CARGO MARINE

2014 – N°7

CYBERSÉCURITÉ & MARÉTIQUE : UN ENJEU EUROPÉEN ?

Ryan **Burton**
Chargé d'études

CENTRE D'ÉTUDES STRATÉGIQUES DE LA MARINE
cesm.marine.defense.gouv.fr/

Ce document est le résultat d'une démarche d'analyse propre à son auteur. Il n'engage pas la responsabilité du Centre d'études stratégiques de la Marine.

TABLES DES MATIERES

Introduction

Juin 2011, le directeur de l'*Antwerp Port Community System* (APCS) est informé de plusieurs attaques informatiques contre le système de gestion des conteneurs du port d'Anvers. Cette tentative d'intrusion dans le système d'information de l'entreprise confirme un sentiment partagé par plusieurs sociétés de transport maritime opérant dans le port belge[1] : depuis plusieurs mois, des conteneurs disparaissent sans explication. La police belge et l'agence fédérale CERT.be sont tout de suite mises à contribution, l'enquête commence. En réalité, détourner des conteneurs en corrompant le logiciel de gestion des stocks n'a rien de nouveau. Cette astuce est même au centre de l'intrigue de la saison 2[2] de la série-fleuve *The Wire* (2003). L'épisode est révélateur de l'usage croissant par la criminalité organisée de moyens opérant depuis le cyberespace - première pour un secteur jusqu'à lors relativement épargné par la cybercriminalité.

Et pour cause, le cyberespace est devenu à la fois un enjeu géopolitique, sinon économique, pour de nombreux « agrégats[3] », mais aussi un espace truffé de vulnérabilités. Une opportunité sans précédent pour « *une criminalité méthodique, organisée, qui se développe, investit recrute et propose en sous-main des services allant d'actes de piratages graves à des actes moins répréhensibles Black SEO[4], VPN)* »[5].

Pour autant, en Europe tout du moins, la cyberdéfense[6] s'organise progressivement. En témoigne, en France, le « *Pacte défense cyber* » présenté par le ministre de la Défense Jean-Yves le Drian, en février dernier, et orchestré par l'Agence nationale pour la sécurité des systèmes d'information (ANSSI) dont les capacités se renforcent de jour en jour. D'ailleurs, ce plan national n'est pas une surprise si l'on en croit le Livre Blanc sur la Défense et la Sécurité nationale (2013), qui a ainsi élevé « *la protection contre les cybermenaces* » au rang de priorité nationale, car « elles *constituent une menace majeure à forte probabilité et à fort impact potentiel. En effet, les intrusions visant l'Etat, les opérateurs d'importance vitaux, ainsi que les grandes entreprises nationales ou stratégiques du pays sont aujourd'hui quotidiennes…*[7] »

Pourtant, dans le domaine de la « marétique », c'est à-dire de l'ensemble des systèmes d'information et de traitement de données relatifs aux activités maritimes et portuaires, la France et l'Europe

1 Christophe Lamfalussy, Comment Anvers a été piraté et s'en est sorti [en ligne]. Libre.be, 25 octobre 2013. Disponible sur : http://www.lalibre.be/economie/actualite/comment-anvers-a-ete-pirate-et-s-en-est-sorti-5269e7ea35708def0d93513c [consulté le 10/03/2014].

2 Dans cette saison, un cartel à Baltimore recrute un docker pour modifier le journal de bord de plusieurs conteneurs et s'en emparer discrètement.

3 Comme tous les espaces « libres », le cyberespace est devenu un formidable levier de productivité pour les entreprises, un espace d'échange pour les individus, mais aussi un espace de trafics, de revendications et de contestations.

4 Un référencement qualifié de « black » repose sur des techniques d'optimisation du référencement non conformes aux recommandations officielles des moteurs de recherche.

5 S.a, L'économie du cybercrime [en ligne], cybersécurité et entreprises, WarR@m, avril 2014, p.4. Disponible sur Slideshare.net/WarRam/ [consulté le 05/07/2014].

6 Au niveau étatique, la cyberdéfense est une composante de la cybersécurité, en cela qu'elle se définit comme « l'ensemble des mesures techniques permettant à un acteur de défendre dans le cyberespace les systèmes d'information jugés essentiels » - Daniel Ventre, Charles Préaux, Que couvrent les dénominations cyber liées à la défense ?. Au cœur de la Cyberdéfense, Défense et Sécurité Internationale, novembre 2013, p.10.

7 Ministère de la Défense, Livre Blanc, défense et sécurité nationale, Paris : Direction de l'information légale et administrative, 2013, p.48.

semblent à la traîne, malgré un rapport très alarmiste de l'*European Network and Information Security Agency*[8], (ENISA) publié fin novembre 2011. Selon l'agence européenne, le niveau de sécurisation de la marétique serait très faible, voire inexistant[9]. Alors que la France prend conscience de la maritimisation croissante de son économie[10], la protection du secteur du transport maritime dans le cyberespace peut-elle être ignorée plus longtemps ? Autrement dit, est-elle un enjeu à l'échelle nationale voire européenne ?

