logiciel malveillant Emotet [24], les humains ont un rôle à jouer dans la sécurité d'un système, ou encore dans son insécurité. Par conséquent, les solutions au problème de la cybersécurité des systèmes maritimes doivent impérativement tenir compte du facteur humain dans leur approche. En outre, nous émettons le constat que chaque architecture des systèmes informatiques d'un navire est différente, il est donc difficile de trouver des solutions générales au problème.

Pour permettre de tester les solutions dans un contexte réaliste tenant compte de l'interdépendance entre les systèmes maritimes, du facteur humain et de l'unicité de l'architecture de chacun des navires, nous postulons que la mise en place d'une infrastructure de test pour la cybersécurité des systèmes maritimes serait bénéfique. Cette infrastructure permettrait de simuler différents éléments interdépendants au sein d'un système maritime ainsi que leurs communications. Ces éléments devraient être des systèmes communs à une majorité de navires pour optimiser l'étendue de l'applicabilité de l'infrastructure. Une fois ces éléments simulés, nous pourrons modéliser un éventail d'attaques au sein de ce système, puis implémenter des solutions à ces attaques. Le tout serait mis sur pied avec une optique d'inclusion des humains et de la prise de décision dans la chaîne pour refléter le plus possible la réalité du facteur humain dans la chaîne d'opération.

1.5 Partenariat avec l'industrie (Neptune-Cyber)

Neptune-Cyber est une compagnie de consultation en matière de cybersécurité maritime basée à Lévis (QC). Sa mission est d'aider les compagnies maritimes à gérer les cyberrisques auxquels elles font face [26]. L'approche solutionnaire de Neptune-Cyber comporte trois étapes. Tout d'abord, une analyse de risque sera faite pour le contexte spécifique du client. Cette première étape assurera la considération par Neptune-Cyber de tous les éléments et menaces impliqués dans la situation. Ensuite, une solution implémentable sera mise en place. Cette solution sera conçue de manière personnalisée selon les besoins spécifiques du client. Finalement, un service de soutien et de formation continue en sécurité sera offert au client. Cette étape est cruciale pour s'assurer que la solution offerte évolue convenablement avec les besoins du client au fil du temps. Effectivement, une bonne solution en cybersécurité doit être en constante évolution pour s'adapter à la nouvelle réalité. Dans le cadre d'un partenariat avec Polytechnique Montréal, notre laboratoire travaille avec Neptune-Cyber pour la recherche en cybersécurité maritime. L'objectif du partenariat est de concevoir des architectures résilientes à des cyberattaques pour les navires futurs [27].

1.6 Objectifs de recherche

L'objectif principal de ce mémoire est de concevoir et d'implémenter une infrastructure de test pour la cybersécurité maritime. Cette infrastructure devra simuler différents systèmes maritimes et leurs communications, puis simuler des attaques contre ces systèmes maritimes.

1.6.1 Développement d'une infrastructure de simulation d'un système d'affichage numérique de cartes et la génération de données simulant différents capteurs d'un navire

Le premier sous-objectif de ce mémoire est le développement d'une infrastructure de simulation incluant un système d'affichage numérique de cartes et la génération d'un flux NMEA-0183 provenant de différents capteurs d'un navire. Le but de cette infrastructure est de simuler le système d'affichage central d'un navire, puis de simuler le flux de données provenant normalement de divers capteurs présents sur un navire, et acheminer ce flux au système d'affichage de la même manière dont il serait acheminé sur un vrai navire. Incidemment, notre focalisation lors de la mise en place de cette infrastructure sera placée sur le réalisme de son implémentation et le reflet qu'elle aura de la réalité.

1.6.2 Développement de cyberattaques contre l'infrastructure de test

Une fois l'infrastructure de test mise en place, notre second sous-objectif sera d'implémenter des cyberattaques réalistes contre cette infrastructure. Ces attaques seront développées dans le but d'évaluer l'effort et les compétences nécessaires à un attaquant pour parvenir à exploiter des vulnérabilités à bord d'un navire, puis d'évaluer les impacts des intrusions qui en résultent. De plus, ces attaques simulées permettront éventuellement à la communauté scientifique de tester des solutions à ces cyberattaques sur des systèmes maritimes dans un contexte de simulation réaliste.

1.7 Structure du mémoire

Ce mémoire est constitué de 6 chapitres.

Le chapitre 1, soit l'introduction, présente la problématique de la cybersécurité maritime. Ensuite, nous détaillons notre proposition de solution, notre objectif de recherche ainsi que nos sous-objectifs.

Le chapitre 2 est la revue de la littérature. Dans ce chapitre, nous distinguons les sections suivantes : vulnérabilités des systèmes maritimes, vulnérabilités des protocoles de communication maritimes, solutions proposées pour les systèmes maritimes, solutions proposées pour les protocoles de communication maritimes, puis les infrastructures existantes de simulation de systèmes maritimes.

Le chapitre 3 est notre méthodologie de conception. Ce chapitre établit nos choix de conception d'infrastructure de test, en décrivant nos objectifs de conception, nos caractéristiques critiques et secondaires et notre approche de simulation.

Le chapitre 4 est notre solution proposée. Ce chapitre est séparé en trois sections, soit la mise en place de l'infrastructure de simulation, les attaques contre l'infrastructure, puis la détection de ces attaques.

Le chapitre 5 présente notre expérimentation et nos résultats. Le chapitre a comme sections nos expérimentations de mise en place de l'infrastructure, nos résultats de la mise en place de l'infrastructure, nos expérimentations d'attaques menées contre l'infrastructure, puis nos résultats des attaques menées contre l'infrastructure.

Le chapitre 6 présente nos conclusions, les limites de notre solution et des propositions de travaux futurs.

CHAPITRE 2 REVUE DE LA LITTÉRATURE

Le présent chapitre débutera par présenter différentes normes et réglementations maritimes. Pour continuer, nous présentons les recherches identifiant les vulnérabilités des systèmes informatiques maritimes, puis les vulnérabilités des protocoles de communication maritime. Ensuite, nous présentons les recherches offrant des solutions de protection, puis de détection d'anomalies pour les systèmes maritimes. Pour poursuivre, nous présentons les différentes infrastructures de test et laboratoires de recherche pour la cybersécurité maritime. Finalement, nous discutons et émettons des conclusions sur cette revue de la littérature.

2.1 Normes et réglementations maritimes

Suite aux évènements du 11 septembre 2001, le code régulant la sécurité des navires, le *International Ship and Port Facility Security* (ISPS) a été mis en place. En outre, l'IMO met en place depuis plusieurs années des règlements et lignes directrices pour aider les gens de l'industrie à mieux se protéger contre les menaces potentielles. L'approche de l'IMO se base sur cinq éléments : identification, protection, détection, réponse et récupération [8]. Par ailleurs, la BIMCO a également publié un document de lignes directrices pour la cybersécurité à bord des navires, dans lequel on explique les meilleures pratiques de cybersécurité sur un navire, en plus de conseiller sur la gestion du risque [7].

2.2 Vulnérabilités de systèmes informatiques maritimes

L'arrivée de technologies de plus en plus développées a pu agrémenter le domaine maritime avec des installations plus efficaces et accommodantes. Cependant, si ces nouvelles technologies comportent de nombreux avantages techniques, elles viennent aussi avec leur lot de failles, et donc de vulnérabilités.

2.2.1 Réseaux de technologie de l'information

Les réseaux de technologie de l'information (TI) peuvent être utilisés sur des navires, entre autres pour la navigation, la gestion des cargaisons et l'administration, ils jouent donc un rôle crucial dans le bon fonctionnement d'un navire [28]. Or, ces réseaux sont souvent mal configurés, ont souvent des antivirus n'ayant pas été mis à jour et permettent un accès à

distance avec de tierces parties, ce qui ouvre la porte à diverses failles sécuritaires [29]. Effectivement, l'accès à distance expose ces systèmes à l'extérieur, et donc à de nombreuses menaces.

2.2.2 Systèmes de contrôle industriels (SCI)

Les systèmes de contrôle industriels sur les navires sont utilisés pour réduire les erreurs humaines, augmenter l'efficacité de l'utilisation des ressources, prolonger la vie de l'équipement et assurer certains avantages économiques [30]. Plus précisément, les SCI contrôlent et surveillent des paramètres cruciaux au fonctionnement d'un navire, tels que la température, la pression, le niveau, la viscosité, le contrôle, la vitesse, le voltage, le courant et la machinerie [31]. Pour assurer une interopérabilité entre les composantes, divers appareils et protocoles sont souvent mis ensemble sans le moindre souci de cybersécurité [29]. De plus, les opérateurs et ingénieurs outrepassent de façon routinière les processus de sécurité de ces systèmes à des fins d'efficacité, ce qui aggrave d'autant plus le problème [32].

2.2.3 Systèmes de visualisation des cartes de navigation électroniques

Pour les aider dans la navigation, les pilotes de navire utilisent des outils pour visualiser électroniquement des cartes de navigation - *Electronic Chart Display Information System* (ECDIS). Ces ECDIS ont été rendus obligatoires en 2012 par l'IMO pour tous les navires commerciaux [29, 33]. En plus d'afficher les coordonnées GPS du navire, le système ECDIS permet de visualiser une multitude de données cruciales à la navigation d'un navire, la profondeur de l'eau par exemple. Ainsi, une attaque sur un ECDIS peut potentiellement causer des dommages importants à un navire, privant incidemment l'officier de navigation de plusieurs informations importantes à la navigation. Or, ces systèmes comportent une multitude de failles sécuritaires, notamment par le fait que les ordinateurs sur lesquels ils roulent sont très vieux, avec des systèmes d'exploitation obsolètes sans la moindre mise à jour sécuritaire [29]. Effectivement, CyberKeel a démontré en 2014 que les ECDIS roulant sur des ordinateurs utilisant Windows 7 font face à des cyberattaques pouvant résulter en la modification ou suppression des données du ECDIS [34]. Ces attaques exploiteraient des failles du protocole *Hypertext Transfer Protocol* (HTTP). Ensuite, un attaquant peut non seulement modifier les données du ECDIS, mais aussi les cartes [35]. Effectivement, les cartes y sont chargées manuellement par *Universal Serial Bus* (USB), ou encore par internet, ce qui augmente considérablement les failles sécuritaires et les risques d'intrusion [29]. En 2013, un cas de fausses cartes a eu pour conséquence de faire échouer un navire aux Philippines [35]. Effectivement, le navire dragueur de mines, d'une valeur estimée à 227 M$, a détruit 43 000 pieds carrés

du récif pour une erreur de 8 miles sur les cartes. [36, 37]. Finalement, plusieurs cas ont été reportés selon lesquels des navires ont échoué en raison d'une mauvaise configuration du ECDIS [38, 39], ou encore de sa mauvaise utilisation [40].

2.2.4 GNSS

Le *Global Navigation Satellite System* (GNSS), soit le système émettant des données GPS, est interconnecté avec une multitude d'autres systèmes. Conséquemment, une perte du signal GPS peut occasionner le mauvais fonctionnement d'une panoplie de ces systèmes, tels que le système de positionnement dynamique, le *Automatic Identification System* (AIS) et le *Global Maritime Distress and Safety System* (GMDSS) [41,42]. Or, il a été démontré qu'une ampoule de 100 watts a un signal 1018× plus puissant qu'un signal GPS, celui-ci est donc grandement sujet à de l'interférence [43]. En effet, plusieurs navires ont observé des interruptions dans leur signal GPS en raison de l'interférence entre les ports de Chypre et d'Égypte [44]. Ensuite, plusieurs cas ont montré la vulnérabilité des systèmes GNSS par rapport à des attaques par brouillage GPS [34, 45–47]. Finalement, en 1995, en raison du mauvais fonctionnement du système GPS, le pilote automatique a mené le navire au mauvais endroit, le conduisant ainsi à échouer [48].

2.2.5 Les communications satellitaires

Le *Very Small Aperture Terminal* (VSAT) est une station de communication utilisée pour envoyer et recevoir des données via un réseau satellite [29]. Or, Santamarta a mené en 2014 une évaluation de risques d'une grande variété de VSAT venant de multiples manufacturiers, et la conclusion fut que tous les appareils audités sont vulnérables à des attaques [49]. En outre, James Pavur et al. ont montré en 2020 qu'il était possible de mener des attaques efficaces contre des réseaux VSAT maritimes en utilisant de l'équipement de télévision très accessible pour un coût de moins de 400$ US [50].

2.2.6 VDR, radar et GMDSS

Le système *Voyage Data Recorder* (VDR) comporte plusieurs vulnérabilités permettant à un attaquant d'exploiter des débordements de la mémoire tampon, ou encore de faire de l'injection de commandes [51]. De plus, en 2015, un navire Indien a vu ses fichiers VDR écrasés avec l'utilisation d'une clé USB [51]. Finalement, en 2008, dû à une mauvaise configuration et un manque de familiarité avec le VDR de la part des opérateurs, les données de voyage du MS Finbo Cargo n'ont pas été sauvegardées [52]

Ensuite, si le brouillage radar est plus difficile à effectuer que le brouillage GPS, il est tout de même possible de le faire en utilisant des techniques avancées [42]. C'est en effet le cas d'un navire-lance-missile dont les signaux radar ont été complètement brouillés par un avion en 2014 [47].

Finalement, le système GMDSS comporte des vulnérabilités. En effet, l'installation d'un logiciel malveillant pourrait permettre à un attaquant d'émettre de fausses informations, ou encore d'empêcher toute communication [49].

2.3 Vulnérabilités des protocoles de communication maritime

Dans cette section, nous allons présenter divers protocoles utilisés par les systèmes maritimes, et en évaluer les maintes failles. Les quatre types d'attaques sur lesquels nous nous baserons pour évaluer ces protocoles sont les attaques par déni de service, usurpation de paquets, interception de paquets et attaques par l'homme du milieu. Nous évaluerons les protocoles NMEA-0183, NMEA-2000, NMEA OneNET et AIS.

2.3.1 NMEA-0183

Étant donné que la norme NMEA-0183 supporte généralement un taux de transmission relativement faible, soit d'environ 9600 bit/s, ce protocole rendra vulnérable à des attaques par déni de service tout appareil l'utilisant, dépendamment du moyen de transmission [53]. Ensuite, il a été montré que des attaques de reniflage et d'usurpation de paquets sont très facilement implémentables contre NMEA-0183 [53]. Pour l'usurpation de paquets, des logiciels de génération de données GPS tels que LabSat 3 GPS Simulator peuvent être utilisés [54]. Finalement, une recherche en 2018 a démontré que la norme NMEA-0183 est vulnérable à des attaques par l'homme du milieu. L'attaque consistait en l'utilisation d'un logiciel malveillant pouvant intercepter et modifier des données GPS [55].

2.3.2 NMEA-2000

Tout comme la norme NMEA-0183, NMEA-2000 a un taux de transmission relativement faible, ce qui la rend également vulnérable à des attaques par déni de service. Effectivement, un dispositif malicieux pourrait envoyer une quantité de trafic saturant le passage et empêcher le bon fonctionnement d'un système utilisant NMEA-2000 [56]. Le protocole NMEA-2000 est également vulnérable à des attaques d'usurpation de paquets [57]. Ensuite, étant donné que la structure du protocole NMEA-2000 veut que chaque nœud du réseau reçoive chacun des messages [58, 59], ce protocole est très vulnérable à du reniflage de paquets, en assumant

qu'un accès physique est possible [60]. Finalement, NMEA-2000 fonctionne selon un principe de diffusion des messages, il serait donc possible d'insérer un dispositif entre deux nœuds du réseau filaire pour y faire une attaque par l'homme du milieu. Même si NMEA-2000 comprend une protection de 15 bits appelée *cyclic redundancy check* [61], cette protection ne fait que détecter les erreurs de transmission [60].

2.3.3 NMEA OneNET

Le taux de transmission du protocole NMEA OneNET peut atteindre jusqu'à 10 Gb/s [62]. Conséquemment, tout dépendamment de la configuration logicielle et matérielle, ce protocole aura une bonne résistance contre les attaques de déni de service [60]. Ensuite, la communication OneNET se fait sans fil avec *Internet Protocol version 6* (IPv6). Pour obtenir une connexion sécurisée, un *Human Interface Device* (HID), soit un dispositif permettant la communication entre un humain et un ordinateur créera une connexion *Hypertext Transfer Protocol Secure* (HTTPS) et donnera ainsi accès au réseau sécurisé. Ainsi, il est possible de réaliser des attaques d'usurpation de paquets sur OneNet en usurpant un HID, et en le mettant en mode sécurisé, lui permettant ainsi d'envoyer de l'information [60]. Par rapport au reniflage de paquets, étant donné que OneNet comporte un mode sécurisé à travers lequel toute information transmise sera chiffrée, on ne peut renifler les paquets et avoir directement accès à l'information [63]. Cependant, comme il est possible d'usurper un HID en mode sécurisé, il est possible d'y écouter également les paquets [60]. En outre, le protocole OneNet n'ayant aucun moyen d'authentification des messages [62], il est vulnérable à des attaques de l'homme du milieu. Par contre, une chaîne de 32 bits appelée *sequence number (SQ)* est utilisée pour prévenir les attaques par rejeu [60].

2.3.4 Système d'échanges automatisés de messages

Les navires échangent des messages en utilisant le protocole de communication AIS. Ce protocole de communication est un système de radio diffusion utilisé par les services de *Vessel Traffic Services* (VTS), les opérations de rescousse, les investigations d'accident et les données météorologiques. Étant donné la nature critique de ces applications, il est impératif que la transmission des informations par le protocole AIS se fasse en toute intégrité. Or, étant donné que ce protocole communique sans authentification ni vérification d'intégrité, des attaquants pourraient injecter de faux signaux via une radio logicielle, ou encore rendre un navire invisible [64].

Comme AIS a un taux de transmission d'information d'environ 9600 bit/s, c'est un protocole très vulnérable à des attaques de déni de service [65]. Ensuite, tel qu'énoncé précédemment, AIS est également très vulnérable à de l'usurpation et au reniflage de paquets [66]. Finalement, un attaquant pourrait facilement effectuer une attaque par l'homme du milieu sur des messages AIS, soit par radio fréquence, soit logiciellement [66].

2.4 Solutions de protection pour les systèmes maritimes

Dans la littérature scientifique, on retrouve plusieurs types de solutions. Tout d'abord, nous avons les solutions de protection, parmi lesquelles on retrouve les méthodes d'analyse de risque, puis les solutions de protections spécifiques.

2.4.1 Méthodes d'analyse de risque

Une première approche pour la protection est la mise en place de méthodes d'analyse de risque, permettant un développement et une utilisation plus avisée de l'équipement maritime. Effectivement, en connaissant mieux les risques, les acteurs du milieu maritime seront plus en mesure de mitiger les menaces auxquelles ils font face.

Il existe des plateformes permettant d'évaluer les cyberrisques pour un scénario maritime donné. Notamment, des chercheurs de l'Université de Plymouth ont mis sur pied *ModelBased Framework for Maritime Cyber-Risk Assessment* (MaCRA), qui permet d'évaluer les cyber risques d'un scénario maritime donné en se basant sur des modèles [67]. En outre, ces modèles se basent sur de vraies données et peuvent s'agir, par exemple, d'une modélisation des divers types d'attaquants. Pour aider dans la prise de décision, cette plateforme cherche à fournir à ses utilisateurs les cinq éléments suivants : une caractérisation des cyberrisques maritimes et leur sévérité respective, des mesures des navires, l'identification des systèmes pour lesquels une amélioration sécuritaire serait davantage bénéfique, l'identification des principaux risques et attaquants, la prestation à l'utilisateur des données sur les risques lui étant utiles dans sa prise de décision. Contrairement aux recherches précédentes dans ce domaine, MaCRA permet également de s'adapter aux nouvelles technologies et failles sécuritaires trouvées, ce qui n'était pas pris en compte avant [67].

Selon Kimberly Tam et Kevin Jones de l'Université de Plymouth, la limite des plateformes d'évaluation des cyberrisques comme MaCRA est leur incapacité de mettre à jour les risques identifiés selon le changement de divers facteurs tel que l'environnement, ou encore des fac-

teurs humains [68]. Leur recherche prétend qu'une amélioration des plateformes existantes en incluant ces facteurs est de mise pour assurer une prise de décision optimale basée sur des risques évalués de façon précise.

Une autre approche à ce problème serait de développer un processus d'évaluation applicable à tous les navires et permettant d'identifier leurs risques respectifs [69]. En effet, des chercheurs de l'Université de Rijeka ont développé un processus d'évaluation des risques. En se basant sur des entrevues menées auprès des membres d'un équipage naval, un processus d'évaluation en trois phases a été développé : une évaluation des activités de préparation, une évaluation de la conduite, et une évaluation des résultats de communication. Ce processus a été testé sur le navire Fukae-maru et est applicable à tous les navires, offrant ainsi des lignes directrices pour mitiger les cyberrisques existants.

Même si ces plateformes peuvent permettre aux marins de mieux gérer les risques sécuritaires sur leur navire, elles ne résolvent pas les problèmes de cybersécurité pour autant. Voyons voir les approches abordant directement les problèmes de cybersécurité sur les navires.

2.4.2 Solutions de protection spécifiques

Systèmes de contrôle industriels

Les systèmes de contrôle industriels jouent un rôle clé dans le fonctionnement des navires, et ce rôle sera appelé à s'élargir avec le développement des navires autonomes et les navires sans équipage. Or, comme relaté dans la section 2.2, les systèmes de contrôle industriels sont exposés à de multiples vulnérabilités.

Pour pallier les failles sécuritaires des systèmes de contrôle industriels maritimes, examinons les solutions présentées au niveau des SCI en général. En 2011, Stouffer, Falco et Scarfone ont élaboré un guide pour la sécurité des systèmes de contrôle industriels. Ce guide présente une suite d'étapes permettant de gérer les risques sécuritaires des systèmes de contrôle industriels. Cette suite d'étapes consiste à catégoriser les systèmes d'information du SCI, sélectionner les contrôles de sécurité, implémenter les contrôles de sécurité, évaluer les contrôles de sécurité, autoriser le système d'information et surveiller les contrôles de sécurité [70]. Ayant été cité plus de 1600 fois, ce guide est considéré comme une bible en matière de sécurité des SCI.

Communications satellitaires

Les communications satellitaires sont beaucoup utilisées sur les navires, notamment en raison de leurs nombreux avantages, dont leur faible coût et leur grande fiabilité. Cependant, tel que démontré dans la section 2.1.5, les communications satellitaires comme VSAT comportent de nombreuses failles sécuritaires.

Yi et al. ont proposé une analyse de trois différentes méthodes d'accord de clés sécurisées permettant supposément de protéger les outils de communications satellitaires comme VSAT contre des attaques d'usurpation d'identité [71]. Parmi ces trois méthodes, on retrouve l'utilisation d'un schéma de jacobi, d'un schéma Diffie-Hellman modifié et un Diffie-Hellman modifié avec un accord de clé. Ils ont démontré qu'aucune de ces méthodes ne permettait vraiment de prémunir une telle protection aux VSAT.

Lee Cheng-Chi a publié en 2013 un article proposant une méthode d'accord de clé simple basée sur des cartes chaotiques offrant une bonne sécurité à l'outil de communication satellitaire VSAT [72]. Effectivement, Lee Cheng-chi postule qu'une telle méthode permet de protéger les communications satellitaires contre toutes les attaques cryptographiques connues avec une confidentialité persistante parfaite. De plus, la solution proposée occasionne de plus faibles coûts de calcul que les solutions comparables.

Finalement, Zhijun et al. ont proposé en 2018 une solution d'authentification des communications VSAT, nommée *Lite Certification Authority* (Lite-CA) [73]. L'objectif de Lite-CA est de réduire, au sein d'un réseau VSAT, le nombre d'interactions simultanées. Cette solution explore un nouvel algorithme de cryptage-HW-F, remplaçant ainsi les systèmes de chiffrement à clé publique et de chiffrement symétrique. Leurs expérimentations ont démontré que l'utilisation de Lite-CA peut être une solution pour augmenter la fiabilité de VSAT.

2.5 Solutions de détection d'anomalies pour les systèmes maritimes

Après les solutions de protection, on retrouve également les solutions de détection, plus précisément d'anomalies. Au lieu de protéger en amont, les solutions de détection arrivent plus tard dans la séquence et sont plutôt en réaction dans le but de détecter les anomalies en aval et permettre au système d'agir en conséquence.

2.5.1 Systèmes d'échanges automatisés de messages

Pour le protocole AIS, dont les failles de sécurité sont particulièrement importantes, plusieurs solutions de détection d'anomalies ont été proposées.

Rikard Laxhammar, Goran Falkman et Egils Sviestin ont comparé deux méthodes de détection d'anomalie dans le trafic naval basées sur les statistiques [74]. La première méthode est un modèle de mélange gaussien, puis la seconde est un estimateur adaptatif de densité de noyau. Ces deux modèles ont été testés en utilisant des données AIS enregistrées. Les résultats ne montraient pas une méthode significativement supérieure à l'autre. En outre, les résultats de détection d'anomalies étaient plutôt décevants étant donné la forte distance que les navires avaient le temps de parcourir avant que la détection d'anomalie ne soit complétée.

Les chercheurs Clément Iphar et al. proposent de définir certaines métriques avec lesquelles on évaluera diverses données extraites d'un message AIS pour déterminer sa validité [75]. Ces données sont composées de 16 informations contenues dans un message AIS, dont le numéro d'identification, la latitude, etc. Les métriques avec lesquels ces données sont analysées sont, entre autres, la précision, la consistance et l'intégrité [75].

Une autre problématique du protocole AIS est la mise en veille intentionnelle de l'émetteur. En effet, à des fins de surveillance, tous les navires doivent émettre leurs positions et diverses informations en permanence à l'émetteur AIS. Cet émetteur tombe parfois en panne. Cette panne peut être justifiée, mais peut également être intentionnelle pour tenter de camoufler des activités illicites. Pour remédier à ce problème, Fabio Mazzarella a proposé un modèle basé sur l'apprentissage machine pour détecter les pannes intentionnelles des émetteurs AIS [76].

2.5.2 Utilisation d'ontologies

Créées dans les années 1990 dans le but de pallier les failles des différents systèmes experts, les ontologies sont apparues comme une nouvelle approche conceptuelle pour la modélisation des connaissances [77]. Récemment, les ontologies sont de plus en plus pertinentes pour la détection d'anomalie. Effectivement, la création d'un système expert basé sur des ontologies semble être efficace en matière de cybersécurité et est également applicable au milieu maritime [78].

Jean Roy et Michael Davenport ont proposé en 2010 une solution de raisonnement automatisée basée sur les ontologies pour aider les marins dans la détection d'anomalie et de menace [79]. Cependant, cette solution reste un prototype à petite échelle et ne semble pas prête pour une application concrète dans l'industrie navale.

Arnaud Vandecasteele et Aldo Napoli ont proposé l'utilisation d'une ontologie pour la détection d'anomalie en intégrant la dimension spatiale dans l'ontologie. Ce faisant, les experts du domaine pouvaient alors préciser des règles pour gérer les comportements anormaux des navires. Le résultat de cette recherche semble très concluant étant donné qu'il permet d'analyser le comportement de plusieurs milliers de navires simultanément [80].

2.6 Infrastructures de tests et laboratoires de recherche pour la cybersécurité maritime

En 1999, Fred Cohen a émis le constat comme quoi la modélisation et la simulation ne produisaient pas de bons résultats dans le domaine de la protection de l'information. Ainsi, il a évalué l'option de simulation de cyberattaques, défenses et conséquences dans un système informatique complexe [81]. Même si cet article date et avait à l'époque peu d'applications pratiques, il a tout de même pavé la voie au développement d'outils de simulation dans le domaine de la cybersécurité.

2.6.1 Cyber Ranges

Les environnements comportant la simulation, l'émulation, des éléments physiques d'un système, tout en incorporant des simulations d'attaque et de détection peuvent être des solutions optimales à des problèmes complexes de cybersécurité [82]. En l'occurrence, les *Cyber Ranges* sont des environnements comportant des composantes virtuelles et physiques permettant de s'entraîner en représentant des scénarios complexes [83]. La cible de ces environnements est généralement les experts en cybersécurité voulant apprendre comment traiter des vulnérabilités en se pratiquant dans un environnement représentatif de la réalité. Le *Cyber Range* simulera des scénarios d'attaques sur le réseau, l'infrastructure, ou encore les logiciels. En plus de l'entraînement, le *Cyber Range* a également pour but de servir d'environnement de test pour des solutions de défense cybersécuritaire [84].

L'utilisation des *Cyber Ranges* pour la détection de menaces et la prévention n'a commencé plus sérieusement que dans la dernière décennie (2010 à 2020) [85]. Selon Yamin et al., deux critères priment pour le développement d'un *Cyber Range*. Le premier critère est l'évolutivité, permettant à l'environnement d'augmenter sa capacité d'entraînement. Le second critère est la fédération, concept selon lequel plusieurs *Cyber Ranges* peuvent être combinés pour offrir une simulation encore plus complète [85].

