



Comité Toulon Provence Corse

FICHE DOCUMENTAIRE IFM n° 7/16

Objet : Le monde maritime face à la cybercriminalité

Préambule

Un rapport du Sénat de juillet 2012 fixait les priorités nationales en matière de cyber-défense et de protection des systèmes d'information, en mettant logiquement l'accent sur la sécurité nationale et les organismes de la Défense nationale. En France, l'ensemble de ces problèmes est géré par l'Agence nationale de sécurité des systèmes d'information (ANSSI), créée en juillet 2009, qui dépend directement du Premier ministre.

Le monde maritime est plus que jamais une cible pour les cybercriminels, qu'il s'agisse des navires désormais largement informatisés, des installations portuaires ou encore du transport de marchandises, par conteneurs notamment, voire d'espionnage industriel. Le Bureau Maritime International (BMI) affirmait en 2014 : « *Le transport et la logistique maritimes sont le prochain terrain de jeux des pirates informatiques* ».







Si au plan des forces - et donc des marines - militaires la réaction face à ces nouvelles menaces a été relativement rapide (en France : Livre Blanc sur la Défense et la Sécurité nationale de 2008, aux USA le Cyber Command), il en va autrement du monde du transport maritime qui a attendu 2014 pour voir le BMI tirer la sonnette d'alarme. L'Agence européenne de cyber-sécurité (European Network and Information Security Agency) (ENISA), créée en 2004, n'a publié un premier rapport sur la menace au plan maritime qu'en décembre 2011, l'année où les installations de contrôle des conteneurs du port d'Anvers ont été piratées par un cartel de la drogue...

Le constat initial de l'ENISA (décembre 2011)

L'agence rappelait en exergue que les cyber-menaces concernent l'ensemble des secteurs industriels dont le fonctionnement dépend de systèmes utilisant les techniques informatiques de communication (Information & Communications Technology) (ICT). Elle constatait que dans le secteur maritime le niveau d'alerte face à cette menace était bas, voire inexistant. Elle recommandait enfin que les systèmes ICT soient conçus au départ pour lutter contre la menace cybernétique et que les règlements maritimes soient amendés pour que, au-delà des aspects physiques de sûreté et de sécurité, la cyber-menace soit prise en compte. Le directeur de l'agence Udo Helmbrecht était clair : « *This report positions maritime cyber security as a logical and crucial step in the global protection efforts of ICT infrastructures* ».

SECTEUR MARITIME

> les infrastructures sensibles face aux cybermenaces

INFRASTRUCTURES SENSIBLES	SYSTÈMES D'INFORMATION UTILISÉS	RISQUES EN CAS DE CYBERATTAQUE
Infrastructure portuaire 	Maintenance des navires	Perte de la marchandise
Navire de pêche 	Gestion automatique des installations (mécanique, carburant...)	Retard d'approvisionnement
Navire marchand 	Gestion automatique de la logistique (gestion des containers...)	Perte de contrôle du navire
Grand navire de tourisme 	GPS et cartes maritimes électroniques	Contrôle maritime faussé
Bâtiment militaire 	Système d'alerte incendie	Déclenchement constant : altération de l'image de l'entreprise
Câbles sous-marins et satellites 	AIS : système d'échanges d'informations sur l'identité d'un bâtiment, sa position, sa route	Vol de données
	Système de combat	
	Télécommunications	

Menace sur les navires

Les navires sont exposés à deux types de menaces par intrusion dans leurs systèmes informatiques : l'espionnage commercial et le sabotage. Dans le premier cas le concurrent indélicat, qui dispose par ailleurs de l'information de position du navire par l'AIS (Automatic Identification System), accède aux données du manifeste cargaison et le cas échéant se procure ainsi les taux de fret. Dans le second cas le pirate prend le contrôle de la passerelle, par exemple via le SCADA (Supervisory Control and Data Acquisition) qui permet le traitement à distance en temps réel des senseurs du navire et le pilotage des installations techniques.

Les exemples de cyber-attaques ne manquent pas. Des pirates somaliens sont ainsi parvenus à pénétrer les systèmes informatiques d'une compagnie de transport maritime pour identifier les navires peu sécurisés ayant une cargaison de valeur. Une plateforme pétrolière a été infiltrée provoquant une inclinaison dangereuse conduisant à sa fermeture temporaire.

L'attaque d'un super porte-conteneurs est naturellement une angoisse chez les experts en cyber-défense, lorsque l'on pense que ces géants, truffés de systèmes d'information ultrasophistiqués, tous potentiellement attaquables, peuvent transporter jusqu'à 20.000 conteneurs dont la valeur se situe entre 2 et 4 milliards de dollars.