Dans un contexte où les Etats s'efforcent de reconquérir ou de réaffirmer leur souveraineté, en mer comme au sein du cyberespace, la capacité des Etat-membres, France en tête, à assurer la protection de leur domaine maritime revêt une importance cruciale. Cette étude se propose dans un premier temps, de faire un état des lieux, du niveau de dépendance des pays européens au transport maritime mais aussi du secteur maritime aux technologies numériques. L'analyse de cette « addiction » permettra de souligner que le cyberespace maritime est un territoire vulnérable, fragilisé par une prise de conscience insuffisante et une constante progression des menaces. Enfin, nous reviendrons sur le dispositif français de sécurisation de la marétique dans le cyberespace, afin de dresser des perspectives en matière de coordination, tant nationale qu'européenne.

1. L'espace maritime européen, un enjeu économique

1.1 Un secteur d'activité incontournable en Europe

« *Le monde maritime est la matrice des échanges internationaux contemporains*[11] », écrivait le Centre d'études stratégiques de la Marine (CESM) dans son Etudes Marines n°5, *La Terre est bleue*. (2013) Dès lors, on comprend que le transport maritime est un des piliers de l'économie européenne, facilitant la mobilité des marchandises vitales, telles que certaines matières premières, le gaz ou le pétrole. Plusieurs éléments illustrent ce fait. En 2010, 52 % du trafic de marchandises en Europe était assuré par le secteur maritime, soit 7 % de plus qu'en 2000. D'autre part, 90 % du commerce extérieur européen repose sur le trafic maritime[12]. Selon l'ENISA, les activités liées au secteur maritime – hors valeur des matières premières telles que le pétrole, le gaz et le poisson – contribuent entre 3 et 5 % au PIB européen.

De même, avec 22 membres disposant d'un littoral, l'activité maritime européenne repose sur plus de 1 200 ports de toutes tailles[13]. Parmi eux, trois ports de taille majeure, Rotterdam, Hambourg et Anvers, reçoivent plus de 50 % du trafic de fret conteneurisé européen à destination du reste du monde. Véritables portes sur le monde, les ports européens auront contribué à hauteur de 18 % pour le chargement du trafic maritime mondial en 2012 et 22 % pour le déchargement.

[8] Créée le 10 mars 2004 par un règlement de l'Union européenne, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a pour mission de conseiller et assister la Commission et les États membres en matière de sécurité de l'information.

[9] Cluster Martime Français, *Livre Bleu de la Marétique*, Seagital , septembre 2013, p.3.

[10] Sénat, *Rapport d'information n° 674*. Commission des affaires étrangères, de la défense et des forces Armées, groupe de travail sur la maritimisation, 17 juillet 2012.

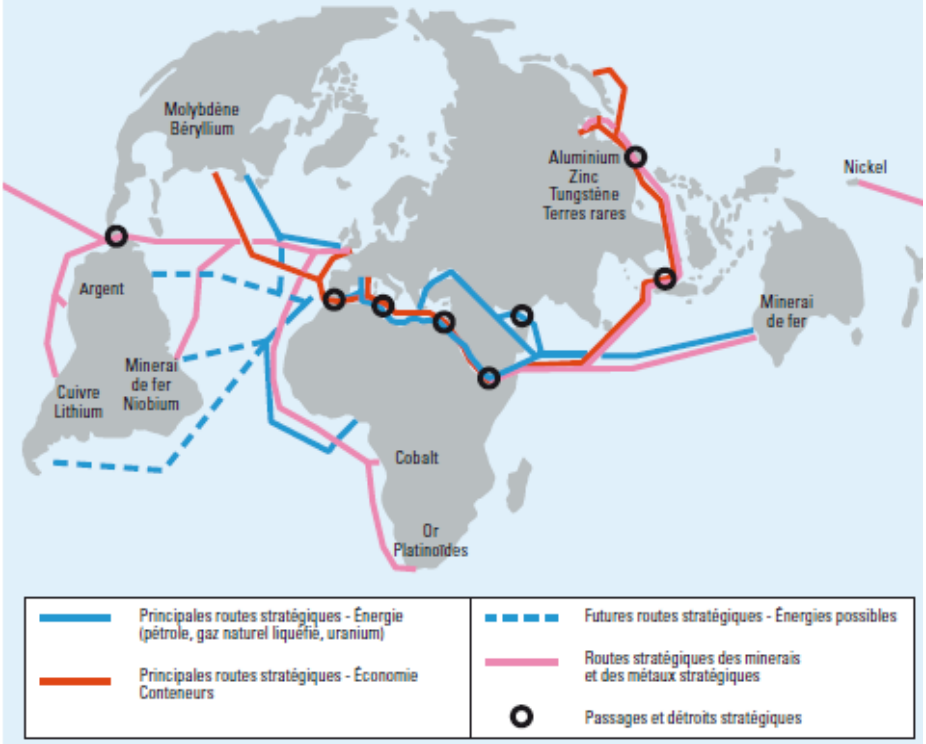
[11] Centre d'études stratégiques de la Marine, *La Terre est bleue* [en ligne]. Etudes Marines n°5, novembre 2013. Disponible sur : http://cesm.marine.defense.gouv.fr/editions/etudes-marines/etudes-marines .