2.6.2 Cyber-MAR

L'application du concept de *Cyber Range* au domaine maritime pourrait faire grandement avancer la cybersécurité maritime [86]. D'ailleurs, le projet nommé Cyber-MAR vise le développement d'un environnement de simulation dans le contexte du domaine maritime, en utilisant une approche basée sur les *Cyber Ranges*. La plateforme se veut être une plateforme basée sur la connaissance, mais aussi un outil de prise de décision en matière de sécurité maritime [87].

2.6.3 Grace Maritime Cyber Testbed

En mars 2021, l'évènement HacktheMachine, organisé par la compagnie Fathom 5 et Booz Allen Hamilton, a eu lieu. Cet évènement comprenait plusieurs compétitions de types *Capture the Flag* (CTF) dans lesquelles des pirates informatiques compétitionnaient pour des prix en tentant de déjouer la sécurité de divers systèmes. Parmi ces compétitions, on trouve Maritime Cyber, dont le but des participants était d'attaquer une infrastructure répliquant l'environnement d'un navire. L'infrastructure, nommée Grace Maritime Cyber Testbed, a été développée par Fathom 5 et comporte de l'équipement électronique utilisé à bord des navires [88].

Grace Maritime Cyber Testbed est constitué de deux sections. Tout d'abord, la console de navigation. Cette console comprend un ECDIS, un pilote automatique, un capteur de vitesse à travers l'eau, une station de captation de données météo et un gouvernail. La communication entre ces équipements maritimes se fait avec la norme NMEA-2000. La seconde partie de l'infrastructure de test est la console des moteurs. Cette console comprend deux manettes de moteur, un actionneur d'accélérateur, une unité de contrôle, une unité de transmission et une hélice. La communication entre ces équipements maritime se fait par *Controller Area Network* (CAN) *bus*. En outre, l'infrastructure utilise un dispositif mécanique pour activer les capteurs, et ainsi faire croire au système qu'il est sur un vrai navire en mouvement sur l'eau [89]

Si elle a été développée dans le cadre de l'évènement HacktheMachine, cette infrastructure vise également à aider et enrichir la communauté de recherche en cybersécurité maritime. Effectivement, une telle infrastructure aidera la communauté en termes de recherche de vulnérabilité et de solutions à cesdites vulnérabilités [88].

2.6.4 Laboratoire dédié à la cybersécurité maritime

Étant donné la forte croissance d'utilisation d'outils numériques sur les navires, le risque de cyberattaques dans le milieu maritime est grandissant, mais la recherche dans ce domaine ne semble pas être proportionnelle aux risques. Pour pallier ce problème, l'Université de Plymouth a proposé Cyber-SHIP, un laboratoire visant à assurer un meilleur développement pour la recherche en cybersécurité maritime. Effectivement, ce laboratoire spécialisé combine des technologies maritimes aux laboratoires traditionnels de cybersécurité. En outre, ce laboratoire a pour objectif d'ouvrir de nouveaux horizons en matière de capacités cybermaritimes. La prochaine génération de laboratoire de cybersécurité devrait contenir des systèmes maritimes non simulés [90].

2.7 Discussion

Cette revue de la littérature des divers apports de la communauté scientifique au domaine de la cybersécurité maritime nous permet de faire les observations suivantes. Tout d'abord, les failles cybersécuritaires dans le domaine maritime sont nombreuses et diversifiées. Ensuite, des solutions de protection générale telles que les méthodes d'analyse de risque sont disponibles, de même que quelques solutions de protection spécifiques. En outre, on compte un bon nombre de solutions de détection d'anomalies, notamment pour AIS. Cependant, toutes ces initiatives n'attaquent pas le problème dans son ensemble en considérant les trois caractéristiques propres à la problématique identifiées au chapitre 1, soit l'étendue de la menace, l'unicité des systèmes informatiques de chaque navire et le facteur humain. Nous croyons qu'une infrastructure de test pourrait s'attaquer efficacement au problème en considérant ces trois caractéristiques.

Le développement d'infrastructures de tests dans le domaine de la cybersécurité maritime commence tranquillement, notamment avec Cyber-MAR, ou encore le Grace Maritime Cyber Testbed. Cependant, le projet Cyber-MAR n'est pas encore abouti, et l'architecture du Grace Maritime Cyber Testbed ne reste que superficiellement connue du grand public.

Conséquemment, nous proposons de développer une infrastructure de test pour la simulation de systèmes maritimes. Effectivement, une telle initiative permettrait d'analyser les vulnérabilités des systèmes maritimes dans un contexte réaliste. Ensuite, cette infrastructure nous permettrait d'analyser et de tester l'effet de diverses attaques potentielles contre des systèmes maritimes, puis d'analyser et de tester des solutions de protection et de détection sur ces différents systèmes. En outre, cette infrastructure pourrait avoir un rôle d'entraînement et d'éducation au sein de la communauté maritime. Une telle infrastructure permettrait à

la communauté maritime de mieux évaluer les risques et de mieux se prémunir contre eux. Cette infrastructure considérera la grande étendue des vulnérabilités des systèmes maritimes, l'unicité des systèmes de chacun des navires ainsi que le facteur humain.

CHAPITRE 3 MÉTHODOLOGIE DE CONCEPTION DE L'INFRASTRUCTURE DE TEST

Dans ce chapitre, nous établissons trois étapes préalables à la conception d'une infrastructure de test en matière de cybersécurité. Tout d'abord, nous définissons les objectifs de conception de notre infrastructure, dans le but de faire des choix de conception éclairés et congruents. Ensuite, en fonction de ces choix de conception, nous établissons différentes caractéristiques d'une infrastructure de test sur lesquelles nous nous appuierons pour prendre nos décisions de conception. Finalement, nous choisissons l'approche de simulation à adopter dans le cadre de mes travaux.

3.1 Objectifs de conception

Différentes architectures d'infrastructure de test peuvent engendrer des résultats complètements différents. Pour cette raison, il est important de définir à l'avance des objectifs de conception sur lesquels nous pourrons nous appuyer pour notre architecture de tests [91]. L'analyse des travaux existants permet d'identifier neuf objectifs différents de conception pour une infrastructure de test : analyse et test d'attaques, analyse d'impacts, analyse de vulnérabilités, éducation et entraînement, analyse de menaces, analyse de performance et création de politiques et normes, analyse et test de mécanismes de protection et analyse et test de mécanismes de détection [92].

Dans le cadre de nos travaux, quatre objectifs parmi ceux présentés sont sélectionnés pour la mise en place de notre infrastructure de test :

1. Analyse de vulnérabilités
2. Analyse et test d'attaques
3. Éducation et entraînement
4. Analyse et test de mécanismes de détection

Nous postulons que ces quatre objectifs de conception permettront le plus à notre infrastructure de servir comme vecteur de solutions à la problématique identifiée au chapitre 1. En effet, la grande étendue des failles potentielles, l'unicité de chacun des navires et la grande part que joue le facteur humain nécessitent que notre infrastructure doive nous permettre de

bien analyser et exploiter des vulnérabilités à travers des scénarios d'attaques, explorer des mécanismes de détection d'attaques, puis traiter le facteur humain en pouvant être utilisée comme outil d'éducation et d'entraînement.

Ces quatre objectifs de conception nous permettent d'éclairer nos choix de conception et d'architecture par rapport à notre infrastructure de test. Voici une description plus approfondie de chacun de ces objectifs dans le cadre de nos travaux.

Analyse de vulnérabilités

Le premier objectif de notre infrastructure de test pour la cybersécurité des systèmes maritimes est de pouvoir explorer les différentes vulnérabilités existantes sur un navire. Effectivement, en ayant une infrastructure reflétant le plus possible la réalité, nous sommes en mesure de mieux cibler les failles présentes et potentiellement exploitables, et ainsi développer des scénarios d'attaque réalistes.

Analyse et test d'attaques

Le second objectif est de pouvoir modéliser des scénarios d'attaques réalistes et de les tester au sein d'une infrastructure de simulation. Après avoir simulé ces attaques, notre objectif est de faire une analyse approfondie de ces attaques. Cette analyse peut évaluer l'effort et les compétences nécessaires à un attaquant pour réaliser ces attaques, puis évaluer et discuter des impacts qui en résultent. Ultimement, cela permet de préparer le terrain pour les tests des solutions de protection et de défense des navires.

Éducation et entraînement

Un autre objectif de notre infrastructure de test sera de faire de l'éducation et de l'entraînement auprès des professionnels du domaine maritime, ou encore des spécialistes en cybersécurité. Effectivement, comme mentionné précédemment, un des facteurs importants en matière de cybersécurité maritime est le facteur humain [93], celui-ci est donc au cœur de la remédiation des vulnérabilités pour ces systèmes maritimes. Conséquemment, avec notre infrastructure de test, il serait de pouvoir nous en servir comme plateforme à travers laquelle divers acteurs du milieu maritime pourraient apprendre et s'entraîner à la cybersécurité des systèmes maritimes. Ces acteurs sont des personnes en lien avec les systèmes maritimes et la navigation, que ce soit en tant qu'utilisateur, de fournisseur de produit ou de composantes, ou encore en tant que concepteur de protocoles de communication. Une telle plateforme

permettrait ainsi d'éduquer les personnes impliquées dans ces environnements navals dont la sensibilisation et les connaissances ont un impact direct sur la vulnérabilité de certains systèmes maritimes.

Analyse et test de mécanismes de détection

Pour cet objectif, nous voulons que l'architecture de l'infrastructure soit propice à l'implantation de diverses solutions pour pouvoir les analyser dans un contexte de simulation réaliste. Ces tests et analyses pourraient autant être effectués dans l'industrie maritime que dans le domaine de la recherche universitaire en matière de cybersécurité maritime.

3.2 Caractéristiques des infrastructures de test

Notre revue de la littérature nous a permis d'identifier plusieurs travaux examinant les caractéristiques influençant positivement la crédibilité d'une infrastructure de test [94, 95]. Après une analyse de notre part, nous retenons les travaux de Daniel Ani, Nurse et Craggs, qui ont adopté une approche englobante et très applicable à nos travaux. Effectivement, Daniel Ani, Nurse et Craggs ont analysé 41 articles portant sur des infrastructures de test pour la cybersécurité de systèmes industriels, et ils ont pu identifier des caractéristiques de conception ayant un impact sur la crédibilité de ces infrastructures [92]. À la lumière de cette revue de la littérature, nous pensons qu'il est important de considérer et de démontrer certaines de ces caractéristiques de conception dans le but de développer une infrastructure de test réutilisable dans le domaine de la cybersécurité. Effectivement, une infrastructure répondant davantage à ces critères augmentera la valeur de ses résultats dans un contexte de cybersécurité.

3.2.1 Options de caractéristiques

Fidélité La fidélité d'une infrastructure de test est le degré de corrélation entre la simulation et le monde réel. Pour quantifier la fidélité d'une infrastructure, on se fie généralement à l'approche utilisée, c'est-à-dire, une approche de simulation logicielle, une approche de simulation physique ou une approche hybride. Généralement, plus une infrastructure comporte des simulations physiques, plus la fidélité de cette infrastructure sera élevée, alors qu'une infrastructure comportant davantage de simulations logicielles aura une fidélité plus basse. Dans le cadre de notre recherche, la fidélité de notre infrastructure résidera également dans le degré de réalisme de ses simulations. Effectivement, simuler un flux de données assez complexe et réaliste pour se rapprocher du flux généré sur un vrai navire augmenterait la fidélité de notre infrastructure.

Évolutivité L'évolutivité d'une infrastructure de test reflète sa capacité à élargir sa configuration et ses fonctionnalités. Pour le cas de notre infrastructure de test, avoir une architecture permettant l'ajout de capteurs dans ses multiples sous-systèmes démontrerait une bonne évolutivité, étant donné que ses fonctionnalités peuvent être élargies sans avoir à recréer une infrastructure à partir de rien.

Flexibilité La flexibilité d'une infrastructure de test consiste en sa capacité à adapter et redéfinir son utilisation pour différents scénarios. Pour le cas de notre infrastructure, faire en sorte qu'elle puisse être utilisée pour tester différents scénarios d'attaques en plus de faire de l'analyse de solutions de détection assurerait une bonne flexibilité pour notre infrastructure, étant donné qu'elle pourra facilement s'adapter et redéfinir son utilisation.

Reproductibilité La reproductibilité d'une infrastructure de test reflète sa propension à reproduire cette infrastructure et les scénarios modélisés. Pour le cas de notre infrastructure, on peut simplement documenter exhaustivement la configuration, l'architecture et les scénarios de l'infrastructure pour s'assurer de pouvoir reproduire les scénarios de façon identique. D'un point de vue scientifique, la reproductibilité est essentielle si l'on veut pouvoir recréer un environnement et des scénarios, pour y tester des solutions par exemple.

Modularité La modularité d'une infrastructure de test reflète sa capacité d'adaptation à de nouvelles exigences. Pour notre infrastructure, lui permettre d'incorporer de nouveaux protocoles pour garder le rythme des pratiques de l'industrie lui assurerait une bonne modularité. Typiquement, une architecture permettant une simulation d'un réseau ou l'ajout d'éléments physiques donnera une infrastructure de test modulable.

Mesurabilité La mesurabilité d'une infrastructure de test désigne sa capacité à quantifier le processus de test sans pour autant affecter le résultat final. La mesurabilité de notre infrastructure de test pourrait être démontrée en incluant des outils mesurant diverses métriques de performance, telles que le temps de réponse.

Coût-efficacité Le coût-efficacité d'une infrastructure de test reflète sa capacité à atteindre des objectifs et scénarios en respectant un budget abordable dans un contexte de recherche. Dans notre contexte de recherche universitaire, notre budget et espace est relativement bas. De plus, pour notre infrastructure de test, de multiples choix de conception auront un impact majeur sur cette caractéristique. Par exemple, l'utilisation d'une machine virtuelle pour simuler un environnement peut s'avérer moins coûteuse que l'utilisation d'équipement physique.

Un autre exemple est l'utilisation d'un simulateur gratuit au lieu d'un simulateur payant pour faire en sorte que l'infrastructure de test coûte moins cher à mettre sur pied. Cependant, l'augmentation du coût-efficacité peut avoir un impact négatif sur la fidélité lorsque l'outil moins coûteux ne confère pas le même réalisme que le plus coûteux.

Exécution sécuritaire L'exécution sécuritaire veut que la simulation des différents scénarios au sein de l'infrastructure de test n'affecte en rien la sécurité des éléments dans le vrai monde. Dans le cas de notre infrastructure, nous pourrions démontrer l'exécution sécuritaire en ayant une architecture complètement séparée de tout réseau. De cette façon, les expérimentations menées au sein de l'infrastructure de test n'auront aucun impact sur un système utilisé dans le monde réel.

Diversité La diversité d'une infrastructure de test reflète sa capacité à, sans affecter son évolutivité, inclure une grande variété de composantes dans le but d'assurer la simulation d'un large éventail de configurations. Pour notre infrastructure, nous pourrions démontrer sa diversité en donnant la possibilité de simuler une multitude de données, ou encore en permettant différents protocoles de communication maritime.

Convivialité La convivialité d'une infrastructure de test désigne sa capacité à être utilisée par un large éventail d'utilisateurs, dans le but de limiter le nombre d'erreurs d'utilisation. On peut démontrer la convivialité de notre infrastructure de test en développant des interfaces utilisateur simples et efficaces, de façon à ce que notre infrastructure puisse être utilisée et configurée à bon escient par le plus d'utilisateurs possible.

Interopérabilité L'interopérabilité d'une infrastructure de test consiste en sa capacité à combiner des simulations logicielles avec des simulations physiques. Nous pourrions démontrer l'interopérabilité de notre infrastructure en ayant une section de simulation complètement logicielle, tout en la faisant communiquer avec une section comportant des capteurs physiques.

Surveillance et journalisation La surveillance et journalisation d'une infrastructure de test reflète sa capacité à surveiller et enregistrer des informations sur la simulation. Nous pourrions démontrer la surveillance et la journalisation de notre infrastructure en ayant une console d'affichage des évènements survenus au sein de l'infrastructure, puis un enregistrement de ces évènements.

Complexité La complexité d'une infrastructure de test désigne la transparence de l'architecture dans le but de pouvoir modifier des données de n'importe quelle zone de l'infrastructure.

Ouverture L'ouverture d'une infrastructure de test désigne sa capacité à supporter l'accès à distance.

3.2.2 Choix des caractéristiques

Après avoir extrait les caractéristiques de conception, Daniel Ani, Nurse et Craggs ont analysé leur impact sur la crédibilité d'une infrastructure de test pour en extraire des pourcentages d'impact de crédibilité [92]. Cette analyse a été effectuée dans le contexte des infrastructures de test en général, soit industrielles et universitaires. Les pourcentages extraits représentent la proportion d'impact respective de chacune de ces caractéristiques sur la crédibilité d'une infrastructure de test. Le tableau 3.1 illustre ces caractéristiques classées en ordre décroissant de leur proportion d'impact.

Tableau 3.1 Caractéristiques et leur proportion d'impact sur la crédibilité d'une infrastructure de test

Caractéristiques	Proportion d'impact (%)
Fidélité	41,46
Évolutivité	28,83
Flexibilité	19,51
Reproductibilité	19,51
Modularité	17,07
Coût-efficacité	9,76
Mesurabilité	9,76
Exécution sécuritaire	7,32
Diversité	4,88
Convivialité	4,88
Interopérabilité	2,44
Surveillance et journalisation	2,44
Complexité	2,44
Ouverture	2,44

Nous postulons qu'il n'est pas envisageable d'accorder un degré d'importance maximal à la totalité de ces caractéristiques. Effectivement, mettre l'accent sur autant de caractéristiques nous compliquerait la tâche et nous empêcherait de nous ferait diverger de nos propres objec-

tifs. Conséquemment, nous classons ces caractéristiques en différentes catégories de priorités en nous basant sur deux critères : les objectifs de conception de notre infrastructure de test, puis le degré d'influence qu'aura chacune de ces caractéristiques sur la crédibilité de notre infrastructure, soit les pourcentages indiqués dans le tableau 3.1. De plus, étant donné que ces pourcentages ont été extraits dans un contexte industriel et universitaire, nous pourrons réévaluer certains d'entre eux pour les adapter à notre contexte universitaire. Effectivement, nous pensons que pour une recherche universitaire, la reproductibilité est une caractéristique de conception particulièrement critique pour une infrastructure de test, étant donné le besoin de reproduction des expérimentations et résultats par d'autres chercheurs. De plus, le coût-efficacité sera à considérer davantage étant donné les limites budgétaires du milieu universitaire.

Nous classons ces caractéristiques en trois catégories : caractéristiques critiques, caractéristiques secondaires et caractéristiques optionnelles. Pour chaque catégorie, nous allons présenter chacune des caractéristiques s'étant classifiées en expliquant à la lumière de son pourcentage d'impact sur la crédibilité d'une infrastructure de test et de nos objectifs choisis.

Caractéristiques critiques

La première caractéristique que nous considérons comme critique est l'évolutivité. En effet, étant donné que nous avons comme objectifs de conception l'éducation et l'entraînement, notre infrastructure a des visées à long terme, et nous prévoyons en faire une plateforme de référence pour les années à venir. De ce fait, il est crucial que l'infrastructure puisse évoluer et jouir d'ajouts au fil du temps sans avoir à recréer l'architecture à partir de rien. De plus, l'évolutivité a un taux d'impact sur la crédibilité d'une infrastructure de test de 28,83%, ce qui est élevé.

La seconde caractéristique est la flexibilité. Effectivement, nous avons comme objectifs de conception «l'analyse et test d'attaques», puis «l'analyse et test de solutions de détection». Or, pour être en mesure de tester et analyser l'impact de diverses attaques ou solution de détection, notre plateforme doit être en mesure de facilement s'adapter et redéfinir son utilisation. Finalement, la flexibilité a un taux d'impact de plus de 19%, ce qui est relativement élevé.

La troisième caractéristique est la reproductibilité. En effet, nous comptons parmi nos objectifs de conception l'analyse et le test d'attaques et de solutions de détection. Or, pour être en mesure d'avoir des résultats crédibles, notre infrastructure doit produire des résultats les plus

similaires possibles pour deux essais donnés. De plus, comme la flexibilité, la reproductibilité a un pourcentage d'impact de plus de 19%, ce qui est relativement élevé, il est important de la considérer.

La quatrième caractéristique que nous considérons comme critique pour la conception de notre infrastructure est la modularité. Effectivement, étant donné que les normes et protocoles du domaine maritime tendent à se redéfinir et évoluer au fil du temps, il est important que notre infrastructure puisse s'adapter facilement aux nouvelles exigences pour rester pertinente. De plus, la modularité aura un impact sur plusieurs de nos objectifs de conception, tels que l'analyse de vulnérabilités, l'analyse et test d'attaques et l'analyse et test de mécanismes de détection.

La cinquième caractéristique d'intérêt critique dans nos travaux est le coût-efficacité. Effectivement, comme nous sommes dans un contexte de recherche universitaire et que nous ne possédons pas un budget et un espace illimité, nous nous devons de garder une considération de rapport qualité/prix, même si nous voulons optimiser la fidélité. De ce fait, une réflexion se devra d'être faite lorsque nous serons confrontés à un dilemme où nous pourrions avoir une meilleure fidélité en échange de matériel coûteux.

La dernière caractéristique est la convivialité. En effet, comme un de nos objectifs de conception est l'éducation et l'entraînement, notre plateforme se doit d'être conviviale pour le plus d'utilisateurs possible de la plateforme dans le but d'éviter les erreurs d'utilisation et de configuration.

Caractéristiques secondaires

La première caractéristique que nous considérons comme secondaire est la fidélité. Effectivement, la fidélité est la caractéristique qui aura le plus d'impact sur la crédibilité de notre infrastructure (41,46%), et nous voulons donc que notre infrastructure soit une représentation la plus réaliste possible de la réalité. Cependant, étant dans un contexte universitaire et n'ayant pas des ressources monétaires et d'espace illimités, nous devons tout de même garder un équilibre et ne pas viser la fidélité à tout prix. Conséquemment, nous avons choisi de considérer considérer le coût-efficacité comme caractéristique critique, puis la fidélité comme caractéristique secondaire.

La seconde caractéristique est la mesurabilité. En effet, la mesurabilité de l'infrastructure a un impact sur deux de nos objectifs de conception, soit l'analyse et test d'attaques, puis l'analyse et test de mécanismes de détection. De plus, la proportion d'impact de la mesurabilité sur la crédibilité d'une infrastructure est de 9,76%, ce qui est moyennement élevé.

La troisième caractéristique est l'exécution sécuritaire. En effet, même si cette caractéristique n'aura pas d'impact sur nos quatre objectifs de conception, sa proportion d'impact sur la crédibilité d'une infrastructure de test est de 7,32%, ce qui est moyennement élevé.

La dernière caractéristique est la diversité. Effectivement, étant donné que nous avons comme objectifs l'analyse et test d'attaques et de solutions de détection en plus de l'analyse de vulnérabilités, nous devons avoir un système doté d'une certaine diversification. Cependant, la diversité tend à faire baisser l'évolutivité, qui est une de nos caractéristiques critiques. Conséquemment, une réflexion devra avoir lieu lorsque nous ferons face à une situation où un choix fera augmenter une caractéristique au détriment de l'autre.

Caractéristiques optionnelles

Les caractéristiques que nous ne considérons pas activement dans la conception de notre infrastructure de test sont l'interopérabilité, la surveillance et journalisation, la complexité et l'ouverture. Effectivement, ces caractéristiques ont toutes un faible taux d'impact sur la crédibilité d'une infrastructure de test, en plus de ne pas avoir de lien spécifique avec l'un de nos objectifs de conception.

En somme, le tableau 3.2 illustre les caractéristiques considérées par rapport à leur impact sur nos objectifs de conception choisis.

Tableau 3.2 Impacts des caractéristiques de conception d'une infrastructure de test sur les objectifs de conception choisis

			Objectifs de conception de l'infrastructure de test			
	Caractéristiques	Proportion d'impact (%)	Analyse de vulnérabilités	Analyse et test d'attaques	Éducation et entraînement	Analyse et test de mécanismes de détection
Crtitiques	Évolutivité	28,83			x	
	Flexibilité	19,51	x	x		x
	Reproductibilité	19,51	x	x		x
	Modularité	17,07	x	x		x
	Coût-efficacité	9,76				
	Convivialité	4,88			x	
Secondaires	Fidélité	41,46	x	x	x	x
	Mesurabilité	9,76		x		x
	Exécution sécuritaire	7,32				
	Diversité	4,88	x	x		x
Optionnelles	Interopérabilité	2,44				
	Surveillance et journalisation	2,44				
	Complexité	2,44				
	Ouverture	2,44				

Comme on peut le voir, les catégories de caractéristiques critiques, secondaires et optionnelles sont illustrées respectivement par le vert, le jaune et le rouge. On constate que les caractéristiques critiques ont généralement un taux d'impact sur la crédibilité d'une infrastructure de test plus élevé, ou encore un fort impact sur nos objectifs de conception, alors que les caractéristiques optionnelles n'ont pas d'impact sur nos objectifs de conception, en plus d'avoir un faible taux d'impact sur la crédibilité d'une infrastructure de test.

3.3 Approches de simulation

Dans le cadre du développement d'une infrastructure de test, l'approche de simulation utilisée peut avoir un impact sur la fiabilité qu'elle projettera [96, 97]. Trois catégories de simulation s'offrent à nous : simulation logicielle, simulation semi-physique et simulation physique [96]. Les approches de simulation possibles incluent soit chacune de ces simulations, soit une combinaison de plusieurs d'entre elles. En général, le choix des catégories sélectionnées sera fortement lié à l'objectif de fidélité fixé au départ et du budget disponible [92]. Plus les simulations impliquées dans une infrastructure de test seront physiques, plus sa fidélité sera généralement élevée [98].

Étant donné que nous avons choisi comme caractéristique critique le coût-efficacité, puis comme caractéristique secondaire la fidélité, notre objectif est que notre infrastructure soit la plus fidèle possible à la réalité, tout en respectant un certain budget. Pour optimiser la fidélité de notre infrastructure, elle devrait idéalement comprendre une portion de simulation complètement physique. Par contre, étant donné la quantité de ressources monétaires et physiques à notre disposition, il ne nous sera pas possible d'en faire autant. Ce que nous proposons de faire est une approche hybride, combinant des simulations logicielles avec une simulation semi-physique. Ainsi, nous pourrons augmenter la fidélité de notre infrastructure tout en gardant un coût de développement relativement bas.

3.4 Synthèse

En somme, nous avons choisi comme objectifs de conception pour notre infrastructure de test l'analyse de vulnérabilité, l'analyse et test d'attaques, l'éducation et entraînement ainsi que l'analyse et test de solutions de détection. Ces quatre objectifs de conception permettent de nous éclairer dans les multiples prises de décisions que nous rencontrerons tout au long de notre conception et nos expérimentations.

Ensuite, nous avons choisi comme caractéristiques critiques la fidélité, l'évolutivité, la flexibilité, la reproductibilité et la convivialité. Ces caractéristiques seront celles auxquelles nous accorderons le plus d'importance lors de nos prises de décision. En outre, nous avons choisi comme caractéristiques secondaires la modularité, le coût-efficacité, l'exécution sécuritaire, la diversité et la mesurabilité. Finalement, l'interopérabilité, la surveillance et journalisation, la complexité et l'ouverture sont des caractéristiques auxquelles nous n'accorderons pas d'importance particulière étant donné leur faible impact sur la crédibilité d'une infrastructure de test et sur nos objectifs choisis.

Pour poursuivre, nous avons choisi comme approches de simulation un hybride entre des simulations logicielles et une simulation semi-physique. Cette approche nous permettra d'augmenter la fidélité de notre infrastructure, par rapport à une approche purement logicielle [98].

CHAPITRE 4 MODÉLISATION DE L'INFRASTRUCTURE DE TEST

Dans ce chapitre, nous présentons la modélisation de notre infrastructure de test en trois étapes. Tout d'abord, nous présentons nos choix de conception. Ensuite, nous montrons la préparation de la modélisation d'attaques pour notre infrastructure. Finalement, nous présentons la modélisation de trois scénarios d'attaques.

4.1 Choix de conception de l'infrastructure de test

Dans cette section, nous présentons la modélisation de notre infrastructure de simulation en présentant les différents choix s'offrant à nous aux différentes couches de l'infrastructure. Tout d'abord, nous faisons le choix des systèmes à simuler. Ensuite, nous choisissons les données à générer au sein de ces systèmes. Pour continuer, nous choisissons les protocoles à simuler pour l'acheminement de ces données, puis nous présentons l'architecture.

4.1.1 Options de systèmes à inclure

L'éventail des systèmes maritimes est très large. Effectivement, nous avons d'abord le système de pont intégré (SPI), soit le principal système électronique d'un navire [99]. Ce système comprend un ensemble de différents systèmes informatiques permettant le bon fonctionnement du bâtiment. De plus, il permet la centralisation de ces différents systèmes en les reliant entre eux.

