CYBER SÉCURITÉ & PARLEMENT

04 - MARS - AVRIL 2015

AUTOUR DES RENCONTRES PARLEMENTAIRES
CYBERSÉCURITÉ & MILIEU MARITIME

EDITO

Par Gilbert LE BRIS, Député du Finistère

Alors que même de grandes multinationales, pourtant particulièrement acclimatées comme Sony ou encore Orange ont été victimes de cyber-attaques, sans savoir s'en prémunir, comment des décideurs publics peuvent-ils réagir ?

Pour sortir des raisonnements binaires, il est nécessaire de définir, caractériser et comparer les risques et les réponses à y apporter. Au sein de l'Assemblée parlementaire de l'OTAN, nous consacrons beaucoup de temps à ce travail parlementaire, sans lequel aucune réponse sérieuse ne peut être apportée. C'est en ce sens que mon collègue Philippe Vitel a coordonné un rapport remarquable sur « le cyberespace et la sécurité Euro-atlantique » en 2014. Par ailleurs, les outils techniques existent également au sein de l'Alliance grâce notamment au Centre d'excellence de cyberdéfense de Talinn en Estonie.

Revenons au secteur maritime, un navire est un objet complexe, qui intègre un nombre important de systèmes d'information et de systèmes industriels qui sont de plus en plus automatisés. Ces systèmes automatiques qui sont en lien avec le monde physique (moteurs, gouvernes, production d'électricité, gestion de la cargaison) sont constitués d'équipements informatiques sensibles à toute la gamme des attaques cyber. Une cyber-attaque sur un tel objet peut avoir des conséquences majeures : naufrage, détournement, accident dans un port, pouvant conduire à des pertes humaines ou des dégâts matériels très importants (explosion, marée noire, ...). Par ailleurs ces navires s'inscrivent dans un environnement lui aussi complexe (infrastructures portuaires, trafic maritime) qui est également soumis à des menaces.

Lire la suite en page 2

Par Philippe VITEL, Député du Var

Aux pirates en mer se sont substitués les hackers. Et ces derniers espèrent tout autant que leurs homologues voler et détourner de leur cadre légal des informations, des données, et des infrastructures, afin d'en faire un usage frauduleux.

L'espace maritime français est, après celui des États-Unis, le deuxième plus vaste du monde. Il est donc un domaine privilégié de notre rayonnement et de notre influence, tant en termes économiques que militaires et diplomatiques. A titre d'exemple, 80 % des échanges commerciaux mondiaux se font actuellement par la voie des océans.

Afin de garantir la maîtrise de cet espace de puissance, la position française doit s'inscrire dans une politique plus audacieuse, qui prendra en compte les opportunités de croissance qu'offre ce domaine en pleine mutation, tout en ayant pleinement conscience des risques qui y sont liés.

Car, comme les autres domaines à forte composante économique, le milieu maritime n'échappe pas à la déferlante numérique qui est l'une des bases fondamentales de la croissance et du développement du monde contemporain. Or, comme les mers et les océans au XVIIe siècle, le numérique est un réseau connectant les continents, et il doit faire face faire à des menaces transverses.

Lire la suite en page 2

Suite et fin de l'édito de **Gilbert LE BRIS,** Député du Finistère

Nous le voyons donc, les conséquences peuvent être sérieuses et il est de la responsabilité des décideurs de donner aux acteurs du secteur les moyens de s'en prémunir. La stratégie de l'autruche n'est donc pas la bonne.