[12] Ibid.

[13] European Network and Information Security Agency, *Analysis of Cyber Security aspects in the maritime sector*, novembre 2011, p.3.

Cette augmentation du transport maritime en Europe ces dernières années souligne un niveau de dépendance croissant au sein des pays membres. Une vulnérabilité confirmée lors du tsunami de mars 2011 au Japon : la destruction de plusieurs usines de fabrication de composants électroniques a mis en difficulté le secteur automobile européen. Produits en Asie, ces composants sont essentiels pour l'assemblage final assuré en France. Or, en raison de la division internationale du travail et de la production, l'Europe est aujourd'hui dépendante de l'arrivée à bon port de ces produits de transformation[14].

Cette activité s'effectue en outre dans un environnement de plus en plus privatisé et fragmenté qui entraîne un accroissement de la vulnérabilité des acteurs du secteur maritime face aux menaces opérant depuis le cyberespace.



Vulnérabilité de la France face aux flux maritimes
(Source : Compagnie européenne d'intelligence stratégique (CEIS), janvier 2012)

1.2 Une pluralité d'activités dans un environnement de plus en plus concurrentiel

Un constat s'impose d'emblée. Si le transport maritime représentait 33 % du fret transporté au sein de l'Union à 15 membres en 1970, depuis, son volume a plus que doublé et représente aujourd'hui 41 % de l'ensemble du volume transporté dans une Union à 29. De même, l'intensification des échanges maritimes a provoqué une profonde restructuration du secteur en Europe. Les mécanismes de concurrence sont devenus incontournables. La recherche d'économies d'échelle a progressivement

[14] Sénat, Rapport d'information n° 674, op. cit, p.16.

alimenté un mouvement soutenu de concentration des trafics dans le petit nombre de ports décrits plus haut (Rotterdam, Hambourg, Anvers). Parallèlement, les secteurs maritimes et portuaires se sont enrichis de nouveaux acteurs. « *Aux réseaux mondiaux des armateurs et des commissionnaires de transport s'ajoutent maintenant les réseaux des grands manutentionnaires portuaires, qui implantent leurs propres terminaux à conteneurs et orientent ainsi les flux*[15] ».

Ce phénomène de restructurations s'est accompagné d'une privatisation des infrastructures portuaires. Ainsi, à partir des années 1990, la France favorise progressivement l'investissement privé sur les quais[16]. Même constat en Allemagne et en Belgique où le secteur portuaire joue un rôle significatif dans l'économie nationale. Sur certains secteurs, entreprises et pôles portuaires se trouvent dans une situation de concurrence exacerbée qui bouleverse le paysage maritime européen et force l'ensemble de ses acteurs à dégager de plus en plus de gains de productivité.

1.3 Un recours au numérique de plus en plus important

C'est dans ce contexte que le recours au numérique devient incontournable. Comme nombre d'activités économiques, l'émergence de l'informatique et des nouvelles technologies de l'information et de la communication (NTIC) représentent un incroyable levier en matière de productivité. A partir des années 1990, ces technologies se sont progressivement imposées dans toutes les activités maritimes, « *de la navigation à la propulsion, de la gestion du fret, au contrôle du trafic maritime*[17] ». En Allemagne, où la concurrence entre les ports d'Hambourg, de Wilhelmshaven et de Brême est très forte, ces derniers ont commencé, dès les années 1980, à mettre en place leurs propres systèmes d'information (SI)[18]. Parmi les outils numériques les plus utilisés, l'Internet est en première place[19], ce qui place le secteur en situation de vulnérabilité face aux menaces opérant depuis le cyberespace. D'autant plus que, selon *Le livre Bleu de la Marétique*, publié par le CMF (2013), si 38 % des acteurs du maritime utilisent à cette date une solution numérique dédiée à leur métier, elles sont pour la plupart difficilement interopérables[20].

Car la vulnérabilité des systèmes employés par le secteur maritime s'explique par des systèmes informatiques ou automates très spécifiques à cette activité. Le rapide développement de l'informatique et les nombreux problèmes inhérents à l'automatisation du secteur, ont ainsi conduit les intégrateurs et les concepteurs de logiciel à se détourner des questions de sécurité. Cet écart entre le niveau d'interconnexion des systèmes et leur niveau de sécurité a généré d'immenses vulnérabilités, notamment dans le domaine portuaires, où un nombre croissant de systèmes de contrôle et d'acquisition de données (SCADA) sont connectés à l'internet sans aucune considération de sécurité informatique, et parfois alors même que cette connexion n'est absolument pas nécessaire pour leur fonctionnement.

---

[15] Conseil national des transports, *Le transport maritime, un avenir pour l'Europe*. Dossier n°6, Observatoire des politiques et des stratégies de transport en Europe, octobre 2004, p.3.

[16] *Ibid*, p.35.

[17] European Network and Information Security Agency, *Analysis of Cyber Security aspects in the maritime sector*, novembre 2011, p.3.