Parmi ceux-ci, on retrouve le système d'affichage numérique des cartes, soit le ECDIS. Ce système est utilisé par l'officier de navigation pour guider visuellement le trajet.

Comme on peut le voir sur la figure 4.1, l'ECDIS prend en entrée une multitude d'informations provenant de différents capteurs présents sur le navire. En outre, en fonction de ces informations, il émettra des commandes à différents autres systèmes, tel que le pilote automatique et le pilote de vitesse.

Ensuite, le GMDSS, utilisé à des fins d'envoi et réception de signaux de détresse, est également intégré au système de pont intégré [100]. Pour poursuivre, le système de pont intégré est aussi composé d'un système de radar. Ce système prend en entrée le cap et la position du navire, de même que le cap et la position des cibles en mouvement situées autour du navire. En plus d'aider visuellement l'officier de navigation à éviter les obstacles, il calcule également des données d'évitement de collision [101]. En outre, le système SPI intègre également le système VDR, soit l'enregistreur de données de voyage. Ce système, utilisé à des

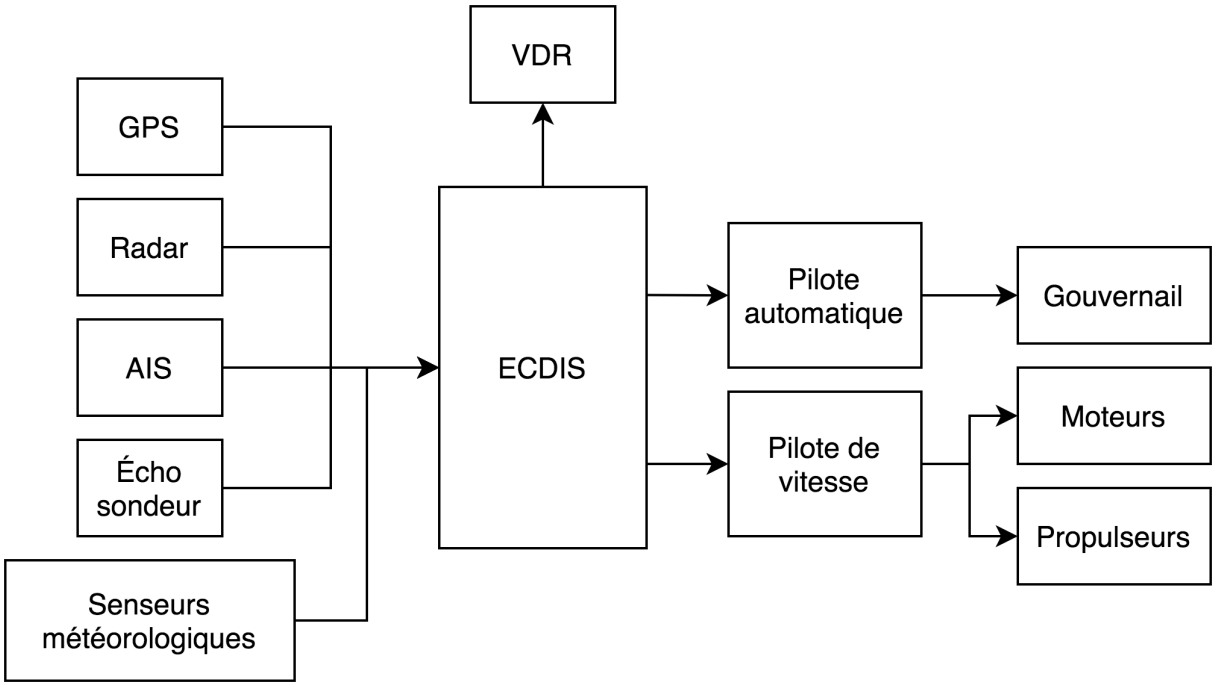

Figure 4.1 Relations entre l'ECDIS et les autres systèmes

fins d'investigation, prend en entrée une très grande quantité de données pour garder le plus de données possible, telles que les données GPS, les données de profondeur, ou encore des captures d'écran du ECDIS toutes les 15 secondes [102]. Un autre système présent au sein du système de pont intégré est le pilote automatique. Les systèmes modernes de pilote automatique sont synchronisés avec le système ECDIS pour ainsi avoir accès à un large éventail de données, tels que la position et la vitesse du navire [103].

Parmi les autres systèmes présents sur un navire, nous avons le système de communication satellitaire, soit le VSAT. Ce système permet plusieurs applications très utiles au navire, tel que de donner une connexion internet aux passagers [104]. En outre, un autre système présent sur un navire est le positionnement dynamique (PD). Ce système exerce un contrôle sur les propulseurs et les hélices et permet au navire de rester sur place. Pour effectuer les calculs nécessaires au maintien du navire en place, le positionnement dynamique se sert de l'information générée par différents capteurs [105]. Finalement, nous avons à bord d'un navire le *Integrated Platform Management System* (IPMS), permettant le contrôle et la surveillance en temps réel de différents systèmes présents sur le navire. Parmi ces systèmes, on retrouve le système de propulsion, les moteurs, les hélices, le système de gestion de l'alimentation, le système de contrôle des dommages et le système d'alarme [106].

4.1.2 Choix des systèmes à inclure

En raison du nombre très élevé de systèmes présents sur un navire ainsi que de leur complexité respective, il ne serait pas réaliste d'avoir comme objectif de les inclure dans leur totalité. Conséquemment, nous devons faire des choix en nous basant sur nos objectifs de conception ainsi que nos caractéristiques critiques et secondaires établis au chapitre 4 pour la mise en place de notre infrastructure, comme illustré au tableau 3.2.

Nos quatre objectifs de conception sont l'analyse de vulnérabilité, l'analyse et test d'attaques, l'éducation et entraînement ainsi que l'analyse et test de solutions de détection. Après avoir établi ces quatre objectifs, nous avons ensuite classé en trois catégories les 14 caractéristiques qui influent généralement sur la crédibilité d'une infrastructure de test. La première catégorie, soit les caractéristiques critiques, comprend la fidélité, l'évolutivité, la flexibilité, la reproductibilité et la convivialité. La seconde, soit les caractéristiques secondaires, comprend la modularité, le coût-efficacité, l'exécution sécuritaire, la diversité et la mesurabilité. En somme, notre infrastructure devra impérativement refléter le plus possible la réalité, assurer une évolution avec l'ajout de nouvelles configurations et fonctionnalités, assurer une flexibilité en adaptant et redéfinissant son utilisation, assurer la reproductibilité de ses résultats et avoir une interface utilisateur la plus conviviale possible. En second plan, notre infrastructure devra être capable de s'adapter aux nouvelles exigences, avoir des processus de test quantifiables, avoir un bon rapport coût/qualité, mener des simulations sans avoir d'impact sur le monde réel et inclure une grande variété de composantes, sans pour autant affecter l'évolutivité de la plateforme.

Dans le cadre du choix des systèmes à intégrer dans notre infrastructure, on constate que ce choix aura un impact direct sur certaines de ces caractéristiques, soit au premier plan l'évolutivité et la flexibilité, puis au second plan la modularité, le coût-efficacité et la diversité. Pour assurer l'évolutivité de notre infrastructure, nous ne devons pas trop diversifier nos simulations dès le début, mais plutôt d'abord simuler un élément central largement utilisé sur les navires dont l'utilisation dépend d'une multitude d'autres systèmes. Ce faisant, la configuration et les fonctionnalités de l'infrastructure pourront être élargies au fil du temps. Ensuite, pour assurer la flexibilité de l'infrastructure, nous devons simuler un système pour lequel il sera facile de redéfinir et réadapter la configuration pour différents scénarios. Finalement, en tenant compte des caractéristiques secondaires, le système simulé devra être un système dont la simulation pourra facilement s'adapter aux nouvelles exigences, être raisonnablement coûteuse et permettre l'ajout d'une multitude d'autres systèmes.

Selon notre partenaire industriel ainsi que ses experts en conception de navires, l'ECDIS est le système le plus sensible d'un navire, notamment en raison de sa forte liaison avec divers autres systèmes du navire, et le fait qu'il s'agit du seul système roulant sur un système d'exploitation standard pour lequel des cyberattaques sont très envisageables.

En analysant ces exigences, nous choisissons d'inclure comme système central le système d'affichage électronique des cartes, soit le ECDIS. Effectivement, ce système est un élément central du système informatique d'un navire et permet d'afficher les cartes, mais aussi l'information recueillie par différents capteurs présents sur un navire, tels que les données GPS et la vitesse du vent pour ne nommer que celles-ci. L'utilisation du ECDIS permettra une évolutivité pour l'infrastructure en permettant l'ajout au fil du temps de différents autres systèmes et capteurs. De plus, elle permettra une bonne flexibilité pour l'infrastructure, dans la mesure où l'ECDIS prend en entrée une multitude de paramètres, il sera donc très facile de redéfinir sa configuration et son utilisation pour l'adapter à différents scénarios. En outre, le ECDIS pourra facilement s'adapter aux nouvelles exigences, en adoptant par exemple de nouveaux protocoles, ne sera pas trop coûteux à implanter et nous permettra de diversifier notre infrastructure en simulant une multitude d'autres données et systèmes. Pour continuer, étant donné que le système ECDIS a été rendu obligatoire par l'IMO pour tous les navires commerciaux [29], notre choix du ECDIS comme élément central de notre infrastructure la rendra plus polyvalente, ce système étant présent sur une bonne partie des navires. L'objectif d'entraînement et d'éducation de la communauté maritime sera touché positivement par cette polyvalence, qui élargira notre bassin de professionnels à potentiellement éduquer et entraîner via notre plateforme. Finalement, l'ECDIS roule sur de vieux systèmes d'exploitation hautement vulnérables à des cyberattaques et sa procédure de mise à jour s'effectue sans soucis de cybersécurité, comme expliqué dans la sous-section 2.2.3. Conséquemment, les vulnérabilités du ECDIS permettront à notre infrastructure d'inclure une grande variété de cyberattaques, ainsi que diverses solutions de détection d'anomalies.

4.1.3 Données à générer

Étant donné que l'ECDIS est uniquement un système d'affichage, nous devons générer nos données séparément et les envoyer au ECDIS pour qu'il les affiche. Pour ce faire, nous devons d'abord déterminer les données que nous voulons générer. Les navires comportent de multiples capteurs générant des données utilisées pour la navigation, dont la plupart seront acheminées au ECDIS :

GNSS Le GNSS va générer des données GPS qui seront utilisées pour afficher la position du navire sur la carte [107].

AIS L'AIS envoie et reçoit des messages en diffusion contenant diverses informations sur lse navires, tel que son numéro d'identification et sa position [108].

Écho sondeur L'écho sondeur va mesurer la profondeur de l'eau et mesurer la distance des obstacles sous l'eau [109].

Compas Le compas donne le cap du navire [110].

Loch Le loch mesure la vitesse relative du navire par rapport à l'eau [111].

Anémomètre L'anémomètre est un appareil utilisé pour mesurer la vitesse et la direction du vent [112].

En se remémorant des caractéristiques choisies pour notre infrastructure de test, on constate que le choix des données à générer influencera principalement la fidélité et la diversité de notre infrastructure. En effet, la quantité de données générées aura un impact direct sur la fidélité du système, car plus l'ECDIS recevra les données comparables à celles d'un vrai navire, plus l'infrastructure reflétera la réalité. Du côté de la diversité, en envoyant le plus de données différentes possible vers l'ECDIS, on augmente la diversité de notre infrastructure tout en conservant son évolutivité, étant donné que le système ECDIS permet facilement d'ajouter et d'enlever des éléments sans avoir à changer l'architecture. Conséquemment, notre objectif sera de simuler le plus de données différentes possible et les envoyer vers l'ECDIS.

4.1.4 Protocoles à simuler

Les données que nous voulons générer, à l'exception d'AIS, utilisent pour leur transmission le protocole *National Marine Electronics Association* (NMEA). Plus précisément, elles utilisent les normes NMEA-0183 ou NMEA-2000. La différence fondamentale entre ces deux normes est l'architecture de communication : NMEA-0183 admet un émetteur et plusieurs récepteurs, et NMEA-2000 permet plusieurs émetteurs et plusieurs récepteurs. De ce fait, NMEA-2000 rend une architecture complexe beaucoup plus facile à mettre en place, avec beaucoup moins de filage impliqué. Cependant, comme chaque élément est connecté individuellement, la norme NMEA-0183 rend la tâche plus facile lorsque vient le temps de trouver un élément qui fait défaut en l'isolant [113].

Pour ce qui est de cette infrastructure de test, toutes les données que nous voulons peuvent être générées avec les deux protocoles. Comme les navires utilisent encore à profusion les deux normes, nous allons utiliser la plus ancienne, soit NMEA-0183. Aucune des deux normes n'a d'impact significatif sur les caractéristiques et objectifs choisis pour la conception de notre infrastructure de test. De plus, dans une perspective d'évolutivité, il nous serait possible d'inclure la norme NMEA-2000 sans faire de modification importante à l'architecture.

4.1.5 Architecture de l'infrastructure de simulation

En somme, nous avons choisi de considérer comme système principal le système d'affichage électronique des cartes, soit le ECDIS. Tel que l'illustre la figure 4.1, ce système est un élément central du poste de pilotage d'un navire, il nécessite donc en entrée une multitude de données. Pour ce faire, nous avons choisi de générer le plus de données différentes possible dans le but de refléter la réalité au meilleur de nos capacités. Ces données comprennent entre autres des données GPS, AIS, et de profondeur. La figure 4.2 montre le sommaire de l'architecture de notre infrastructure de test.

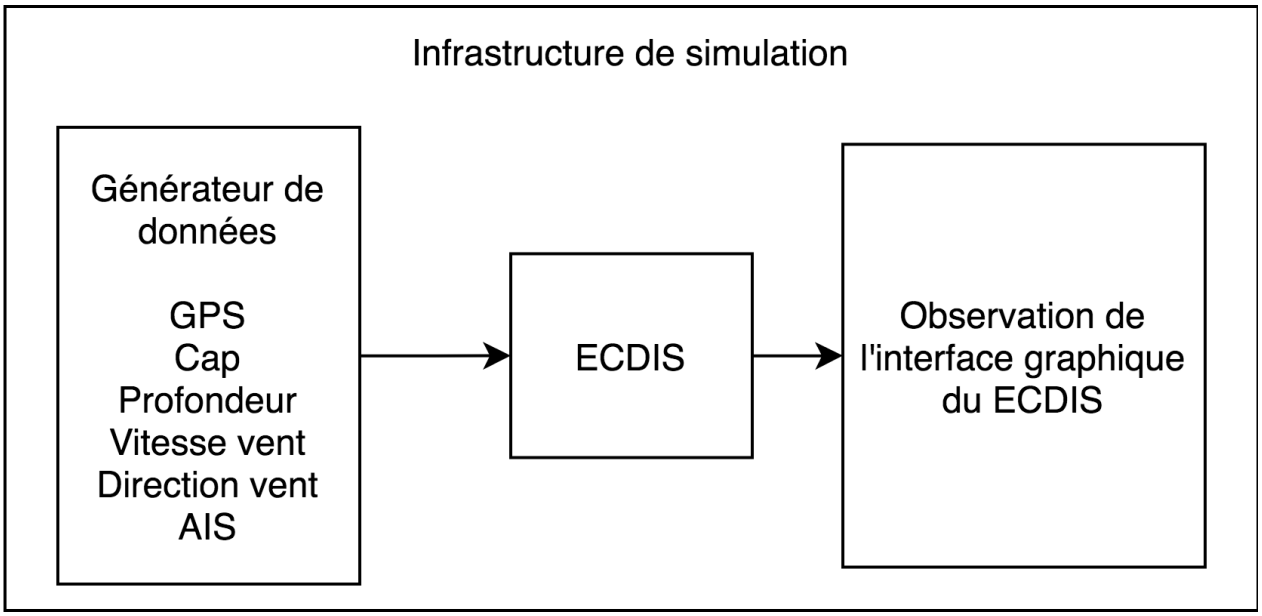

Figure 4.2 Architecture de l'infrastructure de simulation

4.2 Préparation de la modélisation d'attaques

La prochaine étape dans la mise en place de l'infrastructure de simulation est de déployer des attaques réalistes au sein de cette infrastructure. Pour ce faire, nous devons d'abord identifier les vulnérabilités des systèmes, puis des protocoles choisis, identifier les motivations de l'attaquant, identifier la victime ciblée, puis définir la chaîne de frappe avec laquelle nous modéliserons nos attaques. En outre, nous posons nos hypothèses de contexte et décrivons notre environnement de travail.

4.2.1 Vulnérabilités des systèmes et protocoles choisis

Comme relaté dans la revue de littérature, l'ECDIS comporte de nombreuses failles de sécurité, notamment en raison du fait que les logiciels d'ECDIS roulent souvent sur des ordinateurs datés dont les systèmes n'ont plus de mises à jour sécuritaires [29]. En effet, en 2014, CyberKeel a réussi à exploiter des vulnérabilités de Windows 7 pour modifier et supprimer des données d'un logiciel ECDIS [34]. En outre, une attaque visant la modification des cartes a été démontrée en 2014 [35]. Or, étant donné que les cartes sont chargées dans le ECDIS sans préoccupation de sécurité, c'est-à-dire par USB ou internet, le chargement des cartes est une vulnérabilité importante de l'ECDIS [29]. En outre, des cas de mauvaise configuration ou utilisation de l'ECDIS ont mené à des échouements de navire [38–40].

Ensuite, comme mentionné précédemment, le protocole choisi pour la transmission de données vers le simulateur d'ECDIS sera du NMEA-0183, et sera transmis sur une connexion série. Dans le chapitre 2, nous avons vu que le protocole NMEA-0183 est vulnérable à plusieurs types d'attaques. Tout d'abord, des attaques par déni de service, étant donné son taux de transmission relativement faible [53]. Ensuite, NMEA-0183 ne comporte aucun processus de chiffrement ou d'authentification, NMEA-0183 est donc très vulnérable à des attaques de reniflage et d'usurpation de paquets [53]. Finalement, des attaques par l'homme du milieu sont possibles contre NMEA-0183 [55].

4.2.2 Motivation de l'attaquant et victime ciblée

Dans le chapitre 1, nous avons identifié quatre types différents de motifs d'attaque sur des systèmes maritimes : le vol de données sensibles, vol monétaire, déplacement illégal de cargaison et la cause de perturbations ou de pertes. Dans le cadre de nos travaux, nous nous sommes intéressés au motif de causer des perturbations ou des pertes, sans nécessairement en tirer un profit personnel. Conséquemment, le profil de l'attaquant sera un individu voulant perturber l'équipage d'un navire, causer des pertes monétaires à son propriétaire et mettre en danger les vies de l'équipage.

Ensuite, dans le chapitre 1, nous avons explicité les différentes entités regroupées dans le concept de systèmes maritimes, soit les organisations et compagnies maritimes, les ports et navires et autres bâtiments naviguant sur ou sous l'eau. Pour pouvoir nous concentrer sur des scénarios précis, nous ciblons dans nos travaux les navires.

La ou les victimes collatérales des cyberattaques que nous modélisons seront un navire, son équipage et le propriétaire du navire, étant une compagnie ou un individu, nos cyberattaques ont donc des impacts directs ou indirects sur ces victimes.

Pour la cible directe des attaques, c'est-à-dire la victime que nous ciblerons précisément pour mener à bien notre attaque, il s'agit de l'officier de navigation du navire. En effet, c'est cet individu qui sera responsable de la navigation du navire et son facteur humain aura de gros impacts sur le bon déroulement des attaques.

4.2.3 Hypothèses et environnement de travail

Pour infiltrer le système du ECDIS sur un navire, nous utilisons comme moment opportun la mise à jour des cartes, qui s'effectue régulièrement et dont les procédures ne comportent pas beaucoup de protection [29].

L'ordinateur sur lequel roule le logiciel d'ECDIS est rarement connecté à internet. Pour mettre à jour les cartes du ECDIS, deux options se présentent. D'une part, l'officier de navigation doit utiliser un second ordinateur portable pour y télécharger les cartes, dont le lien de téléchargement lui sera acheminé par courriel. D'autre part, l'officier de navigation peut recevoir la mise à jour des cartes directement sur une clé USB. La figure 4.3 présente l'architecture de notre environnement de travail.

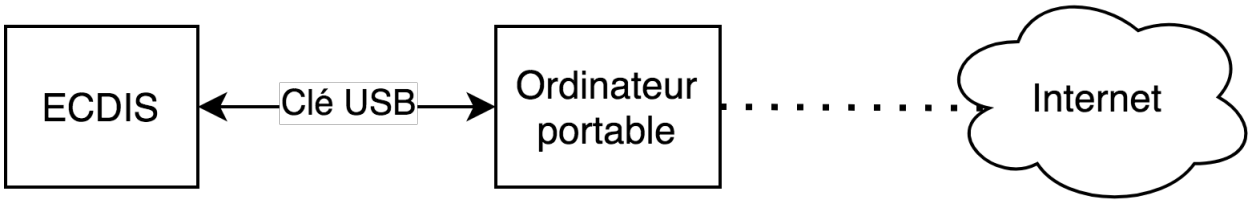

Figure 4.3 Architecture de l'environnement de travail

Comme on peut le voir, nous assumons que seul l'ordinateur portable aura une connexion internet. De plus, selon les deux scénarios de mise à jour de cartes, nous observons deux failles potentielles : la réception d'un courriel duquel on télécharge un fichier, puis l'utilisation d'une clé USB. Par conséquent, ces deux méthodes de mise à jour des cartes seront prises en compte dans nos scénarios d'attaque.

4.3 Modélisation de trois scénarios d'attaques

La présente section présentera une gradation de trois différents scénarios d'attaques. Pour modéliser les scénarios, nous utiliserons la chaîne de frappe de Lockheed Martin pour un réseau, décrite à la sous-section A.4.1. Pour débuter, nous allons définir la chaîne de frappe commune aux trois scénarios, soit les étapes 1 à 6. Par la suite, nous décrirons en détail l'étape 7 de chacun des scénarios.

4.3.1 Chaîne de frappe commune aux trois scénarios

Les trois scénarios que nous présenterons aurons en commun les 6 premières étapes dans leur chaîne de frappe. Par conséquent, nous allons décrire ici ces 6 premières étapes, puis préciser la septième pour chacun des scénarios, soit l'étape «Actions sur l'objectif».

1. Reconnaissance : Déterminer quel navire attaquer, déterminer l'identité de l'officier de navigation de ce navire, obtenir son adresse courriel, trouver une occasion de le rencontrer en présentiel lors d'un évènement professionnel.
2. Armement : Création d'un fichier malveillant camouflé dans un fichier *Portable Document Format* (PDF), puis création en parallèle d'une clé USB infectée.
3. Livraison : Envoi d'un courriel à l'officier de navigation pour la mise à jour des cartes de l'ECDIS contenant le lien de téléchargement de la mise à jour et un fichier PDF infecté de consignes d'installation, ouverture du fichier par l'officier sur l'ordinateur portable. D'un autre côté, remise de la clé USB infectée à l'officier de navigation lors d'un évènement de réseautage sans éveiller les soupçons. Dans l'éventualité où l'officier n'a pas ouvert le fichier infecté, on présume qu'il utilisera éventuellement la clé USB infectée remise lors de l'évènement.
4. Exploitation : Prise de contrôle de l'ordinateur portable par le fichier malveillant, puis la mise en place de fichiers malveillants sur la clé USB non infectée insérée par l'officier dans l'ordinateur portable. Si l'officier n'a pas ouvert le fichier, la clé USB infectée contiendra déjà les fichiers malveillants. Une fois la clé insérée dans l'ordinateur du ECDIS, les fichiers malveillants qu'elle contient installeront les fichiers nécessaires pour mener l'attaque.
5. Installation : Comme on présume que l'ECDIS n'est pas connecté à internet, une installation en vue d'une prise de contrôle à distance ne sera pas possible.
6. Commandement et contrôle : Comme on présume que l'ECDIS n'est pas connecté à internet, une prise de contrôle à distance ne sera pas possible.

Les scénarios que nous modélisons pour l'étape «Actions sur objectifs» sont une gradation d'attaques dont les impacts sont de plus en plus critiques. Tout d'abord, nous considérons une attaque gros grain de type déni de service, dont le but est de rendre l'ECDIS inutilisable et de faire perdre la confiance de l'équipage envers l'ECDIS et le faire rentrer au port. Ensuite, nous avons une attaque un peu plus sophistiquée, faisant de l'usurpation de paquet et des attaques par l'homme du milieu sur les données envoyées à l'ECDIS. Ce faisant, le but est également de faire perdre la confiance de l'équipage envers l'ECDIS et le faire rentrer au port. Finalement, nous aurons une attaque par l'homme du milieu à travers laquelle nous modifions

les données envoyées à l'ECDIS de façon intelligente, c'est-à-dire plusieurs données modifiées à la fois en consistance les unes par rapport aux autres, dans le but de faire prendre des décisions au pilote automatique qui auront des conséquences physiques critiques sur le navire, son échouement par exemple. Pour chacune des modélisations d'attaque, nous décrivons en détail le modèle de l'attaquant et de la victime. Pour l'attaquant, nous utilisons comme critères la motivation, la capacité et l'opportunité. Ces trois critères permettent d'estimer la probabilité qu'une cyberattaque survienne. Ensuite, nous posons nos hypothèses d'attaque, et nous finissons par décrire l'étape sept de la chaîne de frappe, soit «Actions sur objectifs».

4.3.2 Scénario 1 : Attaque par déni de service sur l'ECDIS

Le but de ce scénario est de rendre le logiciel ECDIS inutilisable avec une attaque de déni de service, et ainsi faire perdre la confiance qu'a l'officier de navigation envers l'ECDIS. Incidemment, le navire pourrait devoir retourner au port jusqu'à ce que le problème soit réglé. Les impacts qu'une telle attaque occasionnerait sont des pertes de temps pour l'équipage, et donc incidemment des pertes monétaires pour la compagnie ayant à amarrer son navire le temps de régler le problème, puis des délais potentiels de livraison dans le cas d'un navire marchand. En outre, dépendamment de l'emplacement du navire, une telle attaque pourrait avoir des impacts critiques sur le navire et son équipage, par exemple dans une éventualité où le navire est dans une région dans laquelle il est difficile de se rendre au port sans ECDIS.

Pour ce scénario, l'attaquant aura comme motivation de mener une attaque par déni de service sur l'ECDIS d'un navire, faire perdre la confiance de l'officier de navigation envers l'ECDIS et faire retourner le navire au port. Pour avoir une telle motivation, l'attaquant pourrait être par exemple à la solde d'une compagnie maritime voulant saboter la compétition, ou encore un hacktiviste voulant causer des dommages monétaires à une compagnie ne suivant pas ses valeurs. Ensuite, pour mener cette attaque, l'attaquant a besoin de compétences et connaissances modérées en piratage. Finalement, pour mener l'attaque, l'attaquant doit avoir comme opportunité de connaître l'identité et l'adresse courriel de l'officier de navigation, puis avoir une occasion de le rencontrer en présentiel et de lui remettre une clé USB. La cible de l'attaque est l'officier de navigation d'un navire. Celui-ci est le marin entre autres responsable de surveiller l'ECDIS pendant la durée du trajet naval.

Le bon fonctionnement de cette attaque dépend de quelques conditions en lien avec le facteur humain. Pour nos travaux, nous posons quelques hypothèses assurant ces conditions. Tout d'abord, pour que l'attaque réussisse, l'officier de navigation doit ouvrir le fichier infecté transmis par courriel, ou encore utiliser la clé USB infectée remise en mains propres pour les transférer les fichiers de cartes vers l'ECDIS. Conséquemment, on postule que l'officier ouvrira

le fichier sur l'ordinateur portable ou utilisera la clé infectée. En outre, dépendamment de l'architecture du navire, celui-ci peut avoir un second système ECDIS utilisé comme outil de vérification. Par conséquemment, nous posons l'hypothèse que les modifications effectuées au sein de l'ECDIS principal le seraient également pour le second ECDIS.

Actions sur objectifs Une fois le navire ayant quitté le port, nous allons lancer notre attaque par déni de service sur le ECDIS. Pour ce faire, notre logiciel changera le mot de passe de l'ordinateur, puis le redémarrera, le rendant ainsi inutilisable. L'officier de navigation ne pouvant plus utiliser le système ECDIS, il conduira le navire au port pour corriger la situation. Pour y retourner sans ECDIS, l'officier de navigation pourra se servir de cartes papier, ou encore y aller à tâtons en se servant du radar.

4.3.3 Scénario 2 : Attaques par usurpation de paquets et par l'homme du milieu sur l'ECDIS

Le but avec cette attaque sera de modifier les données envoyées vers l'ECDIS, ou encore en injecter, toujours dans le but de faire perdre la confiance de l'officier de navigation envers le ECDIS. Comme dans le cas de l'attaque précédente, les impacts seraient des pertes de temps, pertes monétaires et des délais de livraison potentiels.