Nous avons traité par ailleurs (voir FD n° 1.15 du 7 janvier 2015, parue dans la Revue Maritime) le problème de l'utilisation des cartes électroniques vectorielles (Electronic Navigational Chart) dont la tenue à jour est effectuée par un centre de coordination régional qui transmet les informations sous forme cryptée, sans pour autant éliminer le risque d'une intrusion malveillante avec les conséquences que l'on peut imaginer : piratage, détournement, abordage, échouement, blocage de chenal ou d'entrée de port, etc... Des chercheurs de l'Université du Texas ont en effet démontré en juillet 2013 qu'il était possible de modifier le cap d'un navire en interférant avec son signal GPS.



Les chantiers de construction navale, c'est le cas notamment pour les marines de guerre mais pas uniquement, s'attachent à développer des moyens pour contrecarrer cette cybercriminalité maritime et, par exemple, disposent à terre d'experts qui surveillent les flux d'informations qui transitent vers le navire.

Menace sur les installations portuaires

Si l'on excepte les sites nucléaires, les ports sont avec les aéroports des cibles privilégiées pour les cybercriminels. Leurs objectifs vont du vol de données commerciales au piratage de technologies, en passant par la déstabilisation de sites industriels, voire la mise en place d'un attentat.

L'exemple des Américains, qui se sont tout particulièrement intéressés au problème, est une excellente façon d'appréhender le problème. Partant du constat que le pays exploite plus de 300 ports avec des mouvements de cargaisons dont la valeur atteint 1300 milliards de dollars chaque année, ils sont arrivés à la conclusion que leurs infrastructures maritimes, échine dorsale de leur économie, constituait une cible préférentielle pour les hackers. En décembre 2015 le Congrès a donc voté une loi faisant de la cyber-sécurité une priorité dans leurs ports et confiant au « Department of Homeland Security » (DHS) la mission de rédiger des directives nationales à l'usage de toutes les administrations et les différentes industries impliquées. L'examen attentif de la situation a montré le manque flagrant de coordination entre ces différentes entités face à la menace. Le port de Los Angeles avec ses 27 terminaux n'avait pour sa part pas conduit d'évaluation de sa vulnérabilité face à une attaque d'envergure, pas plus qu'il ne disposait d'un plan pour réagir dans un tel cas.

Les marines militaires

Les marines militaires modernes mettent en œuvre des unités à la pointe de la technologie, qui utilisent des systèmes d'information complexes et largement interconnectés, longtemps considérés comme impénétrables mais désormais confrontés à une menace d'intrusion et de cyber-attaque.

D'une manière plus générale, de nos jours, toute opération militaire comporte un volet cyber et la défense du cyberspace est devenue à cet égard une nécessité prioritaire. Il s'agit notamment

de se prémunir contre la pénétration des réseaux et les prises de contrôle à distance, voire la destruction d'infrastructures essentielles.

Notre Marine nationale, quant à elle, s'est dotée en septembre 2015 d'un centre spécialisé dans la lutte contre les cyber-attaques. Le Centre Support Cyberdéfense (CSC), installé à Toulon et à Brest, qui est chargé de garantir la capacité des unités navales et aéronavales à détecter et analyser les menaces cyber, en identifiant ses conséquences techniques et opérationnelles, et à les traiter pour préserver l'intégrité des systèmes de combat. Au plan de l'industrie navale la protection contre les cyber-attaques de la multitude de systèmes interconnectés présents sur les unités en construction fait l'objet d'une attention toute particulière des industriels. C'est dans cet esprit que le concepteur-constructeur DCNS propose le nouveau concept ACCESS, pour « Afloat Common Computing Evolutive and Secure System ».

Les liaisons satellitaires

Le champ d'application des satellites dans le domaine maritime est en développement constant. Il s'agit bien entendu en toute priorité des télécommunications et des échanges de données, on vient de le voir. Mais ils participent aussi largement à la sécurité maritime qui est en constante amélioration, le navire restant, malgré l'augmentation du trafic, un mode de transport dont le taux d'accidents est parmi les plus bas. Le nombre de naufrages, tous types de navires confondus, a été divisé par 8 en un siècle, entre 1910 et 2010. L'apport des satellites, en matière de recherche et de secours en mer a aussi été décisif. Enfin, au cours des dernières décennies, notamment face à la menace terroriste, les satellites ont été utilisés de manière extensive pour la surveillance des activités maritimes et l'observation des océans.

Citons, en restant loin de l'exhaustivité, les systèmes de télécommunications (Iridium, Inmarsat, Globalstar, O3B,...), les systèmes de suivi et de contrôle tels que le LRIT (Long Range Identification and Tracking) que les Etats-Unis ont rendu obligatoire en 2006 pour leur flotte de commerce, le Sat-AIS - déjà cité - pour le contrôle du trafic maritime, les systèmes d'alerte et de sauvetage (SSAS : Ship Security Alert System, Cospas-Sarsat) ou encore Saral (suivi des balises Argos). S'y ajoutent bien sûr tous les systèmes à vocation militaire, de télécommunications (Syracuse, Telcomarsat, Skynet,...) et de renseignement.