[18] Conseil national des transports, Le transport maritime, un avenir pour l'Europe, op. cit. p.11.

[19] En fait, le cyberespace est à l'Internet ce que l'espace maritime est à la surface des mers navigable.

[20] Cluster Maritime Français, *Le livre Bleu de la Marétique* [en ligne]. Seagital, mai 2012, p.6. Disponible sur : http://www.seagital.com/wp-content/themes/seagitalawards2013/docs/livre-bleu-V-finale.pdf [consulté le 19/04/2014].

Le secteur maritime se retrouve ainsi face à un problème complexe : la fragmentation du paysage économique, la privatisation de nombreux acteurs et la numérisation croissante de l'activité sans considération pour la sécurité des systèmes d'information placent les opérateurs et les Etat-membres dans une situation de vulnérabilité accrue quand le cyberespace est propice au développement d'activités malveillantes.

2. Le cyberspace maritime, un territoire vulnérable

2.1 Des systèmes d'information vulnérables

A bien des égards, le niveau de vulnérabilité du secteur maritime dans le cyberespace n'est pas sans rappeler le secteur de l'énergie avant l'attaque du ver *Stuxnet* en 2009. L'affaire est même devenue un cas d'école en matière de lutte informatique. Introduit[21] dans le complexe d'enrichissement d'uranium iranien de Natanz[22], le ver, conçu pour infecter le logiciel WinCC-7 qui contrôlait les automates du complexe, réussit à détruire par une combinaison de commandes fausses, une centaine de centrifugeuses destinées à enrichir l'uranium U235[23]. Cet épisode dramatique pour le programme nucléaire iranien, souligna combien les SCADA[24] étaient vulnérables aux attaques informatiques. Il en va de même pour les systèmes d'information et de traitement de données du secteur maritime qui n'ont pas été créés pour fonctionner dans un environnement ouvert et hostile.

Ces dispositifs sont omniprésents dans les systèmes de combats, dans les systèmes de gestion des plateformes (propulsion, électricité), dans les systèmes « métiers », tels que le refroidissement des cales d'un chalutier ou les systèmes liés à la navigation et aux communications.

La plupart de ces dispositifs ont été élaborés par une génération d'informaticiens, parfois d'électromécaniciens, à une époque où la question de la sécurité informatique ne se posait pas. Ainsi, ces systèmes reposent sur des programmes simples, parfois obsolètes, conçus pour évoluer dans des réseaux fermés, loin de toute menace. D'autre part, "*ces systèmes échappent au périmètre des responsables de la sécurité des systèmes d'information (RSSI), qui se contentent d'ailleurs bien trop souvent d'appliquer les mêmes recettes qui fonctionnent sur les réseaux*", précise Emmanuel Dupont, RSSI chez Holcim France Benelux[25]. Ces vulnérabilités sont accrues par la réduction du nombre de personnes à bord des bâtiments, l'utilisation croissante de systèmes informatiques standards pour des raisons de coûts et d'interopérabilité, l'interconnexion grandissante des systèmes ainsi que par l'exigence d'information « en temps réel partagée » qui augmentent la complexité de ces dispositifs[26].

---

[21] Sebastien Sebt, *Nucléaire iranien : le "patient zéro" du virus Stuxnet identifié* [en ligne]. France 24, 21 novembre 2014. Disponible sur : http://www.france24.com/fr/20141121-stuxnet-virus-patient-zero-kaspersky-lab-iran-enquete-nucleaire-foolad/ [consulté le 26/11/2014].

[22] En réalité, Stuxnet aurait probablement été installé comme une mise à jour d'un autre virus lui même présent dans l'un des systèmes SCADA commandé par la centrale iranienne. Pour assurer cette opération, les attaquants auraient donc dans un premier temps infecté plusieurs fournisseurs de systèmes industriels iraniens.

[23] Richard Clarke, Robert Knake, *Cyberwar*. Boston : HarperCollins, Janvier 2012, p.294.

[24] Un système SCADA, en anglais *Supervisory Control And Data Acquisition*, est un système de contrôle et d'acquisition de données, c'est-à-dire un système de télégestion permettant de traiter en temps réel un grand nombre de mesures et de contrôler à distance des installations techniques.

[25] Ryan Burton, *Au commencement, il y avait Stuxnet* [en ligne]. Blog le Monde selon Kaboul, janvier 2014. Disponible sur : http://lemondeselonkaboul.tumblr.com/post/74714199722/usa-au-commencement-il-y-avait-stuxnet [consulté le 20/04/2014].

[26] Délégation aux affaires stratégiques (DAS), *Cyberespace et milieu maritime*. Observatoire du monde cybernétique, mars 2014, pp.17-21.

Dès lors, on comprend mieux pourquoi, fin 2013, des chercheurs de Micro Trend ont réussi à pirater un système d'identification automatique (SIA) - système d'échanges automatisés de messages par radio VHF - permettant aux navires et systèmes de surveillance du trafic maritime de connaître l'identité, le statut, la position et la route d'autres navires. Avec seulement 700 euros d'équipement, le groupe de chercheurs a été capable d'intercepter le signal radio d'un navire, de modifier virtuellement sa route pour faire apparaître sur l'écran de la *Lloyld's List Intelligence*, le mot « *Pwned* »[27]. Plus récemment, une étude de la société NCC Group (2014) révélait qu'un des principaux produits ECDIS[28] (*Electronic Charts Display Information System*) du marché présenterait des vulnérabilités dans son processus de maintien en condition opérationnelles (MCO)[29].