Pour ce scénario, l'attaquant a la même motivation, capacité et opportunité que pour le scénario 1. De plus, la victime ciblée est la même, soit l'officier de navigation. En outre, les hypothèses d'attaque pour ce scénario sont les mêmes que celles pour le scénario 1, en plus de l'hypothèse suivante. L'attaque nécessite un redémarrage de l'ordinateur pour effectuer les installations nécessaires. Par conséquent, nous posons l'hypothèse que l'officier de navigation considérera cette étape comme normale et ne sera pas alarmé.

Actions sur objectifs Une fois le navire ayant quitté le port, l'attaque va débuter en modifiant les phrases GPS envoyées des capteurs vers le ECDIS, puis en envoyant des phrases GPS aléatoires. En constatant que les données GPS affichées sur l'ECDIS ne sont pas compatibles avec la réalité, l'officier de navigation verra sa confiance au ECDIS diminuer et retournera au port dans le but de le faire réparer. Par exemple, la figure 4.4 illustre une injection de phrases GPS NMEA-0183 localisées au milieu de l'Afrique. Pour un navire faisant route de Québec à Halifax, il ne prendra pas de temps à l'officier de navigation pour perdre confiance en l'ECDIS.

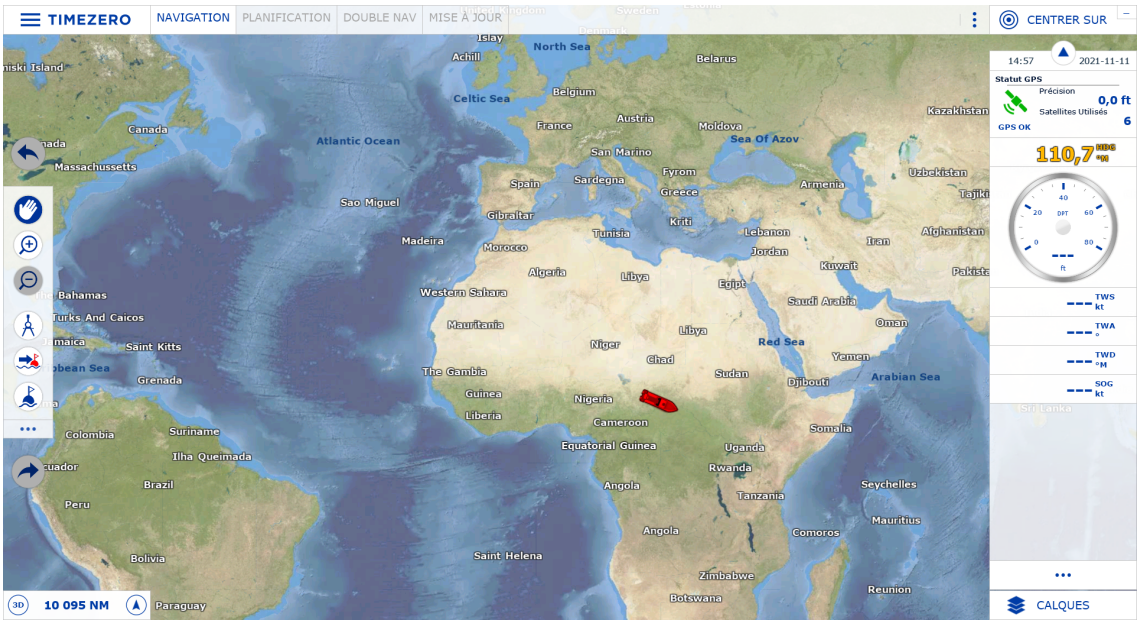

Figure 4.4 Injection de phrases GPS NMEA-0183 localisées au milieu de l'Afrique

4.3.4 Scénario 3 : Attaque sophistiquée sur l'ECDIS

Finalement, nous modélisons une attaque plus sophistiquée par l'homme du milieu sur l'ECDIS. Par sophistication, nous entendons prendre en compte un plus grand éventail de données et les modifier de façon plus subtile et graduelle. Ce faisant, l'attaque sophistiquée induit le pilote automatique et l'officier de navigation en erreur et leur fait prendre des décisions ayant un impact réel sur le réseau TO du navire, plus précisément le gouvernail. Effectivement, dans un passage étroit, l'attaque fera croire au ECDIS, et donc au pilote automatique, que le navire s'enligne vers la côte supérieure du passage, le pilote automatique corrigera donc l'orientation du gouvernail pour rester au milieu du passage. Or, comme le navire n'avait changé de trajectoire qu'en apparence, le navire se dirigera alors vers la côte inférieure du passage, risquant ainsi une collision. Une telle attaque peut avoir des impacts beaucoup plus critiques, tels que des dommages physiques au navire, ou encore à l'équipage. En outre, une telle attaque peut également occasionner des pertes de temps et des pertes monétaires pour la compagnie maritime et l'équipage.

Pour ce scénario, l'attaquant a la même opportunité que pour les deux autres scénarios. L'attaquant a comme motivation de causer des dommages physiques à un navire et son équipage. Quant à sa capacité, en plus d'avoir des compétences et connaissances modérées en piratage, il doit également avoir des compétences et connaissances maritimes modérées. En

effet, des notions de navigation et une maîtrise des données produites par les capteurs d'un navire sont nécessaires à la mise en place de cette attaque. Ensuite, la victime ciblée sera la même que pour les autres scénarios, soit l'officier de navigation.

Pour ce scénario, nous posons les mêmes hypothèses que pour le second scénario. De plus, le bon fonctionnement de cette attaque dépend du fait que l'officier de navigation et les autres marins à bord ne constatent pas la divergence entre la position affichée et la position réelle du navire. Pour ce faire, nous devons poser l'hypothèse selon laquelle les repères visuels de l'équipage sont affaiblis, comme ils le sont la nuit ou dans une tempête. En outre, pour que cette attaque fonctionne, le navire doit être contrôlé par le pilote automatique au moment où elle est menée. Conséquemment, nous posons l'hypothèse que le pilote automatique est enclenché dans le chenal étroit et qu'aucune navigation manuelle n'est utilisée, l'officier de navigation est donc présent pour surveiller le bon déroulement du voyage.

Actions sur objectifs Une fois que le navire a quitté le port, nous allons attendre qu'il se retrouve dans un passage étroit. Une fois dans le passage, nous allons modifier la position GPS reçue par le ECDIS pour que celui-ci semble se diriger vers une des côtes du chenal. Pour que l'attaque soit réaliste et passe inaperçue de l'officier, nous allons également modifier, en accord avec la position, le cap navire et la profondeur de l'eau. Par exemple, si nous changeons la latitude du navire, le cap doit changer également pour rester congruent. De plus, si nous rapprochons le navire de la rive, la profondeur devra diminuer à mesure qu'il s'approche de la rive pour refléter la réalité. Ainsi, à mesure que le navire se dirige vers la côte supérieure du chenal, le pilote automatique tentera de corriger le tir en ajustant la position du gouvernail, orientant ainsi le navire vers la côte inférieure. En supposant que l'officier de navigation ne détecte pas l'attaque assez tôt, le navire entrera en collision avec la côte inférieure du chenal.

4.3.5 Synthèse

Dans la présente section, nous avons modélisé trois scénarios d'attaques. Le tableau 4.1 fait la synthèse, pour chacun des scénarios d'attaques modélisés, de la victime, de la motivation de l'attaquant, de la capacité de l'attaquant, de l'opportunité de l'attaquant, des hypothèses et des impacts.

Tableau 4.1 Synthèse de la modélisation de trois scénarios d'attaques

	Scénario 1 : Déni de service	**Scénario 2 : Usurpation de paquets et homme du milieu**	**Scénario 3 : Attaque sophistiquée**
Victime	Officier de navigation	Officier de navigation	Officier de navigation
Motivation de l'attaquant	Perte de confiance envers l'ECDIS	Perte de confiance envers l'ECDIS	Causer des dommages critiques au navire/équipage
Capacité de l'attaquant	Compétences/connaissances de piratage modérées	Compétences/connaissances de piratage modérées	Compétences/connaissances de piratage modérées Compétences/connaissances maritimes modérées
Opportunité de l'attaquant	Connaître l'identité et l'adresse courriel de la victime Occasion de rencontre physique avec la victime	Connaître l'identité et l'adresse courriel de la victime Occasion de rencontre physique avec la victime	Connaître l'identité et l'adresse courriel de la victime Occasion de rencontre physique avec la victime
Hypothèses	Victime ouvre le fichier PDF infecté Déni de service également sur le second ECDIS	Victime ouvre le fichier PDF infecté Déni de service également sur le second ECDIS Victime ne soupçonne pas le redémarrage de l'ECDIS	Victime ouvre le fichier PDF infecté Déni de service également sur le second ECDIS Victime ne soupçonne pas le redémarrage de l'ECDIS Repères visuels afflaiblis Aucune navigation manuelle
Impacts	Perte de temps, pertes monétaires	Perte de temps, pertes monétaires	Dommages critiques au navire ou à l'équipage Perte de temps, pertes monétaires

CHAPITRE 5 EXPÉRIMENTATION ET RÉSULTATS

Dans ce chapitre, nous débutons en présentation les étapes expérimentales de la mise en place de l'infrastructure de test. Ensuite, nous présentons la mise en place des six premières étapes de la chaîne de frappe des attaques. Pour poursuivre, nous présentons la mise en place de l'étape sept pour chacun des scénarios d'attaque. Finalement, nous présentons nos résultats et notre analyse de la mise en place de l'infrastructure de test et des attaques.

5.1 Mise en place de l'infrastructure de test

Dans le cadre de la mise en place de l'infrastructure de test, nous faisons plusieurs choix d'implémentation, en nous basant sur les caractéristiques considérées pour la conception de notre infrastructure et sur nos objectifs de conception. Dans cette section, nous présentons notre cheminement pour les choix d'environnement, de générateur de données, de la communication de données, puis de logiciel d'ECDIS. Nous finissons avec un portrait de l'implémentation de l'infrastructure de test.

5.1.1 Choix de l'environnement d'implémentation

La première question à se poser a été de déterminer dans quel environnement doit être implémentée notre infrastructure de test. Tout d'abord, la plupart des navires opèrent leur ECDIS sur une architecture Windows 7, et une bonne partie des vulnérabilités du ECDIS proviennent de l'utilisation de ce système d'exploitation [34]. Conséquemment, nous avons choisi d'implémenter notre infrastructure de test dans un environnement Windows 7. Quant à l'environnement de travail, pour la plupart de la durée de développement, nous avons utilisé des machines virtuelles pour leur malléabilité et la possibilité d'exécution sécuritaire. Par la suite, nous sommes passés à une vraie machine sur laquelle nous avons installé Windows 7.

5.1.2 Étude comparative des générateurs de données

Pour la génération de données, deux choix s'offraient à nous : générer nous-mêmes les données, ou utiliser un logiciel qui les génère pour nous. L'avantage de les générer nous-mêmes est que nous pouvons automatiser la génération et l'envoi de données, et nous pouvons complètement contrôler la synthèse des phrases à générer, tel que nous le montrons dans la présente sous-

section. Cependant, l'utilisation d'un logiciel générant les données pour nous va élargir les paramètres possibles et ainsi augmenter la précision et le contrôle que nous avons sur ces paramètres.

Quatre logiciels de génération de données NMEA-0183 ont été comparés. Pour cette comparaison, nous considérons le prix, les instruments NMEA-0183 simulés, les formats NMEA-0183 pour chacun de ces instruments, les types de messages AIS et les sorties possibles du logiciel. Le tableau 5.1 illustre l'étude comparative menée pour ces quatre logiciels.

Tableau 5.1 Comparaison de logiciels générateurs de données NMEA-0183

Produit	Manu	Prix	Instruments NMEA-0183	Formats NMEA-0183	Messages AIS	Sorties
NemaStudio	Sailsoft	406 CAD	GPS Cap Vitesse Écho sondeur Anémomètre Radar Transducteur Attitude Personnalisé Gestion d'alertes du pont	GLL, RMC, VTG, ZDA, GGA, GSA, GSV, XTE, RMB, DTM HDG, HDT, HDM, THS, ROT, RSA VHW, VLW, VBW DBT, DPT, DBK, DBS MWD, MWV, VWR, VWT, MTW TLL, TTM, OSD XDR	Class A vessels Base stations Aids to Navigation Class B vessels SAR aircrafts	Port série UDP/IP
ZNS-890	Zinnos	2000 USD	GPS Cap Vitesse Écho sondeur Anémomètre Radar	GGA, GNS, GLL, RMC, VTG, GSA, GSV, GST, DTM, ZDA THS, HDT, ROT PRATT, PRDID VHW, VBW, VDR DBT, DPT MVW TTM, TTD, TLB	Class A vessels Base stations Aids to Navigation Class B vessels SAR aircrafts Rdm ctrl of AIS object	Port série TCP/IP UDP/IP Voltage
GPS Simulator	NMEAsoft	147 USD	GPS Cap	GGA, GNS, GLL, RMC, VTG, ZDA, GSA, GSV, DTM HDT		Port série UDP/IP
Rdm NMEA Generator		Gratuit	GPS	RMC, GGA, GLL, FSA, GSV, VTG, ZDA		

Comme le montre le tableau 5.1, les deux premiers logiciels sont en mesure de générer une grande variété de données NMEA-0183. Le tableau 5.2 permet de comparer les différents instruments NMEA-0183 simulés pour chacun des logiciels, en excluant les instruments qui ne sont pas d'intérêt à notre infrastructure.

Tableau 5.2 Comparaison des instruments NMEA-0183 simulés pour chacun des logiciels

Produit	GPS	Cap	Vitesse	Sondeur	Vent	Radar	Transducteur	Attitude	Perso.	Alertes pont
NemaStudio										
ZNS-890										
GPS Simulator										
Random NMEA Simulator										

Comme on peut le voir dans le tableau 5.2, le logiciel NEMAStudio peut simuler toutes données qui nous intéressent. En outre, le logiciel ZNS-890 permet tout de même de simuler les données principales, telles que les données GPS, de cap, de vitesse, d'écho sondeur et de vent. Un autre facteur à considérer est la variété des formats NMEA-0183 pour chacun des instruments simulés, particulièrement pour les données GPS. Effectivement, dépendamment du type de format utilisé, les phrases GPS transmettent différentes informations, et ces phrases sont souvent utilisées simultanément sur un navire. Le tableau 5.3 compare les différents formats de phrases GPS NMEA-0183 pour chacun des logiciels.

Tableau 5.3 Comparaison des formats de phrases GPS NMEA-0183 pour chacun des logiciels

	GPS												
Produit	GGA	GNS	GLL	RMC	VTG	GSA	GSV	GST	DTM	ZDA	XTE	RMB	FSA
NemaStudio													
ZNS-890													
GPS Simulator													
Random NMEA Simulator													

Comme le montre le tableau 5.3, tous les logiciels permettent de générer une grande variété de formats de phrases GPS NMEA-0183.

Le choix sur lequel nous nous sommes arrêtés est le logiciel NEMAStudio, développé par Sailsoft. Ce logiciel permet de générer un large éventail de données, soit des données GPS, de cap, de vitesse, d'écho sondeur, de vent, et autres. De plus, son prix de 406 CAD le rend accessible. En outre, le logiciel avait une version d'essai avec comme seule limite un nombre de phrases générées par séance, que nous avons utilisée pour la durée de ce projet. La figure 5.1 montre la génération de données GPS de format RMC sur le port série COM3.

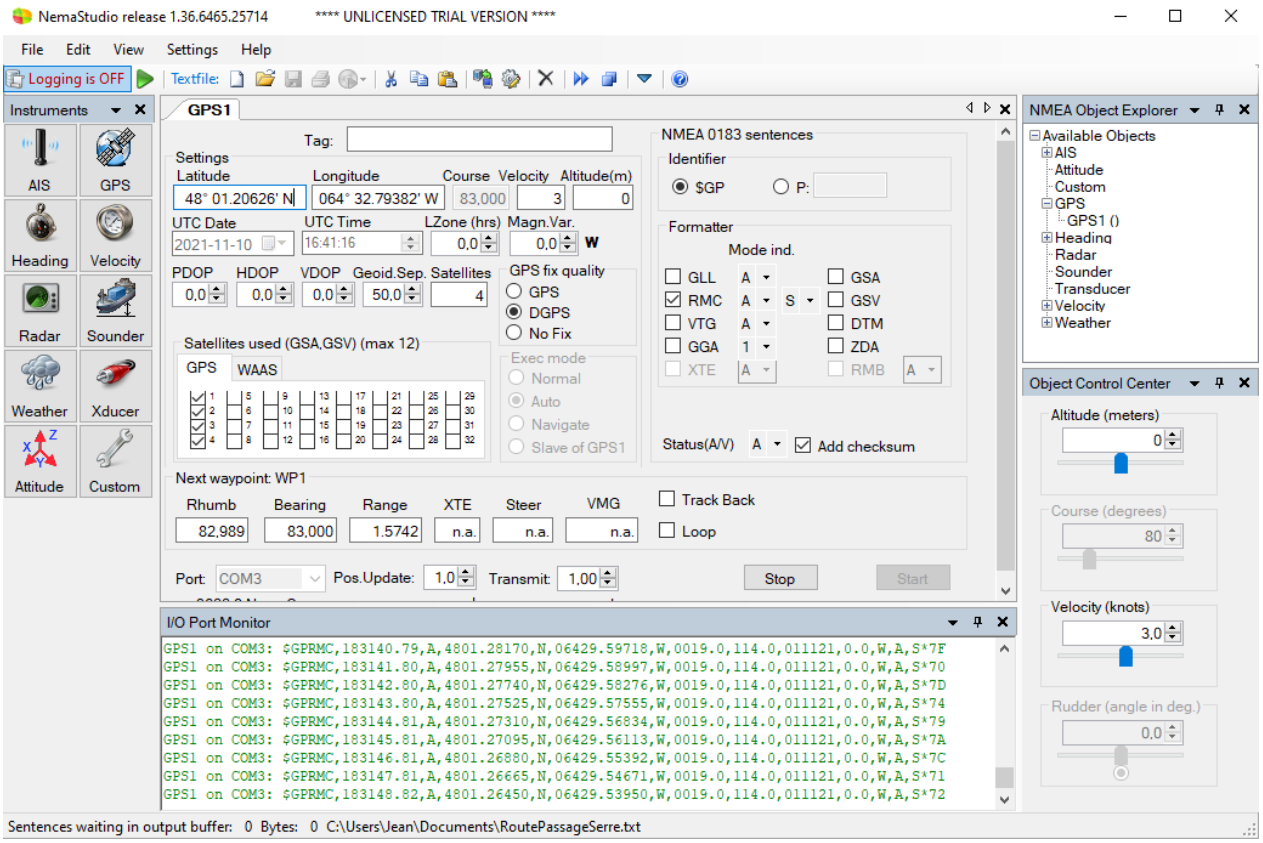

Figure 5.1 Écran de présentation du logiciel de génération de données NMEA-0183 NEMAStudio (Sailsoft)

Comme le montre la figure 5.1, le logiciel NEMAStudio permet de personnaliser une grande quantité de paramètres liés à la génération de données, par exemple la quantité de satellites impliqués, ayant ainsi une incidence sur la qualité sur signal reçu par l'ECDIS.

5.1.3 Choix de simulation de la communication

Dans notre infrastructure, nous générons des données NMEA-0183 pour les transmettre au ECDIS. Sur un vrai navire, cette communication se ferait entre les capteurs générant ces données, un écho sondeur par exemple, et l'ECDIS. Pour transmettre ces données, plusieurs choix s'offrent à nous. Nous pouvons envoyer nos données par communication série, *User Datagram Protocol* (UDP) ou *Transmission Control Protocol* (TCP). Même si la transmission par UDP et TCP est faisable, les données NMEA-0183 sont généralement transmises par communication série sur un navire. Conséquemment, nous choisissons la communication série comme moyen de transmission des données NMEA-0183, ce qui augmente la fidélité de notre infrastructure de test à ce niveau.

Pour la majeure partie de nos expérimentations, pour des raisons de limites d'accès à plusieurs ordinateurs, nous avons opté pour une simulation logicielle d'une connexion série. Effectivement, une vraie connexion série nécessite deux ordinateurs entre lesquels un câble série transmettra les données. Pour simuler une connexion série de façon logicielle, nous devons créer une connexion virtuelle *null-modem*. Une telle connexion permet de simuler la transmission d'informations à travers deux embouts de ports créés logiciellement.

Pour ce faire, nous utilisons le logiciel gratuit et libre d'accès *com0com*. Ce logiciel peut être programmé et lancé à partir d'un script, ce qui nous permet d'automatiser son utilisation. Il nous permet aussi de simuler une connexion de port série en générant une entrée et sortie et en simulant une communication série entre elles. La figure 5.2 illustre la création d'une connexion série virtuelle de COM3 à COM4 avec le logiciel com0com.

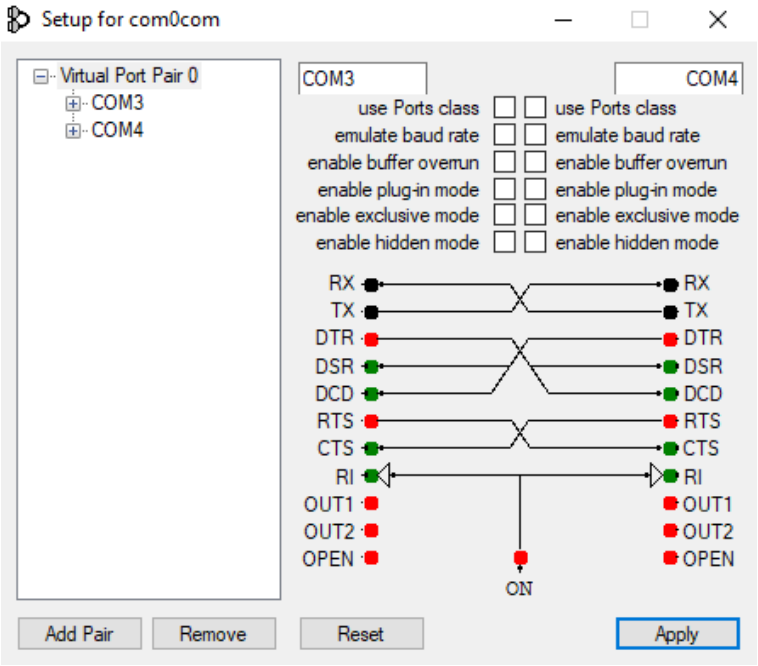

Figure 5.2 Création d'une connexion série virtuelle avec le logiciel com0com

Pour entamer la communication série, il s'agit d'envoyer les données NMEA-0183 générées vers le port COM3, puis de faire écouter le logiciel d'ECDIS sur le port COM4 de la connexion. En outre, le logiciel permet de créer simultanément plusieurs connexions séries.

5.1.4 Étude comparative de logiciels d'ECDIS

Pour notre infrastructure de test, la prochaine étape a été d'identifier un logiciel d'affichage numérique des cartes. Conséquemment, nous avons procédé à une étude comparative des logiciels d'affichage numérique des cartes maritimes. Deux critères principaux éclairaient nos décisions : la fidélité, et dans une moindre mesure, le coût-efficacité. Nous nous sommes arrêtés sur deux produits satisfaisant chacun un critère plus que l'autre.

Le premier, OpenCPN, est un logiciel libre d'accès permettant l'affichage des cartes et de différentes données recueillies sur un navire. Étant donné que le logiciel est libre d'accès, et donc gratuit, il offre une reproductibilité scientifique aux expériences pour lesquelles on l'utilise, c'est la raison pour laquelle il est utilisé dans la communauté scientifique à des fins d'expérimentation. La figure 5.3 illustre un flux de données GPS, de cap, d'écho sondeur et de vent généré par NEMAStudio sous la forme de phrases NMEA-0183 de format GGA, HDG, DBT et MWD respectivement, puis envoyées à OpenCPN. Ensuite, la figure 5.4 illustre le logiciel OpenCPN recevant ce flux de données.

```
06:42:58 (Serial:COM21) $GPGGA,104256.90,4649.18459,N,07111.72235,W,1,00,0.0,0,M,50.0,M,0,0*61<0x0D><0
06:42:58 (Serial:COM21) $SDDBT,04.6,f,01.4,M,00.8,F*39<0x0D><0x0A>
06:42:58 (Serial:COM21) $HCHDG,73.2,00.0,E,00.0,E*74<0x0D><0x0A>
06:42:58 (Serial:COM21) $WIMWD,358.2,T,358.2,M,000.0,N,000.0,M*5A<0x0D><0x0A>
06:42:58 (Serial:COM21) $GPGGA,104257.51,4649.18620,N,07111.71458,W,1,00,0.0,0,M,50.0,M,0,0*6F<0x0D><0
06:42:58 (Serial:COM21) $SDDBT,04.6,f,01.4,M,00.8,F*39<0x0D><0x0A>
06:42:58 (Serial:COM21) $HCHDG,73.2,00.0,E,00.0,E*74<0x0D><0x0A>
06:42:59 (Serial:COM21) $WIMWD,359.6,T,359.6,M,000.0,N,000.0,M*5A<0x0D><0x0A>
06:42:59 (Serial:COM21) $GPGGA,104258.52,4649.18781,N,07111.70681,W,1,00,0.0,0,M,50.0,M,0,0*6E<0x0D><0
06:42:59 (Serial:COM21) $SDDBT,04.6,f,01.4,M,00.8,F*39<0x0D><0x0A>
06:42:59 (Serial:COM21) $HCHDG,73.2,00.0,E,00.0,E*74<0x0D><0x0A>
06:42:59 (Serial:COM21) $WIMWD,357.3,T,357.3,M,000.0,N,000.0,M*5A<0x0D><0x0A>
06:43:00 (Serial:COM21) $GPGGA,104259.54,4649.18942,N,07111.69904,W,1,00,0.0,0,M,50.0,M,0,0*62<0x0D><0
06:43:00 (Serial:COM21) $SDDBT,04.6,f,01.4,M,00.8,F*39<0x0D><0x0A>
06:43:00 (Serial:COM21) $HCHDG,73.2,00.0,E,00.0,E*74<0x0D><0x0A>
06:43:00 (Serial:COM21) $WIMWD,001.1,T,001.1,M,000.0,N,000.0,M*5A<0x0D><0x0A>
06:43:01 (Serial:COM21) $GPGGA,104300.55,4649.19103,N,07111.69127,W,1,00,0.0,0,M,50.0,M,0,0*6B<0x0D><0
```

Figure 5.3 Flux de données GPS, de cap, d'écho sondeur et de vent envoyé à OpenCPN

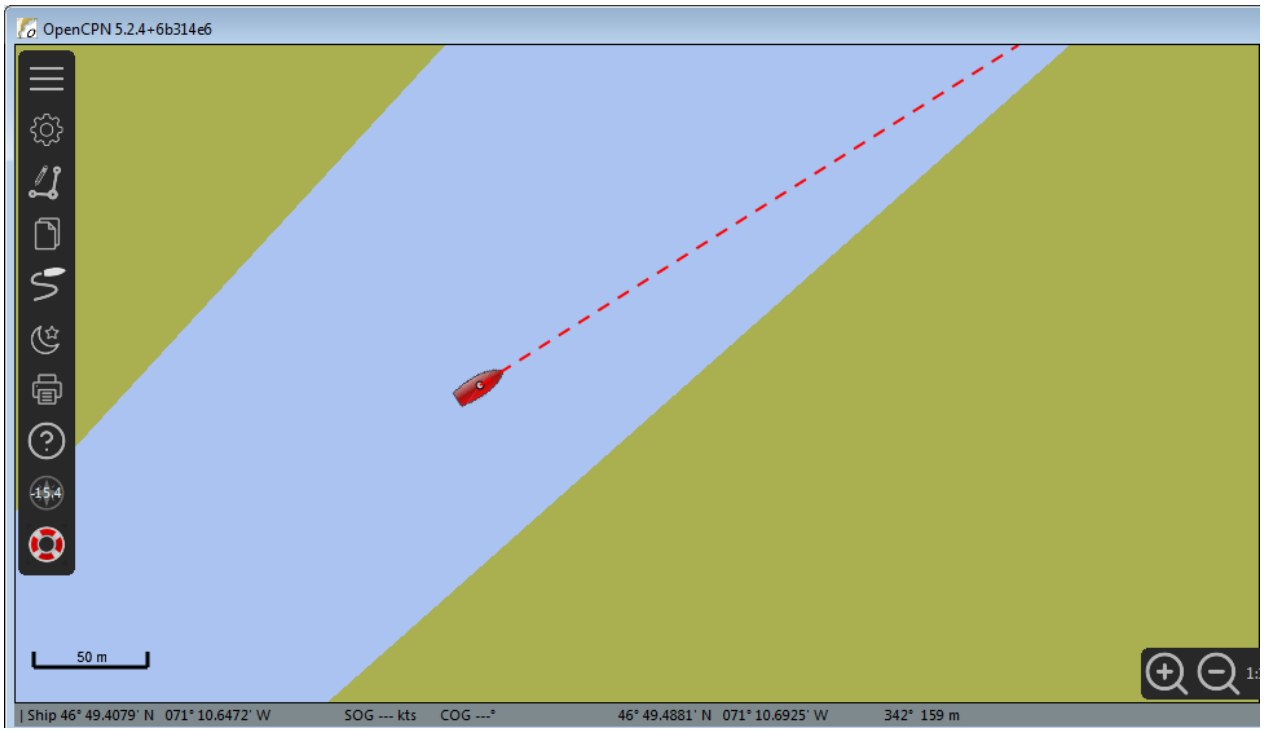

Figure 5.4 Écran d'OpenCPN affichant la position et le cap du navire

Comme le montre la figure 5.4, le logiciel OpenCPN met à jour la position et le cap du navire rouge et son cap selon les données GPS et de cap reçues. Cependant, comme le logiciel OpenCPN n'est pas un véritable ECDIS utilisé par les navires, mais un simulateur d'ECDIS, il n'arrive à interpréter en entrée que les données de base. En l'occurrence, les données d'écho sondeur et d'anémomètre, pour ne nommer que celles-ci, ne sont pas interprétées par OpenCPN. Conséquemment, on constate que le logiciel OpenCPN ne satisfait pas les critères de fidélité ni de diversité comme nous le voudrions.