Tous ces systèmes sont désormais incontournables, ils participent au quotidien des gens de mer, à l'amélioration de leur travail, de leur rentabilité et à leur sécurité, mais ils sont autant de cibles pour les cybercriminels, en attendant que ces derniers ne se tournent, si l'on peut dire, vers l'avenir, en piratant les satellites eux-mêmes, à moins que ce ne soit déjà le cas...

Gestion de la cybermenace au sein de l'Union Européenne

Dans un contexte mondial en constante évolution en ce qui concerne les nouvelles menaces environnementales, la politique de sécurité de l'UE a dû s'adapter, c'est le cas pour le terrorisme en général et les cyber attaques en particulier. Dès 2008, l'Union a formulé une stratégie en matière de cybersécurité en privilégiant la coopération internationale, et c'est ainsi que l'ENISA a vu son rôle se renforcer en la matière.

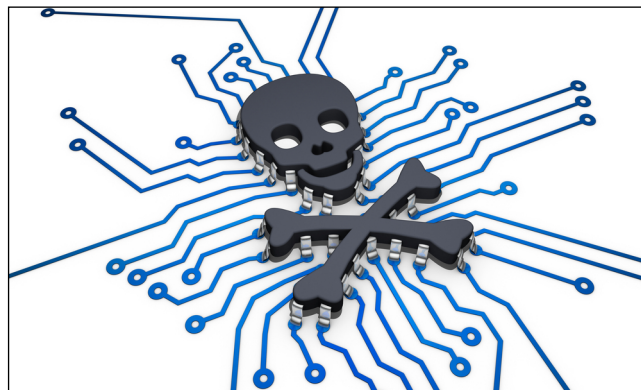
Par ailleurs, à l'été 2016, le Parlement européen a approuvé les premières règles de cybersécurité à l'échelle européenne. Ces normes communes renforcent la coopération entre les pays de l'UE et aident à prévenir les attaques contre les infrastructures interconnectées, puisque les incidents relatifs à la cybersécurité revêtent plus que jamais un aspect transfrontalier qu'une protection fragmentaire et unilatérale ne permet pas de contrôler.

La directive européenne 2016/1148 du 6 juillet 2016 « *concernant les mesures destinées à assurer un niveau commun de sécurité des réseaux et des systèmes d'information dans l'UE* » est entrée en vigueur le 8 septembre de cette année. Et les Etats membres ont jusqu'au 9 mai 2018 pour transposer la directive dans leur législation nationale.

En conclusion

Qu'ils soient civils ou militaires, nombreux sont les acteurs qui gravitent dans l'orbite du maritime : navires marchands ou bâtiments de guerre, flottilles de pêche, croisières touristiques ou navigation de plaisance, installations portuaires dans leur ensemble. Tous ces acteurs utilisent de plus en plus de systèmes informatiques dont la résistance aux cyber-attaques est loin d'être optimale, et dont la protection est indispensable face aux risques environnementaux, économiques et sécuritaires. De leur côté, les cybercriminels, hautement qualifiés et motivés par l'appât du gain, voire par des enjeux politiques, mènent des attaques plus sophistiquées que jamais, obligeant les responsables informatiques à hausser régulièrement leurs niveaux d'alerte et de sécurisation.

La cyber-défense est désormais une priorité stratégique qui touche à la souveraineté nationale et dont la Défense est un acteur majeur dans ce milieu virtuel et sans frontière qu'est le cyberspace.



Définitions

Cyber-défense : ensemble des activités conduites afin d'intervenir, militairement ou non, dans le cyberspace pour garantir l'effectivité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère. La cyber-défense est à différencier de la cybercriminalité qui correspond à l'ensemble des crimes et délits, traditionnels ou nouveaux, réalisés via les réseaux numériques.

Cyberspace : le cyberspace est un domaine global constitué du réseau maillé des infrastructures des technologies de l'information (dont Internet), des réseaux de télécommunication, des systèmes informatiques, des processeurs et des mécanismes de contrôle intégrés. Il inclut l'information numérique transportée ainsi que les opérateurs de services en ligne.

Cyber-attaque : acte malveillant de piratage informatique dans le cyberspace. Les cyber-attaques peuvent être l'action d'une personne isolée, d'un groupe, voire d'un État. Elles incluent la désinformation, l'espionnage électronique qui pourrait affaiblir l'avantage compétitif d'une nation, la modification clandestine de données sensibles sur un champ de bataille ou la perturbation des infrastructures critiques d'un pays (eau, électricité, gaz, communications, réseaux commerciaux).

Sécurité des systèmes d'information (SSI) : ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des actions ou des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.