En réalité, 80% de la marétique repose sur des technologies sans fil, radio HF ou satellites, outils longtemps considérés comme « *inattaquables car trop complexes à pirater*[30] ». Aujourd'hui, il n'en est rien. Une simple connexion internet, 30 euros d'équipements électroniques et un ordinateur suffisent à un groupe de hackers expérimentés pour accéder à la position de navires de commerce. 300 euros d'électroniques supplémentaires[31] et il devient possible de détourner le signal d'un cargo, comme l'ont démontré les chercheurs de Micro Trend. Sans parler du champ de possibilités offert à un Etat désireux de s'engager dans une opération militaire. Certes, le piratage d'un SIA n'est qu'un exemple parmi tant d'autres. Néanmoins, il illustre parfaitement le degré de vulnérabilité de systèmes qui n'ont pas été conçus pour fonctionner dans un environnement ouvert.

3.2 Une prise de conscience insuffisante face à une menace grandissante

En réalité, « *il semblerait que le paradigme a changé mais pas les mentalités*[32] » : en témoigne le rapport de l'ENISA de 2011 qui révèle l'importance du chantier et la prise de conscience insuffisante du secteur. En 2011, le ton se veut alarmant et les mots durs. L'agence écrit : « *le faible niveau de conscience général inquiète […] Il est la conséquence d'un faible sentiment d'urgence combiné à une préparation inadéquate aux risques du cyberespace*[33] ». Deux ans après, le *Livre Bleu de la Marétique* du Cluster Maritime Français reflète parfaitement cette absence d'intérêt pour la cybersécurité maritime. Amer, l'auteur du blog de cybersécurité *Si Vis Pacem* écrit : « *Alors que le cœur du sujet est bien la notion de système de transports intelligent, la pauvreté en matière de cybersécurité laisse pantois*[34] ».
S'il inquiète, ce retard peut s'expliquer : la cybersécurité est un sujet complexe qui s'inscrit dans un vaste périmètre peuplé d'agents tant privés que publics. Reste que depuis une décennie, on assiste à

[27] Dave Lee, *Ship trackers "vulnerable to hacking", experts warn* [en ligne]. BBC News, 22 octobre 2013. Disponible sur : http://www.bbc.com/news/technology-24586394 [consulté le 20/04/2014].

[28] L'ECDIS est un dispositif de visualisation des cartes électroniques et d'information qui permet de fédérer tous les éléments de positionnement (sondeurs, GPS, centrales inertielles etc.), la cartographie, les systèmes de communications et les systèmes de navigation automatiques.

[29] NCC Group, Preparing for Cyber Battleships – Electronic Chart Display and Information System Security, 2014, 10 P.

[30] S.a, *l'ENISA vous mène en bateau* [en ligne]. CNIS Mag, 21 décembre 2011. Disponible sur : http://www.cnis-mag.com/l%E2%80%99enisa-mene-la-securite-en-bateau.html [consulté le 07/03/2014].

[31] S.a, l'ENISA vous mène en bateau [en ligne], op. cit.

[32] European Network and Information Security Agency, *Analysis of Cyber Security aspects in the maritime sector*, novembre 2011, p.8.

[33] *Ibid*, p.8.

[34] S.a, *Livre bleu de la marétique et cybersécurité martitime* [en ligne]. Si vis Pacem, 25 décembre 2013. Disponible sur : http://si-vis.blogspot.fr/2013/12/livre-bleu-de-la-maretique-et.html [consulté le 20/04/2014].

une sophistication croissante des attaques informatiques. L'affaire du port d'Anvers n'a en effet rien d'une fiction : entre 2011 et 2012, il est le théâtre d'un étrange ballet, qui mêle attaques informatiques, ingénierie sociale, criminalité organisée et guerre de gangs. Pendant une année, un cartel, basé aux Pays-Bas, aurait embauché plusieurs hackers pour s'introduire dans le système de suivi et de contrôle du port et repérer les conteneurs d'apparence légitime où se trouvait la drogue en provenance d'Amérique du Sud. Une fois fait, le groupe n'avait plus qu'à s'emparer de la cargaison à la sortie du dépôt[35]. Cette opération extrêmement complexe reposait sur plusieurs vulnérabilités du dispositif de cybersécurité du port. Dans un premier temps, le groupe de hackers a réussi à installer un programme enregistreur de frappe, grâce à un hameçonnage par email. Suite à l'attaque, l'entreprise qui gère les entrepôts a renforcé son pare-feu, mais sans succès, les pirates ayant déjà accès au système[36].