Pour remédier au problème de manque de réalisme rencontré par l'utilisation d'OpenCPN, nous avons exploré une seconde option de logiciel d'affichage de cartes, c'est-à-dire le logiciel TimeZERO, développé par MaxSEA. Ce logiciel n'est pas un logiciel de simulation d'ECDIS, mais un véritable logiciel d'ECDIS utilisé sur les navires. Conséquemment, le degré de réalisme que nous offre ce logiciel est plus élevé. Effectivement, il permet de prendre en entrée toutes les données que nous avons prévu de simuler, il satisfait donc nos critères de fidélité et de diversité. La figure 5.5 illustre le logiciel TimeZero recevant le flux de données GPS, de cap, d'écho sondeur et de vent.

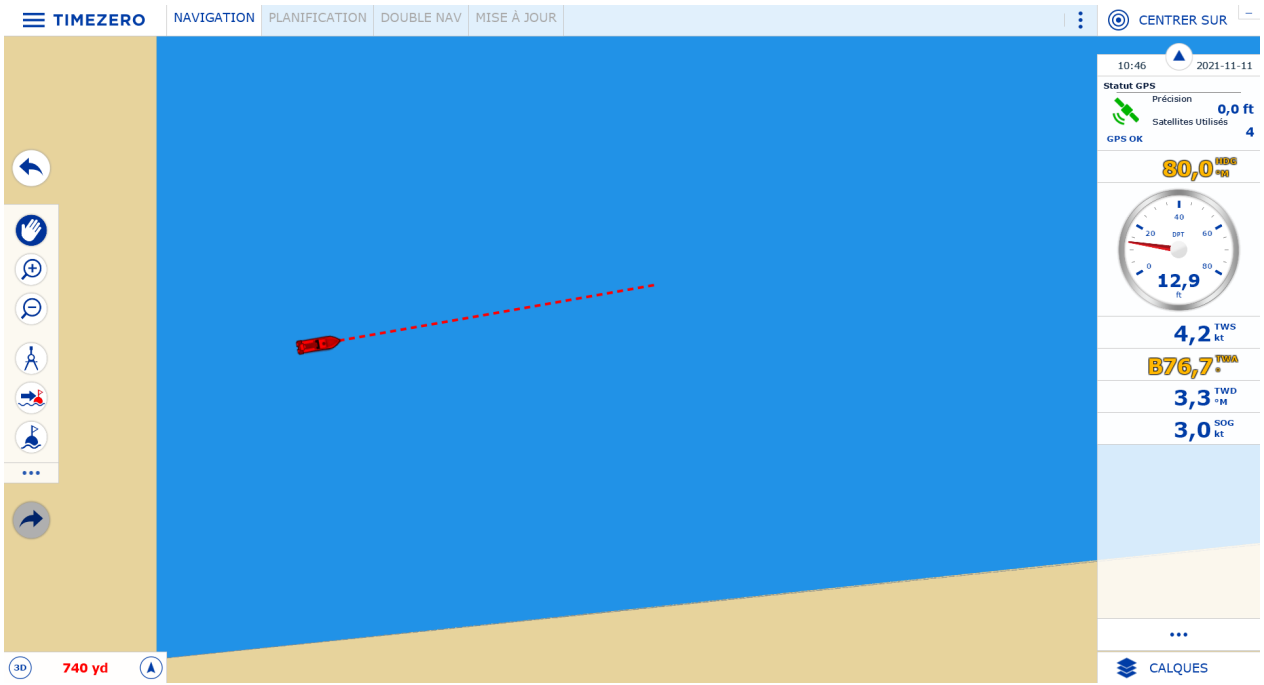

Figure 5.5 Écran de TimeZero Navigator affichant la position et le cap du navire, puis les données d'écho sondeur et de vent

Tel que le montre la figure 5.5, le logiciel TimeZero comporte un tableau de bord permettant d'afficher les données reçues à l'officier de navigation. Dans ce cas-ci, nous pouvons voir à droite un cadran pour la profondeur de l'eau et divers affichages numériques de données sur le vent. En outre, TimeZero permet de personnaliser son tableau de bord. La figure 5.6 montre l'éventail des données pouvant être affichées sur ce tableau.

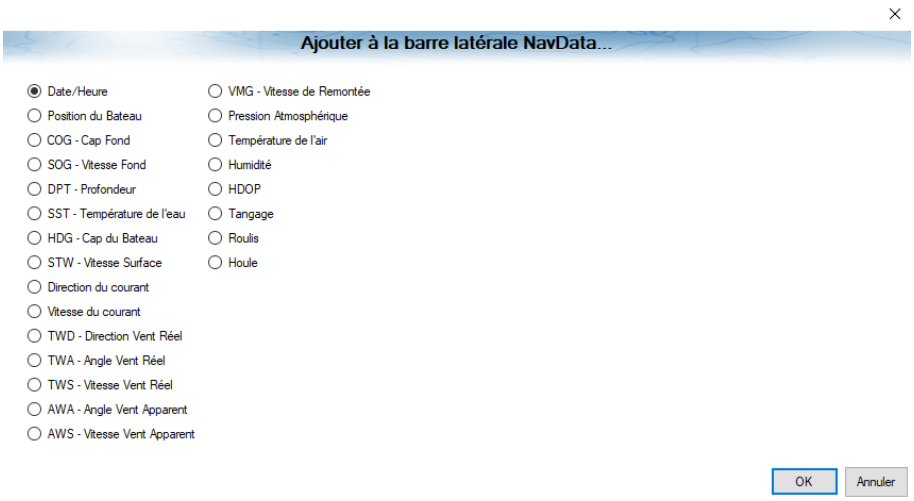

Figure 5.6 Configuration du tableau de bord de TimeZero Navigator

Pour la version du logiciel, nous avions le choix entre TmeZERO Navigator et Professional. Nous avons opté pour Navigator étant donné que cette version nous permettait d'afficher toutes les informations dont nous avions besoin, et même au-delà. Pour le critère de coût-efficacité, nous avons jugé que la version Professional n'aurait pas fait suffisamment augmenter la fidélité de l'instructure pour la différence de prix.

5.1.5 Infrastructure de test

En somme, plusieurs choix ont été faits lors de la mise en place de l'infrastructure dans le but de respecter le plus possible nos caractéristiques de conception, majoritairement la fidélité et la diversité. La figure 5.7 est un schéma sommaire de notre implémentation de l'infrastructure de test.

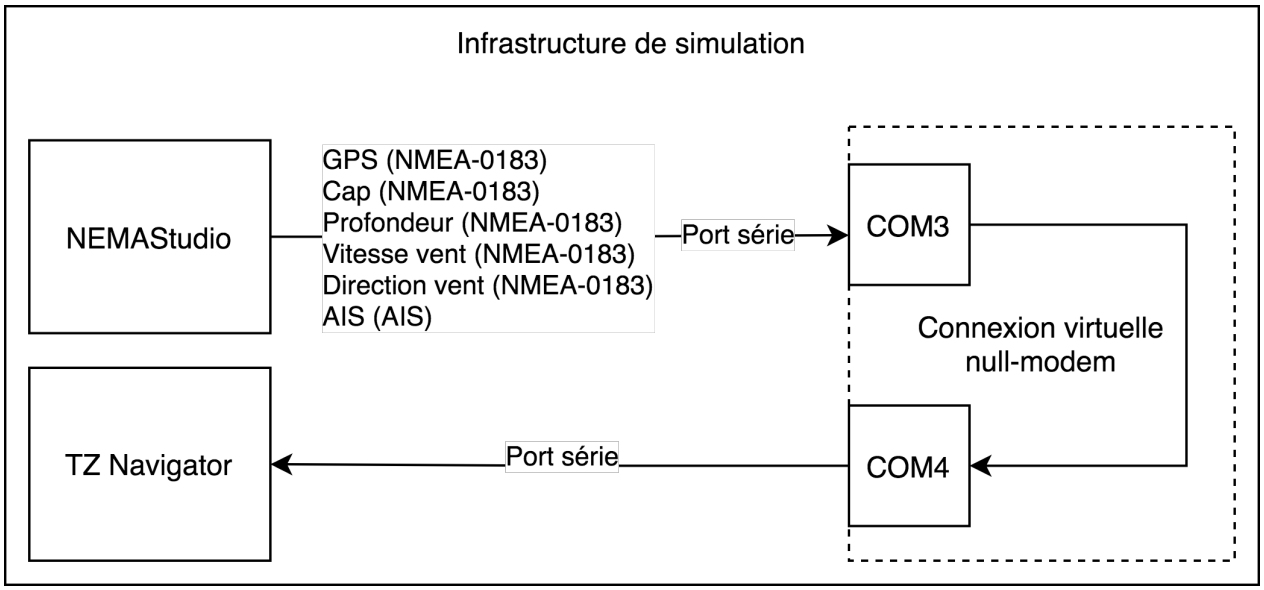

Figure 5.7 Implémentation de l'infrastructure de test

Comme on peut l'observer sur la figure 5.7, les ports COM3 et COM4 sont les deux embouts de la connexion virtuelle *null-modem* créée avec le logiciel com0com. C'est à travers cette connexion virtuelle que les données générées par NEMAStudio peuvent être transmises à TimeZero Navigator.

5.2 Mise en place des étapes 1 à 6 de la chaîne de frappe

Une fois l'infrastructure de test implémentée, la prochaine étape a été d'implémenter les différentes attaques modélisées au chapitre 4. Comme expliqué précédemment, les six premières étapes de la chaîne de frappe sont identiques pour les trois scénarios décrits. Dans cette section, nous décrirons en détail notre implémentation de ces six différentes étapes, à l'exception de la seconde partie de l'étape d'exploitation, qui sera propre à chacun des scénarios, et donc décrite dans la section 5.3.

5.2.1 Reconnaissance

Nous avons établi que l'objectif pour l'attaquant lors de la phase de reconnaissance est de déterminer le navire à attaquer, déterminer l'identité de son officier de navigation ainsi que son adresse courriel, puis déterminer une occasion de le rencontrer dans un contexte qui n'éveillera pas les soupçons, évènement professionnel par exemple. Pour cette étape, aucune implémentation n'a été requise.

5.2.2 Armement

Pour cette étape, deux processus d'armement ont été à développer en parallèle. Tout d'abord, la création d'un fichier malveillant sous la forme d'un PDF, puis la configuration d'une clé USB infectée.

Fichier PDF infecté

Notre but avec ce fichier est que l'officier de navigation l'ouvre sur l'ordinateur portable ayant accès à internet dans le but de donner un accès à distance à cette machine par l'attaquant. Pour ce faire, nous avons décidé de camoufler ce fichier sous la forme d'un fichier PDF, sous le nom « consignes.pdf ». De plus, il faut préciser qu'un incitatif à l'ouverture du fichier est mis en place, par exemple préciser dans le courriel que ce fichier contient de nouvelles consignes en matière de cybersécurité selon les nouvelles règles de la BIMCO. Ce faisant, l'officier l'ouvrira en croyant qu'il s'agit de consignes, et il y lira effectivement une suite de consignes avec des règles de sécurité. En ouvrant le fichier, celui-ci ouvrira une connexion avec la machine de l'attaquant, lui donnant ainsi accès à distance à l'ordinateur portable.

Pour l'implémentation, nous utilisons l'outil *msfvenom*. Celui-ci est un outil lancé par ligne de commande permettant de générer des charges utiles [114]. Nous créons avec *msfvenom* un fichier exécutable nommé « consignes.exe ». Pour la création de ce fichier, nous utilisons

l'option *reverse_tcp*. Cette option permet d'obtenir un tunnel inversé par communication TCP [115]. Finalement, nous camouflons le fichier exécutable à l'intérieur d'un fichier PDF. Conséquemment, lors de l'ouverture de ce fichier, le fichier consignes.exe s'exécute également et donne accès à distance à l'attaquant.

Clé USB infectée

Tel que mentionné, nous utilisons l'option de la clé USB infectée comme alternative dans l'éventualité où l'officier de navigation, pour une raison ou pour une autre, n'ouvrirait pas le fichier infecté transmis par courriel. Conséquemment, lorsque cette clé se connectera à l'ECDIS, elle agira automatiquement sur la machine pour procéder aux installations nécessaires à l'infection de la machine.

Pour le choix de la clé USB, nous sommes allés avec l'option du « Rubber Ducky ». Ce dispositif, sous l'apparence d'une clé USB, est en fait un clavier pouvant injecter dans un ordinateur des commandes lancées comme si un humain les tapait. Conséquemment, pour programmer la clé, nous avons entré à l'avance une série de commandes permettant de prendre le contrôle administrateur de l'ordinateur du ECDIS, puis de lancer les divers scripts d'installation pour l'attaque.

5.2.3 Livraison

Tout comme pour l'étape précédente, deux processus de livraison sont à prévoir. D'une part, la livraison du fichier infecté par courriel, puis parallèlement la livraison de la clé USB lors d'une rencontre physique.

Livraison du fichier infecté par courriel (hameçonnage)

Pour la livraison du fichier infecté par courriel, nous utilisons l'outil *Browser Exploitation Framework* (BeEF). Effectivement, cet outil nous permet de créer des courriels d'hameçonnage. Dans le courriel, nous informons l'officier de navigation qu'une mise à jour des cartes est disponible pour l'ECDIS. De plus, nous joignons à ce courriel le fichier de type PDF et nous mentionnons dans le courriel de lire attentivement les consignes à des fins de bonne utilisation et de sécurité.

Livraison de la clé USB par rencontre physique

Pour la livraison de la clé USB par rencontre physique, plusieurs options sont possibles, telles qu'une conférence du domaine maritime à laquelle l'officier sera présent, ou encore déposer directement la clé dans le bureau de l'officier. Le choix de l'option dépend de plusieurs facteurs, dont la proximité de l'attaquant avec l'officier de navigation, ou son accès au navire à attaquer.

5.2.4 Exploitation

Pour la phase d'exploitation, deux méthodes sont développées en parallèle, soit la méthode d'exploitation en utilisant un fichier infecté transmit par courriel, puis celle utilisant une clé USB infectée remise en présentiel. La seconde phase de l'exploitation, soit l'installation des fichiers nécessaires à l'attaque, est décrite dans la section 5.3, étant donné que ces installations varieront selon chacun des scénarios.

Exploitation avec le fichier infecté

Tel qu'illustré sur la figure 4.3, l'ECDIS n'est pas connecté à internet, l'officier de navigation doit donc télécharger les cartes sur un ordinateur portable et transférer les fichiers vers l'ECDIS avec une clé USB. Dans l'éventualité où l'officier de navigation a ouvert, sur l'ordinateur portable, le fichier contenant la charge utile, celui-ci donnera alors l'accès à distance à l'attaquant, qui pourra ajouter des fichiers infectés la clé USB. Une fois les fichiers transférés sur la clé, celle-ci sera connectée à l'ordinateur sur lequel roule l'ECDIS et exécutera un script pour la prise de contrôle et l'installation des fichiers nécessaires à l'attaque. Lorsque la clé USB sera connectée à l'ordinateur d'ECDIS, nous devrons exécuter plusieurs tâches. Tout d'abord, nous devons obtenir les privilèges d'administrateur. Ensuite, en assumant que l'officier aura enclenché le processus d'installation des nouvelles cartes, nous devons attendre que celles-ci soient installées. Une fois que les cartes sont mises à jour, nous pouvons passer aux prochaines étapes d'installation, qui seront décrites à la section 5.3 pour chacun des trois scénarios.

Exploitation avec la clé USB infectée

Dans le cas où l'officier n'a pas ouvert le fichier PDF, la clé USB infectée contiendra des commandes de prise de contrôle, les fichiers infectés et les cartes de mise à jour. Lorsque la clé sera connectée à l'ordinateur du ECDIS, un script lancé par la clé ira chercher les privilèges d'administrateur, et une fois que l'officier aura installé la mise à jour de cartes, le script effectuera les installations nécessaires, qui seront décrites pour chacun des scénarios.

5.2.5 Installation / Commandement et contrôle

Tel que mentionné dans le chapitre 4, ces étapes ne pourront être implémentées, étant donné l'ordinateur sur lequel roule le ECDIS n'est pas connecté à internet de façon régulière et consistante. Conséquemment un accès à distance permanent ne serait pas envisageable dans ce contexte.

5.3 Mise en place de l'étape #7 pour chacun des scénarios

Dans cette section, nous décrirons en détail, pour chacun des trois scénarios, l'étape #7 de la chaîne de frappe, soit l'étape « Actions sur objectifs ». Celle-ci est l'étape à laquelle on accomplit l'objectif principal de l'attaque. En outre, nous décrirons pour chacun des scénarios la seconde partie de l'étape exploitation, soit l'installation des fichiers nécessaires à l'attaque. Effectivement, ces installations varieront pour chacune des attaques selon les outils à utiliser.

5.3.1 Scénario 1 : Déni de service sur l'ECDIS

Pour cette attaque, nous voulons rendre l'ECDIS inutilisable pour l'officier de navigation en menant une attaque de déni de service sur l'ordinateur sur lequel roule le logiciel d'ECDIS. Après avoir acquis les droits administrateur de l'ordinateur, nous roulons un script de commandes powershell qui attendra quelques heures avant d'agir, le temps que le navire soit en plein trajet maritime. Ce script commence par changer le mot de passe de l'ordinateur, puis le redémarrer. Ainsi, l'officier de navigation ne pourra plus se connecter à l'ordinateur, l'ECDIS sera donc pour lui inutilisable.

Installation nécessaires au scénario 1

Aucune installation n'a été nécessaire pour ce scénario d'attaque, étant donné que nous utilisons uniquement un script de commandes powershell.

5.3.2 Scénario 2 : Usurpation de paquets et attaque par l'homme du milieu sur l'ECDIS

Pour cette attaque, nous voulons intercepter les phrases NMEA-0183 sur le canal de transmission, les modifier et les retransmettre sur le même canal, puis transmettre des phrases NMEA-0183 construites de toutes pièces. Pour ce faire, nous devions d'abord trouver un moyen pour écouter les communications sur le canal de transmission des données NMEA-0183.

Dans notre infrastructure de test, les données NMEA-0183 sont transmises par l'entremise d'une simulation logicielle d'un port série. Or, la communication par un port série a comme particularité de nécessiter l'exclusivité de l'écoute ou de l'écriture pour pouvoir respectivement écouter ou transmettre avec un port série. Autrement dit, si le logiciel d'ECDIS écoute sur le port COM4, il ne nous sera pas possible d'écouter sur ce même port parallèlement au logiciel d'ECDIS. De plus, au moment où nous en étions à cette étape, nous n'avions pas encore accès au logiciel TimeZero Navigator, nous devions donc poser l'hypothèse qu'il ne nous était pas possible de modifier le port sur lequel le logiciel d'ECDIS écoute.

Après quelques recherches, il a été possible d'utiliser un pilote de type filtre supérieur en l'attachant à l'un des embouts de la connexion sérielle alors qu'aucun logiciel n'est en écoute sur cet embout, le COM4 par exemple sur la figure 5.9, puis d'utiliser ce pilote pour écouter et modifier les données. Dans le cadre de la mise en place du scénario 2, nous avons choisi d'explorer cette option.

Le développement logiciel est un domaine où l'on part rarement de zéro. Effectivement, lorsque nous cherchons à développer un logiciel, il y a de bonnes chances que plusieurs aient fait un travail réutilisable sur lequel nous pourrons nous appuyer pour atteindre nos objectifs. Par conséquent, pour le cas du développement d'un pilote d'écoute et de modification de données sur un port série, nous avons commencé par rechercher un projet libre d'accès déjà développé sur lequel nous aurions pu nous appuyer et poursuivre le développement de notre côté. Or, après maintes recherches, aucun logiciel ou pilote libre d'accès en mesure d'écouter sur un port série, modifier les données et les renvoyer au logiciel écoutant sur ce port n'a été trouvé. Par contre, nous avons identifié un projet libre d'accès sur GitHub appelé « ENLYZE PortSniffer » développé par Colin Finck [116], permettant l'espionnage des données voyageant sur un port série en utilisant un pilote de type filtre supérieur, puis une application console envoyant des commandes à ce pilote. Pour pouvoir s'attacher à un embout de la connexion série virtuelle, celle-ci ne doit avoir sur elle aucun logiciel en écoute ou en écriture. Une fois le pilote attaché à l'embout, on peut ouvrir le logiciel d'ECDIS en écoute sur l'embout et

commencer l'espionnage des données. La figure 5.8 montre le logiciel ENLYZE PortSniffer affichant au format hexadécimal les paquets NMEA-0183 transmis de NEMAStudio à l'ECDIS sur un port série.

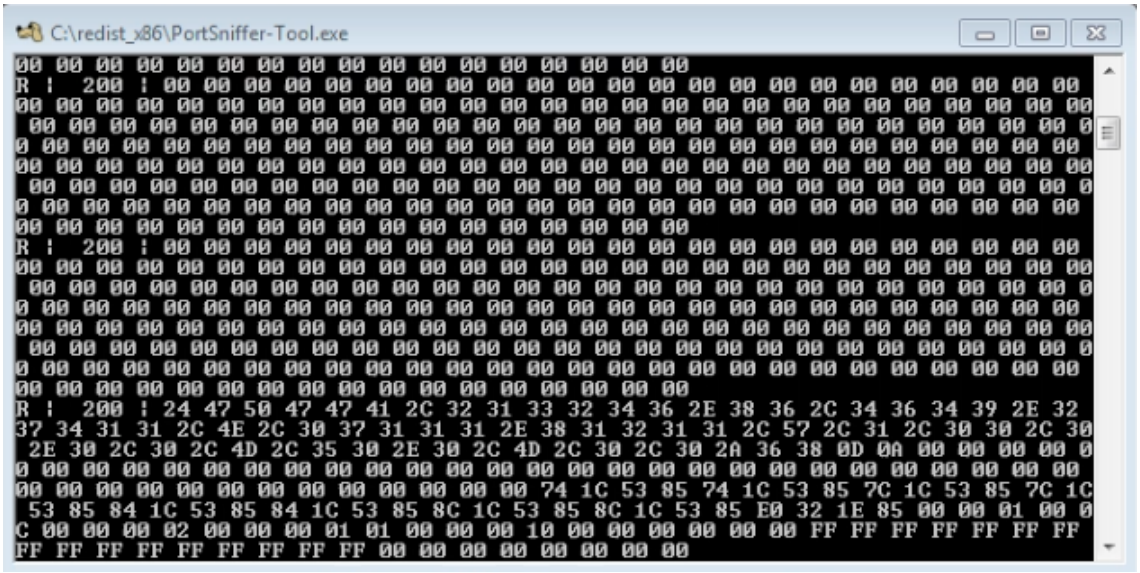

Figure 5.8 Écoute des données transmises sur un port série par ENLYZE PortSniffer

Comme nous voulions être en mesure d'écouter, mais aussi de modifier et renvoyer les données écoutées, nous avons modifié le projet libre d'accès pour rendre une telle attaque possible. Le pilote est écrit en langage C. Après nos ajouts, nous pouvons maintenant surveiller les données transmises sur un port série donné. Ensuite, nous pouvons mener une attaque d'usurpation de paquet, puis une attaque par l'homme du milieu. Pour l'usurpation de paquet, le pilote injecte dans le port série des paquets synthétisés de toutes pièces. La figure 5.9 illustre l'implémentation du second scénario d'attaque dans notre infrastructure de test.

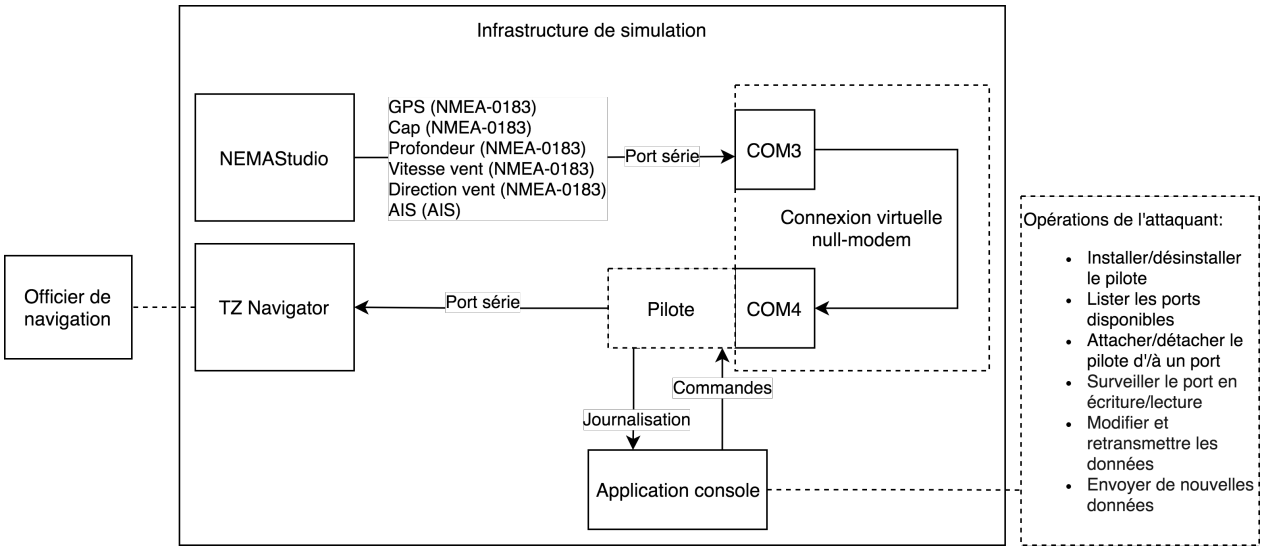

Figure 5.9 Architecture informatique pour l'implémentation du scénario 2

Pour l'attaque par l'homme du milieu, nous envoyons des phrases GPS de format RMC, générées par NMEAStudio, puis nous les interceptons. Ensuite, nous modifions la latitude de chacune de ces phrases de manière à ce que le navire soit décalé de 30 mètres vers le Nord. La phrase NMEA-0183 suivante est une phrase GPS de format RMC pour une route allant de Québec à Halifax.

$$\$GPRMC, 150432.16, A, \underline{4649.55017}, N, 07112.39860, W, 0016.0, 080.0, 111121, 0.0, W, A, S*78$$

Sur la phrase NMEA-0183 précédente, la latitude est indiquée par le nombre «4649.55017». Pour décaler le navire de 30 mètres vers le Nord, c'est ce champ que nous changeons. La phrase NMEA-0183 suivante est la phrase précédente après modification de sa latitude pour le décalage du navire.

$$\$GPRMC, 150432.16, A, \underline{4649.56640}, N, 07112.39860, W, 0016.0, 080.0, 111121, 0.0, W, A, S*7F$$

On remarque que le dernier caractère de la phrase a également changé. Effectivement, les deux derniers caractères d'une phrase NMEA-0183 est un *checksum*, soit un calcule effectué sur la phrase elle-même résultant en une suite de caractères hexadécimaux. Or, les logiciels d'ECDIS ont l'option de vérifier si le *checksum* n'est pas compatible avec la phrase reçue, tant

un tel cas la phrase sera ignorée. Conséquemment, ce champ agit comme mesure de protection pour s'assurer qu'un changement quelconque dans la phrase sans ajuster le *checksum* sera rejeté. Pour contourner cette protection, nous recalculons nous-mêmes un *checksum* dès que nous modifions une phrase NMEA-0183. La figure 5.10 illustre TimeZero recevant les phrases GPS avant la modification de la latitude, puis la figure 5.11 illustre TimeZero recevant les phrases GPS modifiées.

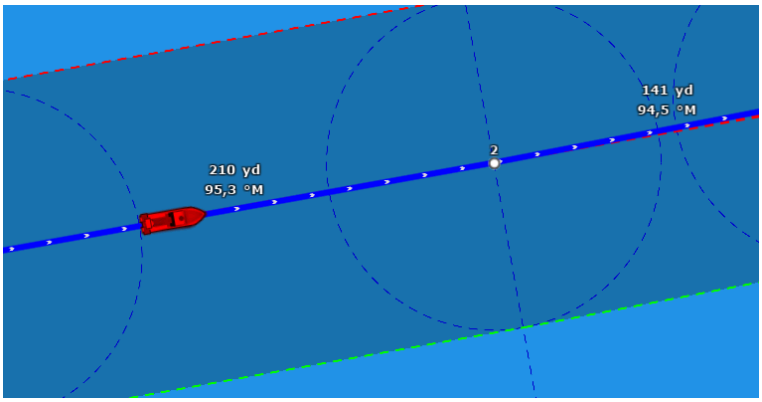

Figure 5.10 Trajectoire d'un navire dans TimeZero avant l'attaque par l'homme du milieu

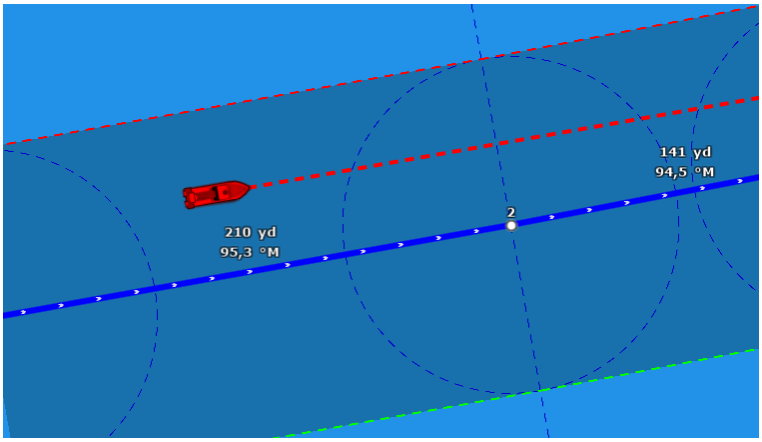

Figure 5.11 Trajectoire d'un navire dans TimeZero après l'attaque par l'homme du milieu

Les figures 5.10 et 5.11 illustrent les résultats d'une attaque par l'homme du milieu menée sur l'ECDIS. Pour l'usurpation de paquets, nous envoyons de temps à autre une phrase GPS de format RMC dont la position est aléatoire, ce qui a comme conséquence de positionner momentanément le navire à un endroit n'ayant aucun rapport avec la position précédente, et ainsi faire perdre la confiance de l'officier de navigation envers l'ECDIS.

Installations nécessaires au scénario 2

Tel que mentionné à la section 5.2, les étapes d'installation du script de la clé USB différeront selon chacun des scénarios. Pour le second scénario, nous avons besoin d'installer le pilote alors que l'ECDIS n'écoute pas sur le port série sur lequel nous voulons installer notre pilote, le logiciel TimeZero doit donc être fermé. Conséquemment, nous devions trouver un moyen pour le fermer sans éveiller les soupçons. Notre solution est de faire apparaître une fenêtre expliquant qu'un redémarrage est nécessaire pour compléter l'installation des cartes. La figure 5.12 illustre cette fenêtre de redémarrage.

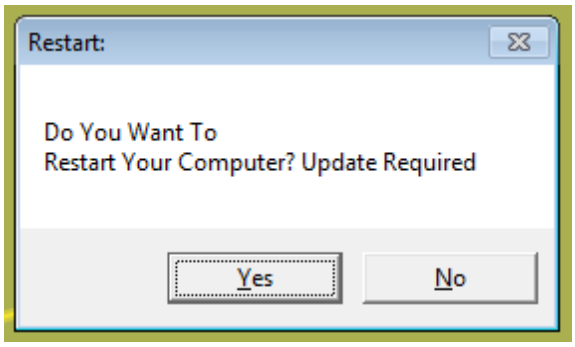

Figure 5.12 Fenêtre de redémarrage

Une fois le redémarrage terminé, nous installons les fichiers nécessaires, puis nous ouvrons le logiciel du ECDIS, soit TimeZero Navigator. En somme, les étapes d'installation sont l'attente de complétion de l'installation de la mise à jour des cartes. Une fois l'installation effectuée, nous lançons la fenêtre de redémarrage. Une fois l'ordinateur redémarré, nous installons le pilote, puis nous ouvrons TimeZero. Comme on doit attendre que le navire soit en pleine mer pour lancer l'attaque, le script attendra quatre heures après avoir intercepté des données GPS pour lancer l'attaque.

5.3.3 Scénario 3 : Attaque sophistiquée sur l'ECDIS

Pour le dernier scénario d'attaque, notre objectif est de mener une attaque sur l'ECDIS avec un degré de réalisme permettant de déjouer l'officier de navigation et le pilote automatique. Pour ce faire, nous devons modifier une plus grande quantité de données parmi celles transmises à l'ECDIS. De plus, dans le but de ne pas éveiller les soupçons de la part de l'officier de navigation, ces données doivent être modifiées de manière à refléter une situation réaliste, et les modifications doivent être congruentes entre chacune des données. Par exemple, si l'on modifie la position du navire pour le rapprocher de la rive, nous devons également

modifier son cap, qui aura changé vu le changement de position pour la même destination. Ensuite, toujours pour une modification de la position rapprochant le navire de la rive, nous devons également modifier la valeur de la profondeur, qui tend généralement à baisser plus on s'approche de la rive.

Génération des données

Pour cette attaque, les données générées sont des données de position du navire, cap du navire, profondeur de l'eau, vitesse du vent et cap du vent. Pour la position et le cap du navire, nous générons des phrases NMEA-0183 de format RMC. Pour la profondeur de l'eau, nous générons des phrases NMEA-0183 de format DPT. Pour le vent, nous générons des phrases NMEA-0183 de format MWD et VWR. La figure 5.13 illustre le flux de données que nous générons pour le scénario 3.

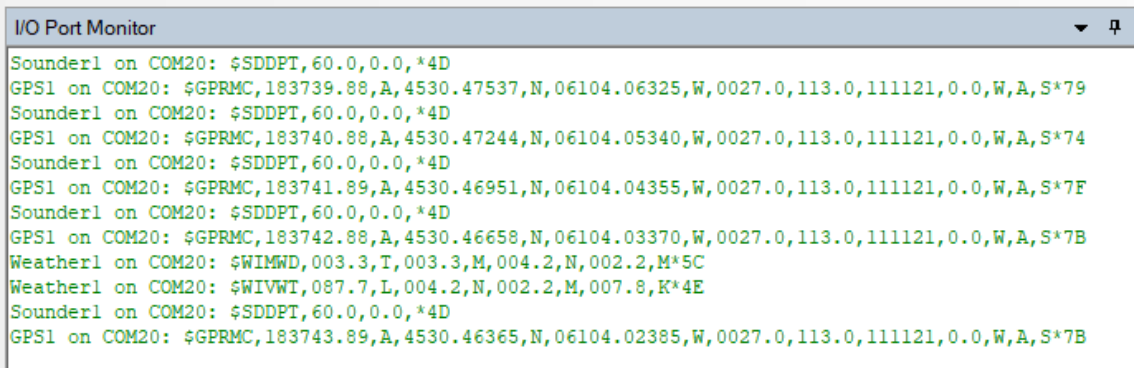

Figure 5.13 Flux de données générées pour le scénario 3

Les données que nous modifions pour le scénario 3 sont la latitude du navire, le cap du navire et la profondeur de l'eau. Pour la latitude du navire et son cap, il s'agit de modifier les phrases RMC. Effectivement, les phrases GPS NMEA-0183 de format RMC permettent, en plus de la position du navire, de communiquer son cap. La phrase suivante est un exemple de phrase GPS NMEA-0183 de format RMC.

$$\$GPRMC, 165540.84, A, \underline{4530.76093}, N, 06106.43568, W, 0003.0, \underline{091.0}, 111121, 0.0, W, A, S*79$$

Pour cette phrase, il s'agit d'incrémenter la latitude, soit le champ correspondant à la valeur «4530.76093», puis de modifier le cap, soit le champ correspondant à la valeur «091.0». Ensuite, pour modifier la profondeur de l'eau, il s'agit de modifier les phrases d'écho sondeur NMEA-0183 au format DPT, dont la prochaine phrase est un exemple.

$$\$SDDPT, \underline{4.1}, 0.0, *7E$$

Pour cette phrase, il s'agit de modifier le champ correspondant à la valeur «4,1», soit la profondeur de l'eau en mètres.

Modification des données

Pour la modification de la position du navire, nous voulons pouvoir faire un décalage de la latitude du navire, comme pour le second scénario. Cependant, si le navire change subitement de position lorsque nous lançons l'attaque, celle-ci peut éveiller les soupçons de l'officier de navigation. Conséquemment, nous voulons que ce décalage se fasse de façon adoucie. Pour la modification du cap du navire, il s'agit d'effectuer des calculs de trigonométrie pour estimer la nouvelle orientation du navire selon le décalage effectué. Par conséquent, pour chaque position modifiée, nous devons faire le calcul pour trouver le nouveau cap compatible avec la déviation de position. Pour les données de profondeur, comme le troisième scénario nécessite que le navire soit dans un chenal étroit lors de l'attaque, nous diminuons la profondeur générée au fur et à mesure qu'on décale le navire vers la rive.

Application Python

Après avoir débuté le développement du pilote pour ajouter les modifications additionnelles de données ainsi que l'adoucissement du décalage de la position, nous avons constaté que le développement d'un pilote agissant au niveau du noyau vient avec son lot de complications. Tout d'abord, le temps de développement d'un tel pilote est beaucoup plus élevé par exemple que pour une application Python, notamment par le fait que le débogage se fait au niveau du noyau, ce qui implique de déboguer avec deux machines virtuelles, et par le fait que le développement logiciel en C est généralement plus chronophage qu'en Python pour ce genre de traitement de données. Ensuite, le fait que ce pilote soit développé au niveau du noyau nous enlève une multitude d'implémentations natives du langage C, tel que les flottants, que nous devions ainsi réimplémenter nous-mêmes pour notre projet. Conséquemment, vu les complications liées au développement du pilote, nous étions à la recherche d'une solution alternative.

En analysant le logiciel TimeZero Navigator et ses failles potentielles, nous avons constaté que la configuration des ports série était sérialisée dans un fichier de type *Extensible Markup Language* (XML), et qu'il nous était possible de le modifier. Par conséquent, nous avons alors la possibilité de modifier à notre guise les ports sur lesquels le logiciel d'ECDIS écoute.

À la lumière de cette découverte, nous avons développé une autre architecture pour le scénario 3 qui nous donnerait une plus grande malléabilité au niveau du développement, et ainsi une augmentation de notre efficacité. Effectivement, comme nous pouvons modifier le port série sur lequel TimeZero Navigator écoute, nous pouvons ainsi rediriger le trafic vers une application Python, qui n'est plus au niveau du noyau. Or, en plus de régler le problème du développement au niveau du noyau, le langage Python permet généralement un temps de développement plus court que le langage C. Cette application retransmettrait ainsi les données vers une seconde connexion série virtuelle sur laquelle TimeZero Navigator écouterait désormais. La figure 5.14 montre l'architecture de l'implémentation de l'attaque sophistiquée sur l'ECDIS pour le scénario 3 en utilisant l'application Python.

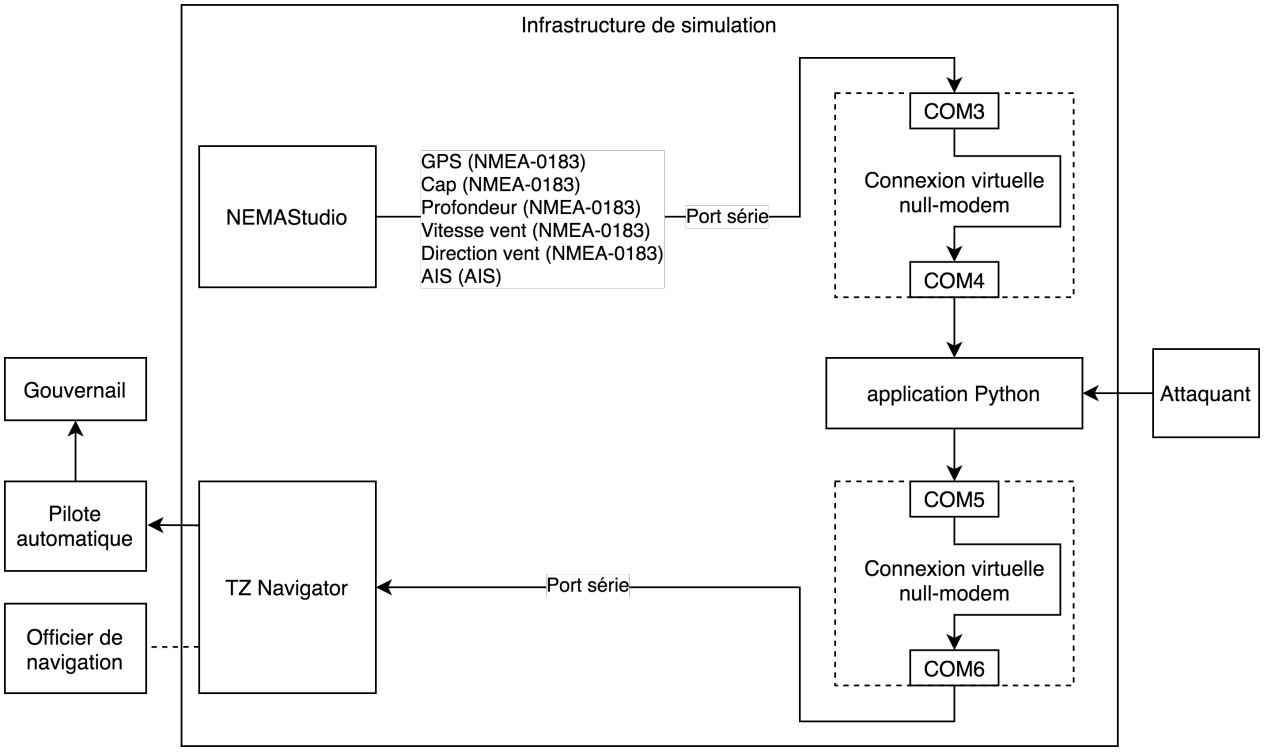

Figure 5.14 Architecture informatique pour l'implémentation du scénario 3

Adoucissement du décalage

Pour l'adoucissement du décalage de la position, nous avons choisi d'implémenter trois paramètres modifiables selon le contexte, soit la distance totale de décalage, la distance incrémentale, puis la fréquence d'incrément. Ainsi, supposons que l'on veut changer la latitude du navire de 100 mètres vers le Nord, ces 100 mètres représenteraient la distance totale de décalage. Ensuite, si la distance incrémentale est d'un mètre et que la fréquence d'incrément est d'une minute, on aurait ainsi un incrément d'un mètre toutes les minutes sur la latitude jusqu'à ce que le décalage atteigne 100 mètres. Ce faisant, la modification de position sera beaucoup mieux camouflée. De plus, en ayant ces paramètres, nous augmentons la flexibilité de notre infrastructure en nous permettant de nous ajuster à différents scénarios pour les travaux futurs.

Pour le cas de notre scénario d'attaque, nous envoyons le flux de données illustré à la figure 5.13. La figure 5.15 illustre un navire approchant un chenal étroit.

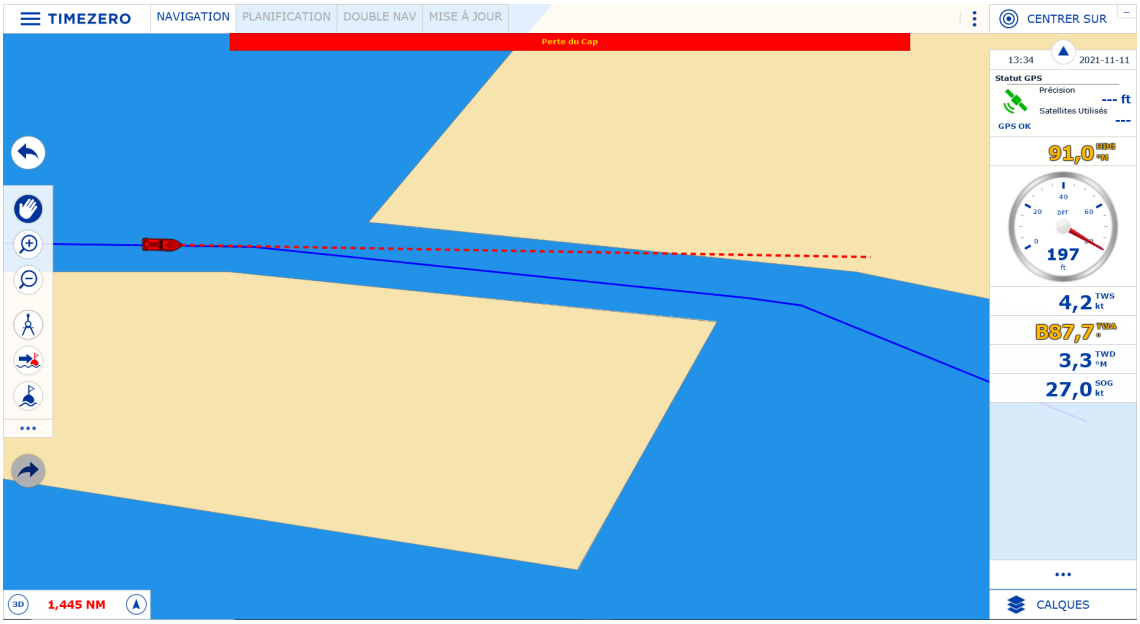

Figure 5.15 Trajectoire d'un navire dans TimeZero Navigator avant l'attaque sophistiquée

Comme le montre la figure 5.15, le logiciel TimeZero Navigator affiche sur son tableau de bord une profondeur de l'eau de 197 pieds, un cap de 92,0 degrés et des données de vent. La ligne bleu foncé montre la trajectoire du navire. La figure 5.16 montre le lancement de l'application Python, la spécification d'un décalage de 100 mètres, puis l'activation de la modification de données. La figure 5.17 montre l'impact de l'attaque sophistiquée sur TimeZero.

```
C:\Users\Jean\Documents\WannaSink_v1\python>python3 sniffer.py
>> D=100
>> t
>>
```

Figure 5.16 Lancement de l'application Python

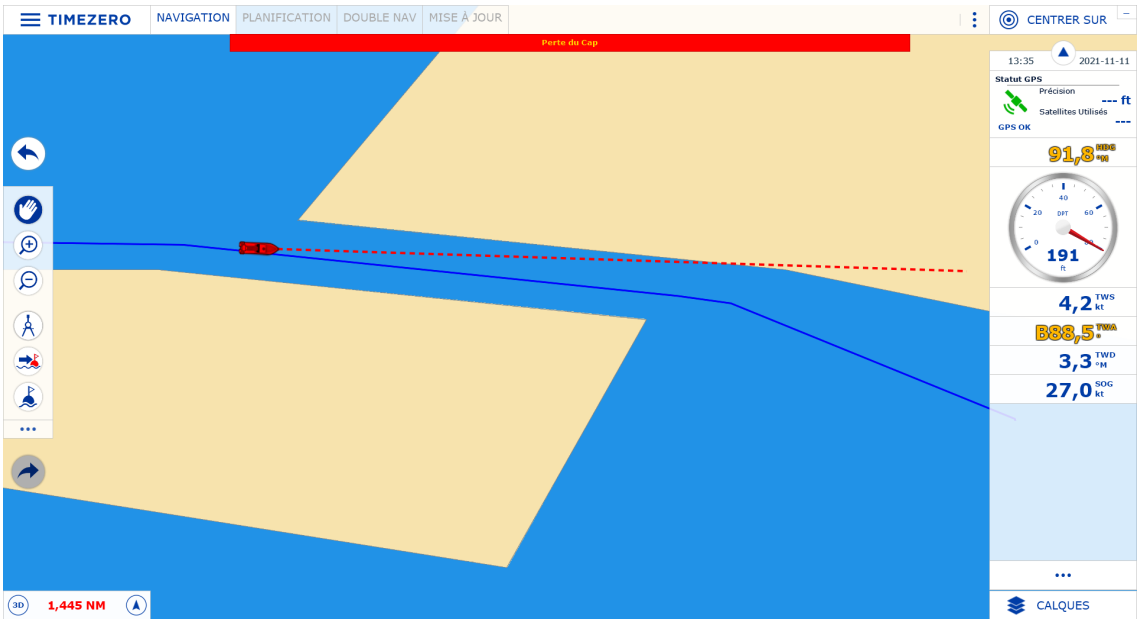

Figure 5.17 Trajectoire d'un navire dans TimeZero Navigator après le lancement de l'attaque sophistiquée (1)

Comme le montre la figure 5.17, au moment de son entrée dans le passage étroit, le navire change légèrement de trajectoire pour se diriger davantage vers le Nord. Le cap est passé de 92 à 91,8 degrés. De plus, on constate que la profondeur de l'eau diminue progressivement, le tableau de bord affichant maintenant une profondeur de 191 pieds. Les figures 5.18 et 5.19 montrent la progression de l'attaque.

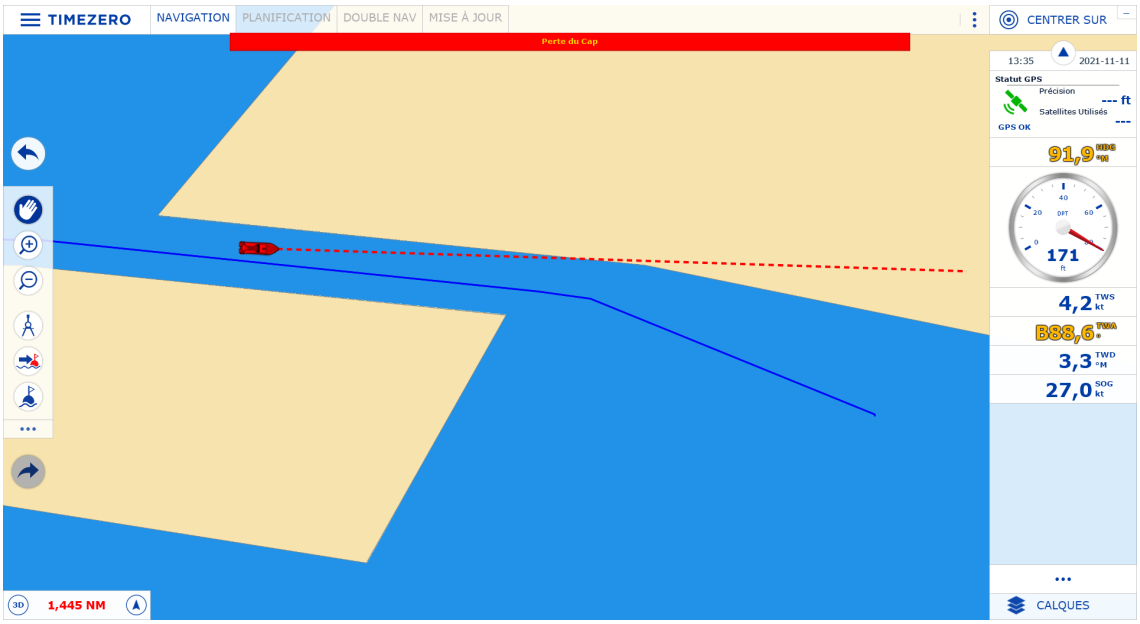

Figure 5.18 Trajectoire d'un navire dans TimeZero Navigator après le lancement de l'attaque sophistiquée (2)

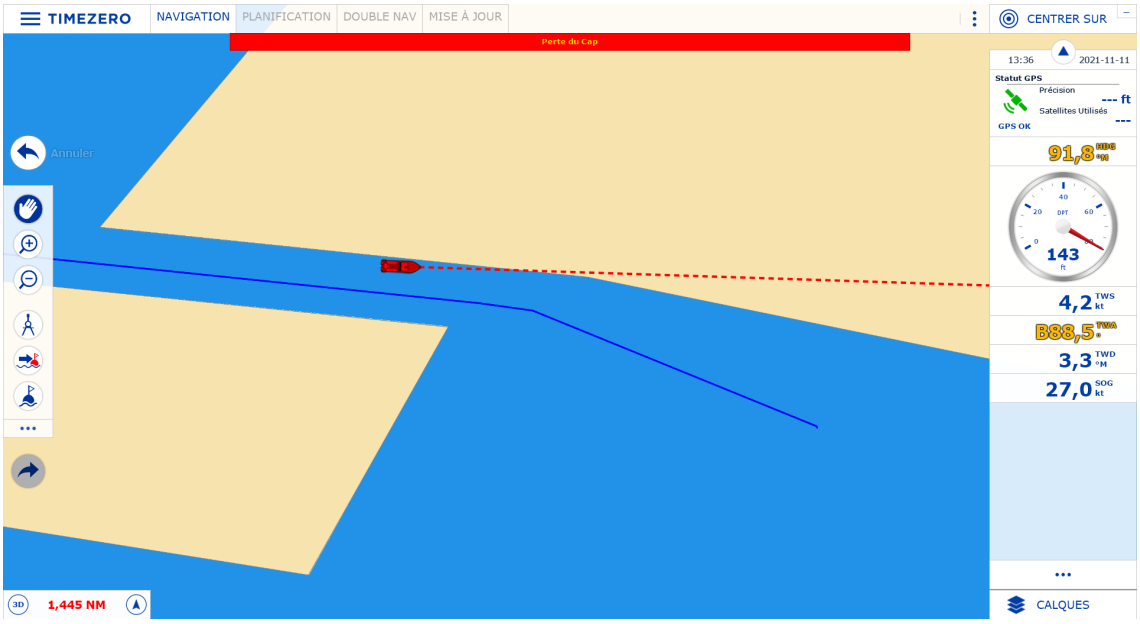

Figure 5.19 Trajectoire d'un navire dans TimeZero Navigator après le lancement de l'attaque sophistiquée (3)

Comme le montrent les figures 5.18 et 5.19, en plus de modifier la latitude du navire, nous modifions le cap du navire et la profondeur de l'eau pour que l'attaque soit réaliste. Avec cette modification des données reçues par le pilote automatique, celui-ci corrigerait la trajectoire du navire pour qu'il continue de suivre la ligne bleu foncé, le faisant donc aller davantage vers le Sud. Or, comme le navire n'avait changé de trajectoire qu'en apparence, la modification de cap du pilote automatique ferait en sorte de diriger le navire droit vers la rive inférieure du chenal.

Il est à noter que l'outil développé pour ce scénario, soit l'application Python, permet une personnalisation de plusieurs paramètres pour mener l'attaque. Ce faisant, nous pouvons facilement réutiliser cet outil pour d'autres scénarios et contextes.

Installations nécessaires au scénario 3

Pour ce scénario, comme nous n'utilisons plus le pilote, les installations nécessaires seront différentes. Effectivement, nous devrons installer les dépendances Python nécessaires à notre application, puis ajouter une connexion série à travers laquelle nous retransmettrons les données vers l'ECDIS. Ensuite, comme la redirection du port série vers notre application nécessite de changer le fichier de configuration de l'ECDIS, cette modification doit impliquer un redémarrage de l'ECDIS.

À la lumière de ces conditions, notre script commence donc par aller chercher les droits d'administrateur. Ensuite, une fois que la mise à jour des cartes sera effectuée, nous lancerons les installations de dépendances nécessaires à notre application Python, puis nous modifions le fichier de configuration de l'ECDIS pour modifier le port d'écoute à «COM6» en utilisant le script Python montré à la figure 5.20.

```python
import xml.etree.ElementTree as ET
import subprocess

class ConfigParser:
    def __init__(self, TZ_path="C:\ProgramData\TimeZeroREC\PreferencesTimeZero"):
        self.TZ_path = TZ_path

    def changePort(self, write=True, port=3000):
        try:
            tree = ET.parse(f'{self.TZ_path}/InputOutput_v09.setting.xml')
        except Exception:
            return -1, -1
        root = tree.getroot()
        for portconfig in root.iter("SerialPortNumber"):
            listen = portconfig.text
            portconfig.text = str(port)
        if write:
            tree.write(f'{self.TZ_path}/InputOutput_v09.setting.xml')

        subprocess.call(["taskkill", "/F", "/T", "/IM", "TimeZero.exe"])  # forced killing, with children, by name
        subprocess.Popen([r"C:\Program Files (x86)\TimeZero\Recreational\TimeZero.exe", "--fast"])

        return f"COM{listen}"
```

Figure 5.20 Script Python pour la modification du port série sur lequel écoute TimeZero Navigator

Pour poursuivre, nous créons une nouvelle connexion virtuelle « null-modem » des ports « COM5 » à « COM6 ». Dans le but de redémarrer l'ECDIS sans éveiller les soupçons, nous émettons la même fenêtre qu'au second scénario, indiquant à l'officier qu'un redémarrage est nécessaire pour l'installation des cartes. Une fois l'ordinateur redémarré, nous lançons notre application Python et ouvrons TimeZero Navigator. Pour ce scénario, le moment où on lance l'attaque doit être au moment même où le navire entre dans un chenal. Conséquemment, pour pouvoir coordonner le début de l'attaque avec l'entrée dans le chenal, un travail futur pourra être fait en analysant les données de trajectoire, puis en évaluant si le navire se dirige dans un chenal et lancer l'attaque au moment opportun.