Par ailleurs, le détournement du pétrolier *Enrico Ievolli* en 2011 au large de la Somalie prouve que certains groupes de pirates se sont parfaitement appropriés le cyberespace. D'après un article de la *National Defense Review*, ces flibustiers 2.0 ont attaqué le pétrolier italien en connaissant parfaitement la position du navire et l'absence d'équipe de protection embarquée (EPE), et se sont guidés en utilisant le SIA du navire à un moment où aucune force occidentale n'était en mesure d'intervenir rapidement sur le lieu de l'attaque[37].

3.3 Quel dispositif pour le cyberespace maritime européen ?

L'ensemble de ces exemples soulignent que si la sécurisation du cyberespace maritime est un enjeu pour nombre d'Etat-membres tels la France, les Pays-Bas ou encore l'Allemagne, la perspective d'un dispositif de protection européen semble peu probable. L'importante disparité, tant des moyens que des stratégies, ne facilite pas le compromis entre les membres de l'Union mais, plus encore, la divergence d'approche fondamentale entre chaque pays en matière de sécurité dans le cyberespace rend complexe une réponse commune. D'un côté, les pays du nord de l'Europe sont opposés à toute réglementation dès lors qu'elle semble remettre en question cet espace de liberté et de l'autre, la France et la Grande-Bretagne souhaitent une application plus contraignante du droit international ainsi que l'adoption d'un comportement vertueux afin d'établir la confiance entre Etats. Dès lors, même si l'ENISA a vu son mandat renouvelé en 2013 avec de nouvelles prérogatives, une coopération régionale contraignante n'a que très peu de chance d'émerger. En effet, chaque tentative de progrès sur le thème de la cyberdéfense ne réussit qu'à mettre en exergue les différentes analyses qui existent entre les Etats[38], manière de rappeler que la cybersécurité est fondamentalement un enjeu de souveraineté.

La réponse à ce stade semble se situer au niveau national, « *seul échelon* », explique Michel Baud, *« où le pouvoir politique est capable, au-delà de la capacité d'analyse de la menace, d'orienter la stratégie en matière de cyber et de définir les différents moyens à y consacrer*[39] ». Reste que le

[35] Christophe Lamfalussy, Comment Anvers a été piraté et s'en est sorti [en ligne], op. cit.

[36] Alex Pasternack, *To move drugs, traffickers are hacking shipping containers* [en ligne]. Motherboard, Vice Magazine. Disponible sur : http://motherboard.vice.com/blog/how-traffickers-hack-shipping-containers-to-move-drugs [consulté le 20/04/2014].

[37] Michael Frodl, *Pirates exploiting cybersecurity weaknesses in maritime industry* [en ligne]. National Defense, mai 2012. Disponible sur : http://www.nationaldefensemagazine.org/archive/2012/May/Pages/PiratesExploitingCybersecurityWeaknessesinMaritimeIndustry.aspx [consulté le 10/04/2014].

[38] Esteral Consulting, Etude sur la cyberdéfense et la cybersécurité au sein des institutions européennes. Delegration aux affaires stratégiques, novembre 2011, p.33.

[39] Michel Baud, *Cyberguerre, en quête d'une stratégie.* Focus stratégique n°44, Laboratoire de la Recherche sur la Défense, IFRI, mai 2013, p.27.

chemin est encore long : il n'existe pas aujourd'hui en France, de dispositif spécifique au secteur maritime, ce dernier étant traité comme les autres domaines concernés par la cybercriminalité par des services spécialisés au sein de la Police Nationale ou de la Gendarmerie. Une voie serait à explorer, celle de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI). Créée en 2011 sous la direction du Premier Ministre, cette agence est notamment chargée de la protection des infrastructures numériques des opérateurs d'intérêts vitaux (OIV). On peut donc imaginer, si ce n'est déjà pas le cas, que plusieurs ports, parmi les plus importants en France, rentrent à l'avenir dans la catégorie des OIV[40] et se trouvent donc au centre des attentions de l'ANSSI, au même titre qu'une centrale nucléaire.

Et il y a urgence : aujourd'hui, force est de constater que la protection de la marétique repose sur la bonne volonté des opérateurs privés, des utilisateurs, c'est-à-dire des armateurs et entreprises portuaires. Certes, une meilleure définition des normes et des standards, notamment en matière de maintien en condition de sécurité (MCS)[41] renforcerait considérablement le niveau de sécurité général. A ce titre, l'*United Kingdom Hydrographic Office* a déjà publié des standards de sécurité de l'information et du chiffrement concernant les systèmes de diffusion de cartographie de navigation avec certains distributeurs[42]. Mais la gouvernance fragmentée de l'espace maritime, qui se traduit par un manque de coordination et de moyens, freine considérablement le développement de nouveaux standards.

Conclusion

A bien des égards, l'Europe est « *une puissance maritime qui s'ignore*[43] ». Moyen d'approvisionnement incontournable, le secteur du transport maritime tient dans cet espace régional une place particulière. Devenu au fil des dernières décennies, un enjeu économique de premier ordre, il est aussi extrêmement fragmenté, concurrentiel et de plus en plus privatisé. Cette nouvelle donne économique a forcé armateurs et entreprises portuaires à avoir de plus en plus recours aux NTIC sans considération pour la sécurité des systèmes d'information. Nombre de ces systèmes qui n'avaient pas été conçus pour opérer dans un milieu ouvert, ont par la suite été connectés en réseaux, puis reliés à l'internet sans protection, ce qui génère aujourd'hui nombre de vulnérabilités critiques.