5.4 Résultats/Analyse

Dans le cadre de cette maîtrise, nous avons entrepris la mise en place d'une infrastructure de test pour la cybersécurité des systèmes maritimes. Ensuite, nous avons mené une gradation d'attaques au sein de cette infrastructure. Dans cette section, nous allons présenter les résultats de ces implémentations et analyser leurs impacts à la lumière de nos objectifs de conception et des caractéristiques critiques et secondaires choisies pour notre infrastructure de test.

5.4.1 Résultats et analyse de la mise en place de l'infrastructure de test

Le système que nous avons choisi d'inclure au sein de notre infrastructure est le système ECDIS, pour lequel nous avons choisi d'utiliser le logiciel TimeZero Navigator. En générant des données avec le logiciel NEMAStudio, nous réussissons à envoyer un flot de données de position du navire, cap du navire, profondeur de l'eau et vitesse et direction du vent au ECDIS, simulant ainsi un navire en mouvement sur l'eau.

Retour sur les objectifs de conception

Pour la modélisation de notre infrastructure de test, nous avions considéré quatre objectifs de conception, soit l'analyse de vulnérabilités, l'analyse et le test d'attaques, l'éducation et entraînement et l'analyse et le test de mécanismes de détection.

Pour ce qui est de l'analyse de vulnérabilités, notre infrastructure de test a été mise en place de façon à permettre une bonne analyse de vulnérabilité pour les développements futurs. Effectivement, même si ce n'est pas une tâche à laquelle nous nous sommes concentrés explicitement dans le cadre de ce mémoire, l'infrastructure de test permettra, avec sa grande modularité et évolutivité, d'ajouter divers éléments et protocoles et d'en tester les vulnérabilités plus en profondeur. Pour cette maîtrise, nous nous sommes concentrés principalement sur l'analyse de vulnérabilité du protocole NMEA-0183 et du système ECDIS.

Ensuite, nous avons démontré que notre infrastructure de test est bel et bien adéquate pour l'analyse et le test d'attaques. En effet, avec la gradation de scénarios que nous avons modélisée et implémentée au sein de notre infrastructure, nous avons pu démontrer la flexibilité de notre plateforme en démontrant différents scénarios ayant chacun des caractéristiques particulières. Or, pour chacun de ces scénarios, l'infrastructure a su bien s'adapter sans avoir à repenser l'architecture à chaque fois. En outre, comme nous le verrons dans la sous-section 5.4.2, notre infrastructure nous permet d'analyser ces attaques suite à leur implémentation.

Pour poursuivre, nous postulons que notre infrastructure remplit et remplira bien notre troisième objectif de conception, soit l'éducation et entraînement. En effet, tel qu'énoncé précédemment, l'architecture de notre infrastructure de test lui permet de s'adapter à plusieurs scénarios d'attaques, notre infrastructure sera donc pertinente dans un contexte d'entraînement où nous voudrons développer une panoplie de nouveaux scénarios. De plus, nous croyons que l'outil que nous avons choisi pour générer les données, soit NEMAStudio, est également malléable pour différentes situations et facile d'utilisation, ce qui est idéal pour l'utilisation à des fins académiques.

Finalement, étant donné qu'une bonne partie du temps de ma maîtrise a été consacrée à l'analyse préliminaire et au déploiement de l'infrastructure de test, les mécanismes de détection pour notre infrastructure seront à développer pour les prochains étudiants travaillant sur ce projet. De plus, cette infrastructure a été conçue pour pouvoir bien accueillir de tels mécanismes. Effectivement, la grande modularité et évolutivité de notre architecture nous permettrait de facilement ajouter de nouveaux éléments, tel qu'un détecteur d'anomalie et d'analyser son efficacité et ses impacts.

Retour sur le choix de simulation

Lors de la modélisation de notre infrastructure, nous avons choisi d'utiliser une approche hybride de simulation, soit en incorporant des simulations logicielles avec des simulations semi-physiques. Cette approche nous permettait d'augmenter la fidélité de notre infrastructure. Or, dans le cadre de ce mémoire, seules des simulations logicielles ont été incorporées. Effectivement, le temps alloué pour ce projet a fait en sorte pour nous de choisir des approches purement logicielles. Cependant, comme l'infrastructure évoluera avec le temps avec les futurs étudiants du laboratoire, l'évolutivité et la flexibilité de notre plateforme permettront d'incorporer des simulations semi-physiques à l'infrastructure de test.

Une idée intéressante d'incorporation d'une simulation semi-physique est d'intégrer un système de pilote automatique, qui recevrait en entrée les données de position du navire émises par l'ECDIS, et aurait une incidence sur les données simulées par NEMAStudio. Ce pilote automatique pourrait ainsi ajuster la direction du navire selon les variations sur l'itinéraire, et ainsi faire varier la position simulée par NEMAStudio.

5.4.2 Résultats et analyse de la mise en place des attaques

Pour l'implémentation des attaques, nous avons modélisé et implémenté trois scénarios à travers une chaîne de frappe, pour laquelle les six premières étapes sont communes aux trois scénarios, à l'exception d'une partie de l'étape d'exploitation. Nous allons commencer par analyser les étapes préliminaires communes aux trois scénarios, puis nous analyserons les attaques pour chacun des scénarios.

Étapes préliminaires

Les étapes préliminaires communes aux trois scénarios implémentés à la section 5.2 nous indiquent qu'il nous est possible d'infiltrer le système d'ECDIS d'un navire avec le scénario de fichier infecté envoyé sous la forme d'hameçonnage, ou encore la clé USB infectée transmise

physiquement à un officier de navigation. Cependant, il serait intéressant, pour des travaux futurs, de mener une étude impliquant de vrais officiers de navigation, dans le but d'avoir des résultats tangibles et de quantifier et comparer les menaces de chacune des attaques entre elles.

Scénario 1 : Attaque par déni de service

Pour le premier scénario, nous avons pu montrer qu'il est possible de mener une attaque par déni de service sur un ECDIS. Effectivement, l'attaque que nous avons menée rend l'ECDIS inutilisable, étant donné que l'officier de navigation n'a plus d'accès visuel à son ECDIS, et ce en plein trajet maritime.

Ce scénario d'attaque a été le plus rapide à développer. Effectivement, la partie de l'intrusion du système a nécessité un temps de développement considérable, mais l'attaque de déni de service en tant que telle a été très rapide à développer. Ensuite, les chances qu'une telle attaque réussisse sont plus ou moins élevées. En effet, pour que l'attaque réussisse, l'officier de navigation doit ouvrir le fichier PDF infecté alors qu'il n'en a pas l'habitude. Pour continuer, les impacts d'une telle attaque seraient, dans l'éventualité où l'officier de navigation prend la décision de retourner au port pour régler le problème du ECDIS, de causer des pertes monétaires à la compagnie propriétaire du navire, ou encore pertes de temps au niveau de la livraison. De plus, pour une situation critique où l'ECDIS serait le dernier repère restant, par exemple si les repères visuels sont altérés lors d'une tempête et s'il arrive que le radar devienne défectueux, une telle attaque pourrait avoir des impacts critiques sur le navire et l'équipage, ceux-ci risquant effectivement une collision.

Scénario 2 : Attaque par usurpation de paquets et par l'homme du milieu

Pour le second scénario, nous avons démontré que des attaques par usurpation de paquets et par l'homme du milieu sont possibles sur des données transmises par des capteurs marins vers un ECDIS. Effectivement, à l'aide d'un pilote de type filtre supérieur, nous avons pu intercepter, sur un port série, les phrases NMEA-0183 de type GGA avant qu'elles ne soient reçues par l'ECDIS, en modifier la latitude et les retransmettre à l'ECDIS. De plus, nous avons démontré qu'il était possible, avec ce même pilote, de faire de l'usurpation de paquets en injectant de nouvelles phrases GGA et les visualiser sur l'écran du ECDIS.

Pour ce scénario d'attaque, un plus grand temps de développement a été nécessaire. En effet, nous avons mis beaucoup de temps pour adapter et développer le pilote utilisé pour mener l'attaque. Ensuite, les chances de réussite de cette attaque sont environ les mêmes. Effec-

tivement, la réussite de l'attaque dépend principalement du fait que l'officier de navigation ouvre le fichier PDF infecté alors qu'il n'en a pas l'habitude. Finalement, les impacts d'une telle attaque sont un peu moins sévères que ceux du scénario 1, puisque l'attaque ne rend pas l'ECDIS complètement inutilisable. En effet, en décalant légèrement le navire ou en injectant des données aberrantes de temps en temps, on permet tout de même à l'officier de navigation d'utiliser le ECDIS pour retourner au port.

Scénario 3 : Attaque sophistiquée

Pour le troisième scénario, nous avons démontré la possibilité de mener une attaque sophistiquée sur un ECDIS, c'est-à-dire une attaque prenant en compte et modifiant divers paramètres dans le but d'induire en erreur l'officier de navigation et le pilote automatique, et ainsi de leur faire prendre une décision ayant un impact critique sur le navire. Pour ce faire, nous avons modifié parallèlement la position du navire, le cap du navire et la profondeur captée de l'eau. De plus, nous avons intégré une paramétrisation personnalisable du décalage de la position, permettant ainsi un adoucissement de ce décalage. En lançant cette attaque dans un passage étroit lorsque les repères visuels sont affaiblis, il est possible que les corrections du pilote automatique entraînent le navire à échouer sur l'une des côtes. Les impacts d'une telle attaque pourraient être très critiques, soit de causer des dommages physiques au navire et des pertes humaines parmi l'équipage.

Pour ce scénario d'attaque, un temps de développement moyen a été requis, soit moins long que pour le scénario 2. Effectivement, même si la modification parallèle des données a été plus longue, le développement de l'application Python était beaucoup convivial que le pilote écrit en langage C. Ensuite, les chances de réussite de cette attaque sont plutôt faible. Effectivement, en plus de dépendre sur le fait que l'officier de navigation ouvre le fichier PDF, notre script d'attaque n'est pas en mesure de détecter lorsque le navire entre dans le chenal, ne pouvons donc pas automatiquement lancer l'attaque sophistiquée au moment opportun, ce qui sera un travail futur. Finalement, les impacts de ce scénario sont critiques.

Pour cette attaque, il aurait été intéressant d'incorporer un vrai système de pilote automatique, pour avoir des résultats tangibles sur la prise de décision du système dans le contexte de notre attaque. En outre, il aurait été intéressant de mener une étude sociologique auprès de vrais marins pour observer les vraies décisions qui auraient été prises lors d'attaques de la sorte, et ainsi quantifier les impacts de chacun des scénarios d'attaque.

Synthèse

Dans la présente sous-section, nous avons présenté et analysé les résultats de l'implémentation des trois scénarios d'attaques. Le tableau 5.4 fait la synthèse, pour chacun des scénarios d'attaques implémentés, du temps de développement, des chances de réussite et des impacts.

Tableau 5.4 Synthèse de l'analyse des scénarios d'attaques implémentés

	Scénario 1 : Déni de service	**Scénario 2 : Usurpation de paquets et homme du milieu**	**Scénario 3 : Attaque sophistiquée**
Temps de développement	Faible	Élevé	Moyen
Chances de réussite	Moyen	Moyen	Faibles
Impacts	Moyennement critiques	Peu critiques	Critiques

CHAPITRE 6 CONCLUSION

Le présent chapitre commence par faire une synthèse des travaux effectués dans le cadre de ce mémoire. Ensuite, nous discutons des limites de notre solution et proposons des idées de travaux futurs. Finalement, nous établissons les conclusions de nos travaux à la lumière de nos objectifs, expérimentations et résultats.

6.1 Synthèse des travaux

Dans le cadre de cette maîtrise, notre objectif était de concevoir et d'implémenter une infrastructure de test pour la cybersécurité maritime. Pour ce faire, l'approche était de simuler différents systèmes maritimes avec leurs communications, puis faire des attaques contre ces systèmes maritimes.

6.1.1 Développement d'une infrastructure de simulation

Pour atteindre notre objectif global, nous nous sommes fixé deux sous-objectifs de recherche. Le premier sous-objectif était le développement de l'infrastructure de test, en incluant un système maritime et en simulant un flux de données provenant de différents capteurs d'un navire. Nous avons débuté en établissant nos objectifs de conception, soit l'analyse de vulnérabilité, l'analyse et test d'attaque, l'analyse et test de solutions de détection ainsi que l'éducation et entraînement. Ensuite, nous avons établi diverses caractéristiques critiques et secondaires à considérer dans notre conception, tel qu'illustré dans la figure 3.2. Nous avons opté pour une approche de simulation hybride, impliquant ainsi des simulations logicielles et une simulation semi-physique. En tenant compte de cette méthodologie de conception, nous avons mis en place notre infrastructure, tel qu'illustré dans la figure 4.2. Cette infrastructure de test permet de générer un flux de données maritimes, simulant ainsi les données de capteurs sur un navire, et de les envoyer vers un ECDIS via la simulation logicielle d'une connexion série.

Nous postulons que l'infrastructure de test que nous avons mise en place reflète bien la réalité, et que son architecture permettra à la communauté scientifique de l'utiliser pour tester différentes attaques et solutions. En outre, son évolutivité et sa flexibilité permettront à d'autres chercheurs d'ajouter et de modifier des éléments à l'infrastructure, et ainsi élargir son utilisation.

6.1.2 Développement de cyberattaques contre l'infrastructure

Notre second sous-objectif était l'implémentation de cyberattaques réalistes contre l'ECDIS au sein de notre infrastructure de test. Pour ce faire, nous avons modélisé une gradation de trois scénarios d'attaque. Le premier scénario est une attaque par déni de service sur l'ECDIS, que nous avons mise en place en infiltrant l'ordinateur du ECDIS et en le rendant inutilisable par l'officier de navigation. Notre deuxième scénario est une attaque par usurpation de paquet et par l'homme du milieu sur l'ECDIS. Nous avons implémenté cette attaque en développant un pilote de type filtre supérieur pouvant intercepter, modifier et retransmettre des paquets sur l'embout d'un port série. Finalement, notre dernier scénario d'attaque était une attaque de type sophistiquée sur un ECDIS, soit une attaque modifiant plusieurs données à la fois dans le but d'induire le pilote automatique du navire en erreur. Nous avons réalisé cette attaque en redirigeant le trafic de la connexion série vers une application python, qui modifie en parallèle les données de position du navire, de cap du navire, de profondeur de l'eau et AIS, puis les retransmet au ECDIS.

La mise en place de ces trois scénarios d'attaque nous a permis de bien évaluer les compétences nécessaires à un attaquant pour arriver à exploiter des vulnérabilités informatiques à bord d'un navire, ECDIS en l'occurrence pour ce projet. En outre, nous avons pu évaluer les chances de succès et les impacts pour chacune de ces attaques. L'implémentation de ces attaques permettra à la communauté scientifique de tester différentes solutions de protection ou de détection pour y remédier.

6.2 Limites de la solution présentée et perspectives

Notre solution propose les premières briques d'une infrastructure de test maritime. Cette section aborde différentes améliorations possibles pour notre projet.

6.2.1 Approche de simulation

Tout d'abord, l'un de nos objectifs est encore à atteindre, soit celui d'inclure au sein de notre infrastructure une simulation semi-physique. Effectivement, nous souhaitions adopter une approche de simulation hybride, avec une simulation logicielle et une simulation semi-physique. Faute de temps et d'accessibilité au laboratoire, cet objectif pourra être repris par les prochains étudiants qui travailleront sur nos travaux. Effectivement, il sera intéressant d'inclure une simulation semi-physique dans l'infrastructure dans le but d'augmenter sa fidélité, et donc sa crédibilité.

Comme le développement de l'infrastructure de test se continuera dans les prochaines années dans notre laboratoire, nous allons émettre des propositions d'amélioration par rapport à la simulation semi-physique. Effectivement, un élément qui aurait été intéressant à incorporer à notre infrastructure est un pilote automatique. Avec un pilote automatique physique, nous pourrions lui envoyer les données de l'ECDIS, et ainsi avoir la vraie réaction du dispositif présent sur les navires. Un autre système qui serait intéressant à ajouter est un écran de visualisation de radar, auquel nous pourrions envoyer des données simulées. Ainsi, notre infrastructure de simulation prendrait en compte plus d'un repère visuel, et nous pourrions ainsi modéliser et implémenter des attaques encore plus sophistiquées, évaluer leur potentialité, évaluer l'effort et le bagage nécessaires à l'attaquant pour parvenir à les réaliser et proposer des solutions pour les contrer.

6.2.2 Expérimentation

Ensuite, l'expérimentation aurait pu être plus tangible et davantage prendre en compte le facteur humain. En effet, le facteur humain joue un rôle prépondérant quant aux vulnérabilités des systèmes maritimes. Ainsi, nous aurions aimé pouvoir tester nos attaques en tenant compte des réactions et des comportements de l'officier de navigation et de son équipage dans un contexte pleinement réaliste. Ainsi, nous aurions obtenu des résultats tangibles et chiffrés, permettant conséquemment d'enrichir la discussion sur les résultats.

Pour des travaux futurs, nous pensons qu'une étude sociologique rigoureuse serait à mener auprès de marins pour mesurer l'impact et la portée de chacune des attaques que nous avons développées dans le cadre de ce mémoire. Une telle étude permettrait de produire des résultats plus crédibles et de mieux cerner les impacts.

6.2.3 Implémentation de solutions de détection d'anomalies

Un autre développement futur intéressant pour notre infrastructure est l'intégration d'un système de détection d'anomalies. Effectivement nous pensons que l'inclusion d'un système permettant la détection d'anomalies au sein de notre infrastructure en augmenterait la crédibilité. Conséquemment, nous proposons comme travaux futurs à ce projet d'ajouter à l'infrastructure un détecteur d'anomalies. Par exemple, un logiciel prenant en entrée les phrases émises par NEMAStudio, puis en entrée les phrases modifiées uniquement avec l'ECDIS. Ce détecteur déterminerait quelles données auraient le plus de chances d'être des anomalies, puis nous pourrions analyser le taux de faux positifs et faux négatifs d'une telle solution.

Nous pourrions également comparer plusieurs solutions de détection entre elles grâce à notre infrastructure. Avec l'ajout de l'aspect de détection d'anomalies, nous pourrions alors parler d'une infrastructure de co-simulation.

6.3 Sommaire

En conclusion, en mettant sur pied une infrastructure de test incluant un système ECDIS et en générant un flux de données simulant des données émises par les capteurs d'un navire, nous avons répondu à notre objectif principal. En outre, l'implémentation de notre gradation de trois scénarios d'attaque a révélé certaines vulnérabilités des systèmes maritimes et a permis d'évaluer l'effort requis, les chances de réussite et les impacts de chacun de ces scénarios d'attaque. Pour la suite, dans une optique d'amélioration continue de la crédibilité de notre infrastructure, nous pensons que l'incorporation d'éléments physiques, tels qu'un pilote automatique ou un radar, serait à considérer. L'avenir de la cybersécurité maritime résidera dans la sensibilisation des acteurs du milieu maritime. Effectivement, le facteur humain joue une trop grande place dans la vulnérabilité des systèmes informatiques maritimes pour ne pas le prendre au sérieux. Dans cette même lignée, le développement d'infrastructures de test adaptées au contexte maritime sera une des clés pour aider le développement cybersécuritaire de l'industrie.

RÉFÉRENCES

[1] M. J. Ljøsne, “Network scanning industrial control systems - a vulnerability analysis,” mémoire de maîtrise, Department of Informatics, University of Oslo, 2019. [En ligne]. Disponible : https://www.duo.uio.no/bitstream/handle/10852/70862/1/thesis.pdf

[2] G. Kessler, J. P. Craiger et J. C. Haass, “A taxonomy framework for maritime cybersecurity : A demonstration using the automatic identification system,” 2018. [En ligne]. Disponible : https://www.semanticscholar.org/paper/A-Taxonomy-Framework-for-Maritime-Cybersecurity%3A-A-Kessler-Craiger/eb1e56983511a2563d56a88cc8a5f6d4eb31f58b

[3] Y. Zhang, “Review on cybersecurity risk assessment and evaluation and their approaches on maritime transportation,” 2017. [En ligne]. Disponible : https://www.researchgate.net/publication/328018682_Review_on_Cybersecurity_Risk_Assessment_and_Evaluation_and_Their_Approaches_on_Maritime_Transportation

[4] P. M. Staff, 2020. [En ligne]. Disponible : https://www.professionalmariner.com/naval-dome-maritime-cyberattacks-up-900-percent-in-three-years/

[5] S. Friedberg, “Cybersecurity predictions : A shift to managing cyber as an enterprise risk,” *AON*, 2018. [En ligne]. Disponible : https://www.thehaguesecuritydelta.com/media/com_hsd/report/205/document/2018-Cybersecurity-Predictions-Report-Aon-Cyber-Solutions.pdf

[6] G. Kessler, “Cybersecurity in the maritime domain,” *AON*, 2019. [En ligne]. Disponible : https://commons.erau.edu/cgi/viewcontent.cgi?article=2377&context=publication

[7] F. M. Kronholm, “Industry publishes new and improved cyber security guidelines,” 2020. [En ligne]. Disponible : https://www.bimco.org/news/priority-news/20201223-new-cyber-security-guidelines

[8] K. Bolton, “The clock is ticking for compliance with IMO’s 2021 cyber security regulations,” 2020. [En ligne]. Disponible : https://www.lr.org/en/insights/articles/imo-cyber-secuity-regulation-compliance/

[9] J. DiRenzo, D. A. Goward et F. S. Robert, “The little-known challenge of maritime cyber security,” 2015. [En ligne]. Disponible : http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf

[10] J. Ovcina, “Naval dome : 4002020,” 2020. [En ligne]. Disponible : https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/

[11] CyberKeel, “Maritime cyber-risks,” 2014. [En ligne]. Disponible : https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

[12] M. Professional, “Ships battling mystery cyber virus infections,” 2018. [En ligne]. Disponible : https://www.imarest.org/themarineprofessional/item/4639-ships-battling-mystery-cyber-virus-infections

[13] M. Mimoso, “Icefog espionage campaign is hit and run targeted operation,” 2013. [En ligne]. Disponible : https://threatpost.com/icefog-espionage-campaign-is-hit-and-run-targeted-operation/102417/

[14] M. Siegel et J. Irish, “Data on India’s new submarines were hacked, and it could be an act of economic warfare,” 2016. [En ligne]. Disponible : https://www.businessinsider.com/france-dcns-india-submarine-data-leak-may-be-economic-warfare-2016-8

[15] R. Davies, “Shipping firm Clarksons braces for data leak after refusing to pay hacker,” 2017. [En ligne]. Disponible : https://www.theguardian.com/technology/2017/nov/29/shipping-charksons-data-hacker-cyber-attack

[16] R. Allison, “Hacker attack left port in chaos,” 2003. [En ligne]. Disponible : https://www.theguardian.com/technology/2003/oct/07/usnews.uknews

[17] T. Bateman, “Police warning after drug traffickers’ cyber-attack,” 2013. [En ligne]. Disponible : https://www.bbc.com/news/world-europe-24539417

[18] K. B. Belmont, “Maritime cybersecurity : Cyber cases in the maritime environment,” 2016. [En ligne]. Disponible : https://aapa.files.cms-plus.com/SeminarPresentations/2016Seminars/2016SecurityIT/K.%20Belmont%20-%20AAPA%20Maritime%20Cybersecurity%20FINAL.pdf

[19] N. Lord, “The cost of malware infection ? for Maersk, 300M,” 2020. [En ligne]. Disponible : https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million

[20] I. Nastali, “Port cranes GPS signals blocked,” Rapport technique, 2019.

[21] C. Farivar, “Professor fools $80M superyacht’s GPS receiver on the high seas,” 2013. [En ligne]. Disponible : https://arstechnica.com/information-technology/2013/07/professor-spoofs-80m-superyachts-gps-receiver-on-the-high-seas/

[22] J. Saul, “Cyber threats prompt return of radio for ship navigation,” 2017. [En ligne]. Disponible : https://www.reuters.com/article/us-shipping-gps-cyber-idUSKBN1AN0HT

[23] T. Blake, “Hackers took ‘full control’ of container ship’s navigation systems for 10 hours,” 2017.

[24] J. Rundle, “Coast guard details February cyberattack on ship,” 2019. [En ligne]. Disponible : https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401

[25] S. Swanbeck, “Coast guard commandant addresses cyber-security vulnerabilities on offshore oil rigs,” 2015. [En ligne]. Disponible : https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities

[26] “Maritime cyber risk management company,” Rapport technique. [En ligne]. Disponible : https://neptunecyber.com/about/

[27] A. Trussart, “Transport maritime : à l’abordage des cyberpirates,” 2021.

[28] A. Cohen et D. Thorne, “Global threats : Cybersecurity in ports,” Center for International Business Education and Research (CIBER), Rapport technique, 2017. [En ligne]. Disponible : https://portalcip.org/wp-content/uploads/2017/03/Max-Bobys.pdf

[29] D. Bothur, C. Valli et G. Zheng, “A critical analysis of security vulnerabilities and countermeasures in a smart ship system,” *Australian Information Security Management Conference*, 2017. [En ligne]. Disponible : https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1209&context=ism

[30] J. Wang et S. M. Zhang, “Management of human error in shipping operations,” *IEEE Professional Safety*, p. 23–28, 2000.

[31] M. Zaghloul, “Online ship control system using supervisory control and data acquisition,” *IEEE International Journal of Computer Science and Application*, 2014.

[32] “Beyond data breaches : global interconnections of cyber risk,” Atlantic Council, Rapport technique, 2014. [En ligne]. Disponible : https://www.jasadvisors.com/custom/uploads/2014/04/Risk-After-Next-Whitepaper.pdf

[33] *ECDIS – Guidance for good practice*, International Maritime Organization Norme, 2017. [En ligne]. Disponible : https://www.classnk.or.jp/hp/pdf/activities/statutory/ism/imo/msc1-circ1503-rev1.pdf

[34] CyberKeel, “Security risks and weaknesses in ecdis systems,” *Marine Cyberwatch*, 2014. [En ligne]. Disponible : http://www.cyberkeel.com/images/pdf-files/Oct2014.pdf

[35] Northern California Area Maritime Security Committee, “Cyber security newsletter,” 2014. [En ligne]. Disponible : https://www.sfmx.org/wp-content/uploads/2017/03/Cyber-Security-Newsletter-2014-1.pdf

[36] Daily Mail Reporter, “The $277 million minesweeper set for the scrap heap : U.S. navy’s wooden ship stuck on reef in the philippines dismantled and hauled away,” 2013. [En ligne]. Disponible : http://www.dailymail.co.uk/news/article-2299808/USS-Guardian-Wooden-ship-stuck-reef-Philippinesdismantled.html

[37] C. Clark, “Untold tale behind uss guardian reef grounding : NGA’s map was wrong by 8 miles,” 2013. [En ligne]. Disponible : http://breakingdefense.com/2013/07/untold-tale-behind-ussguardian-reef-grounding-flawed-nga-map-data

[38] “CSL thames grounding : Not enough ECDIS training,” 2012. [En ligne]. Disponible : http://maritimeaccident.org/2012/03/csl-thames-grounding-not-enough-ecdis-training

[39] Maritime First, “Ovit : Moody crew, dodgy ECDIS, inexperience and a shy master,” 2014. [En ligne]. Disponible : http://maritimeaccident.org/2014/11/ovit-moody-crew-dodgy-ecdis-inexperience-and-a-shy-master

[40] M. Wingrove, “Accident report : Ship damaged due to incorrect ECDIS use,” 2017. [En ligne]. Disponible : https://www.marinemec.com/news/view,accident-report-ship-damaged-due-to-incorrect-ecdisuse_49611.htm

[41] CyberKeel, “GPS jamming as industry threat. marine cyberwatch, 1 october 2014,” 2014. [En ligne]. Disponible : http://www.cyberkeel.com/images/pdf-files/Oct2014.pdf

[42] H. Lanziner, “A low-cost solution to GPS vulnerabilities. technology–BC shipping news,” 2014. [En ligne]. Disponible : https://rntfnd.org/wp-content/uploads/BC-Shipping-News.pdf

[43] D. Hoey et P. Benshoof, “Civilian GPS systems and its potential vulnerabilities,” Rapport technique, 2005. [En ligne]. Disponible : www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA440379

[44] C. R. Madden, “ECDIS : What happens when the GPS signal goes away ?” 2018. [En ligne]. Disponible : https://www.maritime-executive.com/blog/ecdis-what-happens-when-the-gps-signal-goes-away

[45] J. Saul et J. Kim, “South Korea revives GPS backup project after blaming north for jamming,” 2016. [En ligne]. Disponible : http://www.reuters.com/article/us-shipping-southkorea-navigation-idUSKCN0XT01T

[46] National PNT Advisory Board, “Jamming the global positioning system—A national security threat : Recent events and potential cures,” 2010. [En ligne]. Disponible : http://www.glarrnav.org/pdfs/interference_to_gps_v101_3_.pdf

[47] Voltaire Network, “What spooked the USS Donald Cook so much in the black sea ? US-Russian incident,” 2014. [En ligne]. Disponible : http://www.voltairenet.org/article185860.html

[48] “The grounding of the royal majesty,” 2003. [En ligne]. Disponible : https://ti.arc.nasa.gov/m/profile/adegani/Grounding%20of%20the%20Royal%20Majesty.pdf

[49] R. Santamarta, “Satcom terminals : Hacking by air, sea, and land,” *IOActive*, 2014. [En ligne]. Disponible : https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf

[50] J. Pavur, D. Moser, M. Strohmeier, V. Lenders et I. Martinovic, “A tale of sea and sky on the security of maritime vsat communications,” *IEEE Symposium on Security and Privacy (SP)*, vol. 1, p. 1384–1400, 2020.