Ces multiples faiblesses proviennent d'une marétique fragile, d'un dispositif de sécurité quasi-inexistant et d'une prise de conscience trop faible au sein des opérateurs privés. Parallèlement, on observe depuis une décennie, une sophistication croissante des attaques informatiques. S'il s'agit aujourd'hui essentiellement de nuisances à l'échelle d'un pays, (cybercriminalité, utilisation du volet cyber dans le cadre d'acte de piraterie), la vulnérabilité du cyberespace maritime européen laisse le champ libre à d'autres acteurs plus redoutables.

Ainsi, l'attaque du port d'Anvers en 2011 démontre l'urgence de renforcer un dispositif de protection aujourd'hui quasi-inexistant. Pour autant, la solution ne semble pas régionale. Face au défi du

[40] Pour des raisons évidentes de sécurité, la liste des OIV est tenue secrète par les autorités françaises.

[41] La MCS définit notamment l'ensemble des actions de maintenance préventives et correctives à mener sur des systèmes numériques.

[42] Délégation aux affaires stratégiques (DAS), *Cyberespace et milieu maritime*. Observatoire du monde cybernétique, mars 2014, p.25.

[43] Pour reprendre une expression célèbre attribuée au cardinal Richelieu, *« la France est une puissance maritime qui s'ignore »*.

cyberespace, l'Europe se trouve confrontée à ses propres limites. Qui plus est, la sécurité donc la cybersécurité est fondamentalement un enjeu de souveraineté. Face à cette impasse, que faire ? En premier lieu, il paraît nécessaire de continuer à sensibiliser les acteurs privés. Puisque, le combat cybernétique est fondé sur la détection et l'exploitation des vulnérabilités de l'adversaire, il convient de renforcer les acteurs en « première ligne » de cette guerre de l'ombre. Pas seulement au niveau des fonctions RSSI pour la plupart déjà confrontées aux cyberattaques, mais également les directions générales, seules capables de donner au directeur des systèmes d'information (DSI), des moyens à la hauteur de l'enjeu et à forcer l'ensemble à prendre en compte cette dimension.

Cette tâche de sensibilisation peut sembler difficile, ingrate et insuffisante, mais elle est nécessaire pour préserver ce secteur incontournable pour l'économie européenne. Le volet étatique, avec des structures dédiées, doit venir compléter un dispositif destiné aussi à préserver notre souveraineté : dans nos économies ouvertes, le transport maritime constitue le réseau sanguin de nos civilisations.

Liste des abréviations

ANSSI : Agence nationale pour la sécurité des systèmes d'information ;

APCS : Antwerp Port Community System ;

CESM : Centre d'études stratégiques de la Marine ;

CERT : Computer Emergency Response Team ;

DSI : Direction des systèmes d'information ;

ECDIS : Electronic Charts Display Information System ;

ENISA : European Network and Information Security Agency ;

EPE : Equipe de protection embarquée ;

MCO : Maintien en condition opérationnelle ;

MCS : Maintien en condition de sécurité ;

NTIC : Nouvelles technologies de l'information et de la communication ;

OIV : Opérateur d'importance vitale ;

RSSI : Responsable sécurité des systèmes d'information ;

SCADA : Systèmes de contrôle et d'acquisition de données ;

SEO : Search engine optimization ;

SIA : Système d'identification automatique ;

TEU : Twenty Equivalent Unit ;

VHF : Very high frequency ;

VPN : Virtual private network.

Bibliographie

Ouvrages et monographies

- CLARKE Richard, KNAKE Robert, *Cyberwar*. Boston : HarperCollins, Janvier 2012, 296 p.

Documents institutionnels et sources primaires

- CENTRE D'ETUDES STRATEGIQUES DE LA MARINE, La Terre est bleue [en ligne]. Etudes Marines n°5, novembre 2013, 68 p. Disponible sur : http://cesm.marine.defense.gouv.fr/editions/etudes-marines/etudes-marines [consulté le 17/04/2014].

- DELEGATION AUX AFFAIRES STRATEGIQUES (DAS), Cyberespace et milieu maritime. Observatoire du monde cybernétique, mars 2014, pp.17-25.

- CONSEIL NATIONAL DES TRANSPORTS, Le transport maritime, un avenir pour l'Europe. Dossier n°6, Observatoire des politiques et des stratégies de transport en Europe, octobre 2004, 106p.

- EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, Analysis of Cyber Security aspects in the maritime sector, novembre 2011, 31 p.

- ESTERAL CONSULTING, Etude sur la cyberdéfense et la cybersécurité au sein des institutions européennes. Delegration aux affaires stratégiques, novembre 2011, 43 p.

- MINISTERE DE LA DEFENSE, Livre Blanc, défense et sécurité nationale, Paris : Direction de l'information légale et administrative, 2013, 160 p.

- NCC GROUP, Preparing for Cyber Battleships – Electronic Chart Display and Information System Security, 2014, 10 P.

- SENAT, Rapport d'information n° 674. Commission des affaires étrangères, de la défense et des forces armées, groupe de travail sur la maritimisation, 17 juillet 2012, 226 p.

Articles de revues

- BAUD Michel, La cyberguerre n'aura pas lieu, mais il faut s'y préparer. Politique étrangère, Dossier Internet, outil de puissance, IFRI, février 2012, pp.305-316.

- BRYANT Dennis, Marine Cybersecurity: Is Your Ship Safe ? Are you Sure ? [en ligne]. MarineLink.com, février 2013. Disponible sur : http://www.marinelink.com/news/cybersecurity-marine-your362503.aspx [consulté le 20/04/2014].

- VENTRE Daniel, PREAUX Charles, Que couvrent les dénominations cyber liées à la défense ? Au cœur de la Cyberdéfense, Défense et Sécurité Internationale, novembre 2013, p.8-11.

Documents électroniques

- BURTON Ryan, Au commencement, il y avait Stuxnet [en ligne]. Blog le Monde selon Kaboul, janvier 2014. Disponible sur : http://lemondeselonkaboul.tumblr.com/post/74714199722/usa-au-commencement-il-y-avait-stuxnet [consulté le 20/04/2014].

- CLUSTER MARITIME FRANCAIS, *Le livre Bleu de la Marétique* [en ligne]. Seagital, mai 2012. Disponible sur : http://www.seagital.com/wp-content/themes/seagitalawards2013/docs/livre-bleu-V-finale.pdf [consulté le 10/03/2014].

- LLOYD'S LIST INTELLIGENCE, *Can AIS be trusted* [en ligne]. 16 octobre 2013. Disponible sur : http://info.lloydslistintelligence.com/ais-can-no-longer-be-trusted/ [consulté le 20/04/2014].

- S.a, *l'ENISA vous mène en bateau* [en ligne]. CNIS Mag, 21 décembre 2011. Disponible sur : http://www.cnis-mag.com/l%E2%80%99enisa-mene-la-securite-en-bateau.html [consulté le 07/03/2014].

- S.a, *Livre bleu de la marétique et cybersécurité martitime* [en ligne]. Si vis Pacem, 25 décembre 2013. Disponible sur : http://si-vis.blogspot.fr/2013/12/livre-bleu-de-la-maretique-et.html [consulté le 20/04/2014].

- S.a, *L'économie du cybercrime* [en ligne]. Cybersécurité et entreprises, WarR@m, avril 2014. Disponible sur slideshare.net/WarRam/ [consulté le 05/07/2014].

Articles de presse

- LAMFALUSSY Christophe, *Comment Anvers a été piraté et s'en est sorti* [en ligne]. Libre.be, 25 octobre 2013. Disponible sur : http://www.lalibre.be/economie/actualite/comment-anvers-a-ete-pirate-et-s-en-est-sorti-5269e7ea35708def0d93513c [consulté le 10/03/2014].

- LEE Dave, *Ship trackers "vulnerable to hacking", experts warn* [en ligne]. BBC News, 22 octobre 2013. Disponible sur : http://www.bbc.com/news/technology-24586394 [consulté le 20/04/2014].

- FRODL Michael, *Pirates exploiting cybersecurity weaknesses in maritime industry* [en ligne]. National Defense, mai 2012. Disponible sur : http://www.nationaldefensemagazine.org/archive/2012/May/Pages/PiratesExploitingCybersecurityWeaknessesinMaritimeIndustry.aspx [consulté le 10/04/2014].

- PASTERNACK Alex , *To move drugs, traffickers are hacking shipping containers* [en ligne]. Motherboard, Vice Magazine. Disponible sur : http://motherboard.vice.com/blog/how-traffickers-hack-shipping-containers-to-move-drugs [consulté le 20/04/2014].

- SEBT Sebastien, *Nucléaire iranien : le "patient zéro" du virus Stuxnet identifié* [en ligne]. France 24, 21 novembre 2014. Disponible sur : http://www.france24.com/fr/20141121-stuxnet-virus-patient-zero-kaspersky-lab-iran-enquete-nucleaire-foolad/ [consulté le 26/11/2014].

LES ÉDITIONS DU CESM

Centre de réflexion stratégique, le CESM diffuse cinq publications régulières sur la stratégie navale et les principaux enjeux maritimes :

Études marines :
revue semestrielle, véritable plongée au cœur du monde maritime (géopolitique, juridique, historique, économique…).

Cargo Marine :
études diverses et salées réalisées par le pôle Études et ses partenaires pour un point précis sur des sujets navals et maritimes.

La Hune du CESM :
tour du monde bimestriel des enjeux navals et maritimes vus par la presse et le net.

Brèves marines :
chaque mois, un éclairage synthétique sur des thèmes historiques, géopolitiques et maritimes.

Les @mers du CESM :
veille maritime bihebdomadaire de la presse et du net.

Rendez-vous sur notre site internet :
cesm.marine.defense.gouv.fr

Rejoignez le CESM sur :