[51] E. Kovacs, “Ship data recorders vulnerable to hacker attacks. security week–internet and enterprise security news, insights and analysis,” 2015. [En ligne]. Disponible : http://www.securityweek.com/ship-datarecorders-vulnerable-hacker-attacks

[52] Marine Accident Investigation Branch Report, “Electrical failure and loss of starboard engines on ro-ro passenger ferry european endeavour resulting in contact with linkspan,” 2008.

[53] C. Wullems, O. Pozzobon, M. Looi et K. Kubik, “Enhancing the trust of location acquisition systems for critical applications and location-based security services,” *In Proceedings of the 4th Australian Information Warfare and IT Security Conference*, 2003.

[54] LabSat, “Labsat 3,” 2021. [En ligne]. Disponible : https://www.labsat.co.uk/index.php/en/products/labsat-3

[55] M. S. Lund, O. Hareide et O. Jøsok, “An attack on an integrated navigation system,” 2018.

[56] K. Furumoto, A. Kolehmainen, B. Silverajan, T. Takahashi, D. Inoue et K. Nakao, “Toward automated smart ships : Designing effective cyber risk management,” p. 100–105, 2020.

[57] M. Caprolu, R. D.Pietro, S. Raponi, S. Sciancalepore et P. Tedeschi, “Vessels cybersecurity : Issues, challenges, and the road ahead,” vol. 58, p. 90–96, 2020.

[58] A. Taylor, N. Japkowicz et S. Leblanc, “Frequency-based anomaly detection for the automotive CAN bus,” p. 45–49, 2015.

[59] J. Kim, J. Yim, Y. Kang et Y. Park, “Comparison of COTS inertial sensors for getting marine elevator’s platform tilt values,” p. 989–992, 2015.

[60] K. Tran, S. Keene, E. Fretheim et M. Tsikerdekis, “Marine network protocols and security risks,” *Cybersecurity and Privacy*, 2021.

[61] National Marine Electronics Association, “NMEA 2000® interface standard standard for serial-data networking of marine electronic devices,” National Marine Electronics Association, Rapport technique, 2016. [En ligne]. Disponible : https://www.nmea.org/Assets/20090423%20rtcm%20white%20paper%20nmea%202000.pdf

[62] National Marine Electronics Association, “OneNet standard for IP networking of marine electronic devices,” National Marine Electronics Association, Rapport technique, 2021. [En ligne]. Disponible : https://www.nmea.org/content/STANDARDS/OneNet

[63] G. Kessler, “Protected ais : A demonstration of capability scheme to provide authentication and message integrity,” TransNav Int., Rapport technique, 2020. [En ligne]. Disponible : https://www.transnav.eu/Article_Protected_AIS:_A_Demonstration_Kessler,54,1002.html#

[64] M. Balduzzi, K. Wihoit et A. Pasta, “Hey captain, where’s your ship ? attacking vessel tracking systems for fun and profit,” *IEEE The Eleventh Annual Hack in the Box,*, 2013. [En ligne]. Disponible : http://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf

[65] A. Stewart, E. Rice et P. Safanov, “Digital authentication strategies for the automated identification system,” 2018. [En ligne]. Disponible : http://micsymposium.org/mics2018/proceedings/MICS_2018_paper_64.pdf

[66] M. Balduzzi, A. Pasta et K. Wilhoit, “A security evaluation of AIS automated identification system,” *Annual Computer Security Applications Conference*, p. 436–445, 2014. [En ligne]. Disponible : http://micsymposium.org/mics2018/proceedings/MICS_2018_paper_64.pdf

[67] K. Tam et K. Jones, “MaCRA : A model-based framework for maritime cyber-risk assessment,” *UoP Technical Report*, 2019.

[68] K. Tam et K. Jones, “Factors affecting cyber risk in maritime,” *International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 2019.

[69] B. Svilicic, J. Kamahara, M. Rooks et Y. Yano, “Maritime cyber risk management : An experimental ship assessment,” *Journal of Navigation : in press, 2019*, 2019.

[70] K. Stouffer, J. Falco et K. Scarfone, “Guide to industrial control systems (ICS) security,,” 2011.

[71] X. Yi et al., “Security of park-lim key agreement schemes for VSAT satellite communications,” *IEEE Transactions on Vehicular Technology*, 2003.

[72] L. Cheng-Chi, “A simple key agreement scheme based on chaotic maps for VSAT satellite communications,” *IEEE Int. J. Satell. Commun*, vol. 31, n°. 5, p. 177–186, 2013.

[73] Z. Wu, Q. Pan, M. Yue et S. Ma, “An approach of security protection for VSAT network,” 2018. [En ligne]. Disponible : https://ieeexplore.ieee.org/abstract/document/8456083

[74] R. Laxhammar, G. Falkman et E. Sviestins, “Anomaly detection in sea traffic - a comparison of the gaussian mixture model and the kernel density estimator,” *12th International Conference on Information Fusion*, p. 756–763, 2009.

[75] C. Iphar, A. Napoli et C. Ray, “Detection of false ais messages for the improvement of maritime situational awareness,” *IEEE OCEANS 2015 - MTS/IEEE Washington*, p. 1–7, 2009.

[76] F. Mazzarella, M. Vespe, A. Alessandrini, D. Tarchi, G. Aulicino et A. Vollero, “A novel anomaly detection approach to identify intentional AIS on-off switching,” *IEEE Expert Syst. Appl*, p. 110–123, 2017.

[77] F. Gandon, “Graphes RDF et leur manipulation pour la gestion de connaissances,” *IEEE Habilitation à Diriger des Recherches*, 2008.

[78] A. Vandecasteele et A. Napoli, “An enhanced spatial reasoning ontology for maritime anomaly detection,” *IEEE 7th International Conference on System Of Systems EngineeringIEEE SOSE*, p. 247–252, 2012.

[79] J. Roy et M. Davenport, “Exploitation of maritime domain ontologies for anomaly detection and threat analysis,” *IEEE 2010 International WaterSide Security Conference*, p. 1–8, 2010.

[80] A. Vandecasteele et A. Napoli, “Spatial ontologies for detecting abnormal maritime behaviour,” 2012. [En ligne]. Disponible : https://ieeexplore.ieee.org/abstract/document/6263532

[81] F. Cohen, “Simulating cyber attacks, defenses, and consequences,” *Computers and Security*, 1999. [En ligne]. Disponible : http://www.blacksheepnetworks.com/security/info/misc/cohen/simulate.html

[82] B. Stewart, L. Rosa, L. Maglaras et T. J. Cruz, “A novel intrusion detection mechanism for scada systems which automatically adapts to network topology changes,” *EAI Endorsed Trans. Ind. Netw. Intell. Syst*, 2017. [En ligne]. Disponible : https://eudl.eu/doi/10.4108/eai.1-2-2017.152155

[83] B. Hallaq et A. Nickolson, “Cyran : A hybrid cyber range for testing security on ics/scada systems,” *Security Solutions and Applied Cryptography in Smart Grid*, 2016. [En ligne]. Disponible : https://www.researchgate.net/publication/305488437_CYRAN_A_hybrid_cyber_range_for_testing_security_on_ICSSCADA_systems

[84] H. Taylor, “Cyber-range,” Rapport technique, 2021. [En ligne]. Disponible : https://cybersecurityguide.org/resources/cyber-ranges/

[85] M. Yamin, B. Katt et V. Gkioulos, “Cyber ranges and security testbeds : Scenarios, functions, tools and architecture. computers and security,” *Computer Science*, 2020. [En ligne]. Disponible : https://www.semanticscholar.org/paper/Cyber-ranges-and-security-testbeds%3A-Scenarios%2C-and-Yamin-Katt/cf1c777d00eb4429ff28334ca02ebad08b27e5f6

[86] K. Tam, K. Moara-Nkwe et K. D. Jones, “The use of cyber ranges in the maritime context : Assessing maritimecyber risks, raising awareness, and providing training,” 2020. [En ligne]. Disponible : https://www.semanticscholar.org/paper/Cyber-ranges-and-security-testbeds%3A-Scenarios%2C-and-Yamin-Katt/cf1c777d00eb4429ff28334ca02ebad08b27e5f6

[87] “Cyber-mar fact sheet,” Rapport technique, 2020. [En ligne]. Disponible : https://www.cyber-mar.eu/wp-content/uploads/2019/12/Cyber-MAR_Fact-sheet_v.4.pdf

[88] HACKtheMACHINE, “Department of the navy to host virtual HACKtheMACHINE competition,” 2021. [En ligne]. Disponible : https://www.prnewswire.com/news-releases/department-of-the-navy-to-host-virtual-hackthemachine-competition-301244803.html

[89] Fathom5. Hackthemachine 2021 virtual kickoff! Youtube. [En ligne]. Disponible : https://www.youtube.com/watch?v=nb2J7ODdgb4

[90] K. Tam, K. Forshaw et K. D. Jones, “Cyber-ship : Developing next generation maritime cyber research capabilities,” *International Conference on Marine Engineering and Technology*, 2019.

[91] M. Govindarasu et C. Liu, “Cyber physical security testbed for the smart grid : Fidelity, scalability, remote access, and federation,” *CyberPhysical Systems Virtual Organization*, 2013.

[92] U. D. Ani, J. M. Watson, B. Green, B. Craggs et J. Nurse, “Design considerations for building credible security testbeds : A systematic study of industrial control system use cases,” 2019.

[93] T. Pseftelis et G. Chondrokoukis, “A study about the role of the human factor in maritime cybersecurity,” 2021. [En ligne]. Disponible : https://spoudai.unipi.gr/index.php/spoudai/article/view/2887

[94] C. Siaterlis et B. Genge, “Cyber-physical testbeds,” vol. 57, p. 64–73, 2014.

[95] H. Holm, M. Karresand et A. Vidström, “A survey of industrial control system testbeds,” *Secure IT Systems*, vol. 9417, p. 11–26, 2015.

[96] W. Zhao, Y. Peng et F. Xie, “Testbed techniques of industrial control system,” p. 61–65, 2013.

[97] T. M. R. B. Vaughn, “Addressing critical industrial control system cyber security concerns via high fidelity simulation,” p. 1–4, 2016.

[98] H. Kavak, J. J. Padilla et D. Vernon-Bido, “A characterization of cybersecurity simulation scenarios,” *Society for Modelling and Simulation International (SCS) and ACM*, p. 1–8, 2016.

[99] L. Perera et C. G. Soares, “Collision risk detection and quantification in ship navigation with integrated bridge systems,” *Ocean Engineering*, vol. 109, p. 344–354, nov. 2015.

[100] “Global maritime distress and safety system (GMDSS),” Rapport technique, 2017. [En ligne]. Disponible : https://www.fcc.gov/bureau-divisions/mobility-division/ship-radio-stations/global-maritime-distress-and-safety-system

[101] A. Bhattacharjee, “Marine radars and their use in the shipping industry,” Rapport technique, 2021. [En ligne]. Disponible : https://www.marineinsight.com/marine-navigation/marine-radars-and-their-use-in-the-shipping-industry/

[102] “Voyage data recorders,” Rapport technique. [En ligne]. Disponible : https://www.imo.org/en/OurWork/Safety/Pages/VDR.aspx

[103] R. Kantharia, “10 things to consider while using auto-pilot system on ships,” *Marine Navigation*, 2021. [En ligne]. Disponible : https://www.marineinsight.com/marine-navigation/10-things-to-consider-while-using-auto-pilot-system-on-ships/

[104] “VSAT advantage : A cost analysis of VSAT broadband versus L-band pay-per-use service.” IDIRECT, Rapport technique, 2017. [En ligne]. Disponible : https://www.groundcontrol.com/Maritime_VSAT/Marine_VSAT_Comparison.pdf

[105] “Dynamic positioning,” Rapport technique. [En ligne]. Disponible : https://www.nautinst.org/resource-library/technical-library/dynamic-positioning.html

[106] “IPMS integrated platform management system for navy vessels,” Logimatic, Rapport technique, 2019. [En ligne]. Disponible : https://www.logimatic.dk/wp-content/uploads/2019/10/Logimatic_IPMS_web.pdf

[107] "Expanding opportunities for maritime use of GNSS," Rapport technique, 2016. [En ligne]. Disponible : https://www.euspa.europa.eu/gnss-applications/segment/maritime/expanding-opportunities-maritime-use-gnss

[108] K. Cutlip, "AIS for safety and tracking : A brief history," Global Fishing Watch Web site, Rapport technique, 2017. [En ligne]. Disponible : https://globalfishingwatch.org/data/ais-for-safetyand-tracking-a-brief-history/

[109] "Echo sounder – principle, working and errors," *Cult of Sea*. [En ligne]. Disponible : https://cultofsea.com/bridge-equipment/echo-sounder/

[110] "Navigation and seamanship," 2011. [En ligne]. Disponible : http://ecoursesonline.iasri.res.in/mod/page/view.php?id=48166

[111] "Speed logs information," *Engineering360*. [En ligne]. Disponible : https://www.globalspec.com/learnmore/specialized_industrial_products/transportation_products/speed_logs

[112] W. Logger, "History of the anemometer," 2012. [En ligne]. Disponible : https://www.windlogger.com/blogs/news/history-of-the-anemometer

[113] Casual Navigation, "NMEA 0183 vs NMEA 2000," Rapport technique. [En ligne]. Disponible : https://casualnavigation.com/nmea-0183-vs-nmea-2000/

[114] Offensive Security, "Msfvenom." [En ligne]. Disponible : https://www.offensive-security.com/metasploit-unleashed/msfvenom/

[115] Infinite Logins, "Msfvenom reverse shell payload cheatsheet." [En ligne]. Disponible : https://infinitelogins.com/2020/01/25/msfvenom-reverse-shell-payload-cheatsheet/

[116] C. Finck, "Portsniffer." [En ligne]. Disponible : https://github.com/enlyze/PortSniffer

[117] W. Kelton, "International maritime organization (IMO)," 2020. [En ligne]. Disponible : https://www.investopedia.com/terms/i/international-maritime-organization.asp

[118] "About us and our members," Rapport technique. [En ligne]. Disponible : https://www.bimco.org/about-us-and-our-members

[119] "History of the NMEA," Rapport technique. [En ligne]. Disponible : https://www.nmea.org/content/MEMBERSHIP/about_nmea

[120] A. Bhattacharjee, "What is integrated bridge system (IBS) on ships ?" Maritime Navigation, Rapport technique, 2021. [En ligne]. Disponible : https://www.marineinsight.com/marine-navigation/what-is-integrated-bridge-system-ibs-on-ships/

[121] "Navigation safety regulations," Rapport technique, 2005. [En ligne]. Disponible : https://laws-lois.justice.gc.ca/eng/regulations/sor-2005-134/page-5.html

[122] Unknown, “Review of maritime transport 2016,” UNCTAD, Rapport technique, 2016. [En ligne]. Disponible : https://unctad.org/system/files/official-document/rmt2016_en.pdf

[123] “An introduction to radar watchkeeping and SOLAS requirements for ships,” Rapport technique, 2021. [En ligne]. Disponible : https://www.marineinsight.com/marine-navigation/introduction-radar-watchkeeping/

[124] “Autopilot adjustment and use,” Rapport technique. [En ligne]. Disponible : https://glomeep.imo.org/technology/autopilot-adjustment-and-use/

[125] National Marine Electronics Association, “NMEA 0183–standard for interfacing marine electronic devices,” National Marine Electronics Association, Rapport technique, 2002. [En ligne]. Disponible : https://www.plaisance-pratique.com/IMG/pdf/NMEA0183-2.pdf

[126] K. Tran, S. Keene, E. Fretheim et M. Tsikerdekis, “Marine network protocols and security risks,” 2021. [En ligne]. Disponible : https://www.mdpi.com/2624-800X/1/2/13/pdf

[127] “NMEA 0183 vs 2000 : What’s the difference ?” Rapport technique, 2016. [En ligne]. Disponible : https://www.nmeaboater.com/content/newsm/news.asp?show=VIEW&readMore=True&a=149

[128] G. Rietman, “Will NMEA 0183 be around forever ?” Rapport technique, 2018. [En ligne]. Disponible : https://rietman.wordpress.com/2018/12/12/will-nmea-0183-be-around-forever/

[129] K. Jackson, “How lockheed martin’s ’kill chain’ stopped securid attack,” *DARKReading*, 2013.

[130] M. Lockheed, “Gaining the advantage : Applying cyber kill chain methodology to network defense,” 2020. [En ligne]. Disponible : https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

ANNEXE A NOTIONS MARITIMES ET DE CYBERSÉCURITÉ

Dans cette annexe, nous commencerons par présenter plusieurs organisations ayant une forte influence dans le domaine maritime. Par la suite, nous décrirons certains systèmes maritimes, puis certains protocoles de communication réseau utilisés sur les navires. Finalement, nous présenterons certaines notions de cybersécurité.

A.1 Organisations maritimes

International Maritime Organization (IMO) L'IMO est une agence américaine fondée suite à une conférence des Nations Unies à Genève en 1948. Cette agence a pour mission d'améliorer la sécurité des expéditions marines et de prévenir la pollution marine et atmosphérique causée par les navires. L'IMO émet régulièrement des normes et des règlements pour l'industrie maritime [117].

Baltic and International Maritime Council (BIMCO) La BIMCO est une association indépendante basée à Copenhague composée d'une multitude d'acteurs oeuvrant dans le monde maritime. Le but de cette organisation est de faire la promotion de normes pour améliorer le bon fonctionnement des déplacements maritimes [118].

National Marine Electronics Association (NMEA) La NMEA est à l'origine de normes de communication largement utilisées dans le domaine maritime. L'association fut fondée en 1957 par un ensemble de détaillants de matériel électronique maritime dans le but d'améliorer leurs communications avec les manufacturiers. Dans les années 1980, la norme NMEA-0183 vit le jour et fut rapidement adoptée comme norme internationale dans le monde maritime [119].

A.2 Systèmes maritimes

Système de pont intégré (SPI) Le SPI est considéré comme étant le système électronique principal d'un navire [99]. Effectivement, le SPI permet la centralisation d'une multitude d'informations nécessaires à la navigation. En centralisant ces informations, il permet également de relier ces systèmes entre eux. Parmi ces systèmes, on retrouve généralement le pilote automatique, le radar, les *Automatic radar plotting aids* (ARPA), le gyroscope, le système de positionnement dynamique, l'ECDIS, le GMDSS et le gouvernail [120].

Electronic Chart Display Information System (ECDIS) L'ECDIS permet de visualiser numériquement les cartes maritimes. En remplaçant les cartes en version papier, l'ECDIS confère plusieurs avantages, dont notamment l'affichage en temps réel de la position du navire sur la carte et des informations sur les rives et les phares. L'utilisation d'un ECDIS sur les navires est obligatoire depuis le 1er juillet 2012 [33]. Étant donné qu'il permet l'affichage des cartes et l'affichage de différentes informations captées sur le navire, l'ECDIS joue un rôle central dans l'affichage de l'information sur le navire.

Global Navigation Satellite System (GNSS) Le GNSS affiche diverses informations utiles pour la navigation telles que la position, la trajectoire et la vitesse d'un navire. Ses applications incluent la navigation en mer, l'approche des ports, la navigation dans les ports et l'amarrage automatique. Cette technologie est largement utilisée dans le domaine maritime, elle est d'ailleurs la principale source de données de position pour l'ECDIS [107].

Compas magnétique et gyroscope Le compas magnétique et le gyroscope sont des instruments utilisés pour mesurer l'orientation du navire. Le compas magnétique indique le Nord magnétique, alors que le gyroscope indique le vrai Nord [110].

Loch Le loch est un appareil utilisé pour mesurer la vitesse d'un navire par rapport à l'eau. Anciennement, le système consistait en un chronomètre et morceau de bois qu'on lançait à l'eau. Le temps pour que le navire dépasse le morceau de bois donnait la vitesse. Le loch utilise aujourd'hui des technologies comme les ultrasons et les transducteurs Doppler [111].

Écho sondeur Le système d'écho sondeur mesure la profondeur de l'eau et protège des collisions avec les objets sous-marins. L'écho sondeur envoie des signaux sonores dans l'eau et calcule ensuite la distance des objets et du fond de l'eau par rapport au navire. De façon routinière, les navires mesurent la profondeur de l'eau dans le but de la comparer avec la profondeur affichée sur la carte. Cependant, dans les zones critiques, les navires ont besoin de cette profondeur pour assurer la sécurité du navire [109].

Anémomètre L'anémomètre mesure la vitesse et la direction du vent [112].

Global Maritime Distress and Safety System (GMDSS) Le GMDSS est utilisé à des fins de sécurité pour envoyer et recevoir des messages de détresse via des connexions satellites. Les messages de détresse contiennent le numéro d'identification et le type du navire. C'est en 1988 que l'IMO a officiellement adopté ce système [100].

Automatic Identification System (AIS) L'AIS est un système cyberphysique utilisé pour partager en continu diverses informations sur la navigation de chacun des navires. L'information est envoyée via la transmission radio et contient, notamment, le numéro d'identification du navire, sa position et sa vitesse. Depuis 2005, l'IMO oblige tous les navires de 300 tonnes et plus à utiliser l'AIS [121]. Les données AIS sont aujourd'hui généralement sauvegardées par les autorités maritimes à des fins d'investigation d'accidents et d'analyse de trafic [122].

Very Small Aperture Terminal (VSAT) Le VSAT est un outil de communication satellitaire permettant d'envoyer et de recevoir de l'information. Le VSAT peut avoir de multiples applications de communication sur un navire, telles que donner l'accès internet aux passagers, ou encore obtenir de l'aide médicale à distance [104].

Voyage Data recorder (VDR) Le VDR est utilisé pour enregistrer les déplacements de chacun des navires, et l'IMO l'a rendu obligatoire en 2002 pour tous les navires de plus de 3000 tonnes. Ce système est utilisé à des fins d'investigation, par exemple pour les accidents survenus en mer. Comme alternative au VDR, il existe une version simplifiée, soit le *Simplified Voyage Data Recorder* (S-VDR), qui sauvegarde les informations avec moins de détails [102].

Radar et Automatic Radar Plotting Aid (ARPA) Le radar est un système de détection utilisant des ondes radio qui indique la position et la vitesse des objets à proximité. Le système ARPA est utilisé de pair avec le radar pour afficher l'information sur les contacts détectés [101]. Ce faisant, ce système aide l'officier de navigation à éviter plus facilement les obstacles en les affichant visuellement et en calculant des données d'évitement de collision [123].

Positionnement dynamique (PD) Le système de positionnement dynamique permet au navire de rester sur place en agissant sur les propulseurs et les hélices. Le système informatique se sert de différents capteurs, tel que les senseurs de vent et de mouvement, pour effectuer les calculs nécessaires au maintien du navire en place [105].

Pilote automatique En plus de permettre au pilote de ne pas avoir les mains sur le gouvernail pour la durée du voyage, le système de pilote automatique permet également des économies de carburant en adoucissant les virages [124].

Integrated Platform Management System (IPMS) Système distribué utilisé à bord de sous-marins et navires, l'IPMS permet de surveiller et contrôler en temps réel plusieurs éléments cruciaux à la navigation, tels que le système de propulsion, les moteurs, les hélices, le système de gestion de l'alimentation, le système de contrôle des dommages et le système d'alarme [106].

A.3 Protocoles de communication maritime

NMEA-0183 La norme NMEA-0183, développée par NMEA dans les années 1980, est une norme de communication entre matériels maritimes, tels que le GPS, le sondeur, le radar, etc. Cette norme spécifie une communication en série pour transmettre des données sous forme de phrases émises par un émetteur, appelé *talker*, puis transmises à un ou plusieurs récepteurs, appelés *listeners*. Les phrases NMEA-0183 se construisent en utilisant des caractères ASCII avec différentes structures selon le type de données envoyées [125]. Voici un exemple de phrases NMEA-0183 utilisant le type de formateurs GGA, soit un type de phrase GPS :

$$\$GPGGA, 092750.000, 5321.6802, N, 00630.3372, W, 1, 8, 1.03, 61.7, M, 55.2, M, , *76$$

Cette phrase contient de multiples informations d'un émetteur GPS, entre autres l'heure de transmission, la latitude et longitude avec leurs directions respectives. Cette phrase aurait pu être construite par un émetteur GNSS sur un navire et envoyée vers le système ECDIS pour y afficher la position du navire à un instant donné. Les phrases NMEA-0183 n'utilisent aucune authentification, chiffrement, ni validation [126]. De ce fait, un attaquant interceptant des phrases NMEA-0183 en transmission pourra facilement connaître leur contenu.

NMEA-2000 La norme NMEA-2000 est une norme de communication entre matériels maritimes développée par NMEA et arrivée sur le marché en 1997. Basée sur une communication CAN bus, cette norme prévoit une transmission de plusieurs émetteurs vers plusieurs récepteurs, par rapport à NMEA-0183 qui ne permet qu'un émetteur pour plusieurs récepteurs. De plus, son taux de transmission de données est beaucoup plus élevé que celui de NMEA-0183 (250 kb/s par défaut), et ses phrases se construisent de façon plus compacte en utilisant un encodage binaire, par rapport aux caractères ASCII utilisés par NMEA-0183 [61]. La norme NMEA-2000 n'offre aucune protection concernant l'authentification et la confidentialité [126].

La norme NMEA-0183 est encore aujourd'hui utilisée pour la communication maritime [113]. Si sa successeure NMEA-2000 tend à prendre le dessus pour les navires récréatifs, NMEA-0183 demeure tout de même la cheffe de file pour les navires commerciaux [127]. En effet,

même si NMEA-2000 comporte des avancées technologiques considérables, NMEA-0183 est toujours restée capable de servir les opérateurs à petite et grande échelle, et la norme continue de se développer et de s'adapter année après année [128].

NMEA OneNet Annoncée pour 2021, la norme NMEA OneNet est un incrément de la norme NMEA-2000 basée sur le protocole internet IPv6 et un réseau local Ethernet *Institute of Electrical and Electronics Engineers* (IEEE). NMEA OneNet permet une communication via un réseau entre divers équipements maritimes. Par rapport aux autres normes NMEA, OneNet permet d'utiliser une bande passante largement supérieure, soit jusqu'à 10 Go/s, ainsi qu'un plus grand niveau de complexité au sein du réseau créé. Tout comme la norme NMEA-2000, les messages NMEA OneNet sont binaires. En outre, les équipements utilisant NMEA OneNet ont une option « mode sécuritaire », à travers laquelle tous les messages sont chiffrés [62].

A.4 Notions de cybersécurité

A.4.1 Chaîne de frappe

La chaîne de frappe est une méthode de modélisation d'attaque en cybersécurité [129], utilisée dans ce mémoire. La chaîne de frappe que nous utiliserons est celle de Lockheed Martin pour un réseau, qui comprend sept étapes distinctes [130].

1. Reconnaissance : Identification des cibles.
2. Armement : Préparation des armes à utiliser pour l'attaque, un logiciel malveillant par exemple.
3. Livraison : livraison de l'arme à la cible, par exemple livraison d'une clé USB contenant un logiciel malveillant à la victime.
4. Exploitation : Utilisation d'une vulnérabilité pour gagner l'accès au système ciblé.
5. Installation : Installation d'une porte arrière dans le système cible pour que l'attaquant y ait subséquemment accès.
6. Commandement et contrôle : Prise de contrôle à distance du système cible.
7. Actions sur l'objectif : Accomplissement de l'objectif principal d'attaque sur le système cible, par exemple un vol de données sensibles.