Comment alors placer le curseur afin de prendre toutes les mesures nécessaires, sans pour autant s'engager dans une course à l'échalote, motivée par notre ignorance collective ? Dans ce cas comme dans beaucoup d'autres, il est utile de regarder en arrière. Une analogie intéressante est celle de la découverte des virus biologiques à la fin du 19ème siècle. S'est alors posée la question de la lutte contre ces ennemis invisibles. La réponse peut parfaitement être adaptée à la lutte contre les menaces invisibles de notre société de la communication. Tout d'abord il fut créé des centres d'expertise, comme l'Institut Pasteur en 1888, qui visaient à disposer des meilleurs experts et installations pour mener la lutte. C'est la réponse par le haut : en ce sens, la France s'est dotée d'un pôle d'excellence cyber qui est notamment très actif en matière de sécurité maritime. Par ailleurs, il fallait également atteindre tout un chacun afin qu'ils appliquent des pratiques simples visant à limiter les épidémies. C'est la réponse par le bas, et c'est là que la diffusion des mesures d'hygiène sont devenues prioritaires, non seulement pour les spécialistes, mais également pour l'ensemble de la population. Nous disposons déjà d'un bon tissu de formations à la cyber sécurité destinées aux experts, il nous manque cependant une vrai politique de « santé publique » visant à la diffusion des mesures simples évitant la propagation des vulnérabilités liées au cyber espace. D'ailleurs l'initiative entreprise par les « Rencontres Parlementaires Cybersécurité & Milieu Maritime » ainsi que la présente lettre, vont dans le bon sens. Je pense cependant qu'il faut aller plus loin dans la sensibilisation de tout à chacun, à des mesures simples permettant de se prémunir contre les risques les plus courants.

Par ailleurs, les failles utilisées par les cyber-attaquants sont souvent le fruit d'une défaillance au stade de la conception des systèmes. Il me semble donc qu'un dernier point est la mise en œuvre d'un dispositif juridique, renforçant l'obligation de moyens pour les architectes en systèmes d'information au moment de la conception de celui-ci.

Suite et fin de l'édito de **Philippe VITEL,** Député du Var

Si l'utilisation de radars ou la numérisation des plateformes portuaires et des infrastructures maritimes facilitent et sécurisent les transports maritimes, et permettent plus globalement une meilleure efficacité et un rendement amélioré des activités maritimes, l'imbrication du numérique dans le domaine maritime pose néanmoins des questions essentielles en termes de sécurité.

Il est ainsi aisé d'imaginer les conséquences désastreuses que pourraient avoir une attaque informatique d'importance dans le système logistique d'un port, ou au sein des systèmes informatiques d'un navire militaire… Le milieu maritime doit désormais, lui aussi, se prémunir face aux risques numériques. Les enjeux sont réels, en termes d'influence et de puissance, et ne doivent pas être sous-estimés par les acteurs publics et privés.

Puissance maritime par sa taille, la France doit également l'être par les moyens qu'elle met en œuvre pour valoriser et protéger ce domaine clef.

Il y a en effet urgence à réagir et à faire coopérer les différents acteurs du milieu maritime, pour répondre de manière optimale aux différentes menaces. Une première étape a été réalisée en ce sens, lorsque l'État a élevé la cyberdéfense au rang de priorité nationale dans le Livre blanc de la défense et de la sécurité nationale de 2013. Les pouvoirs publics ont pris conscience de l'importance croissante du cyberespace à tous les niveaux opérationnels – terre, air, mer – et surtout, des nouveaux risques qu'il engendre.

Cependant, nombreux sont les efforts qu'il reste à faire pour protéger ce secteur particulier, qui contribue à notre rayonnement sur la scène internationale et à notre croissance économique. Aussi la cybersécurité en milieu maritime ne doit-elle pas être abordée sous le seul angle de la cyberdéfense, mais également être appréhendée du point de vue des acteurs économiques, locaux et nationaux.

À cet égard, il est aujourd'hui indispensable de mettre en place une stratégie de prévention auprès des acteurs du milieu maritime, afin de les préparer à anticiper et à lutter contre les risques et les menaces cybernétiques.

Rendez-vous

le 9 mars 2016

pour la deuxième édition des

Rencontres Parlementaires

CYBERSECURITE & MILIEU MARITIME

Le combat numérique au cœur des opérations : quels enjeux pour le monde maritime ?

L'espace numérique, ou le cyberespace, est devenu un espace de confrontation à part entière. La possibilité, envisagée par le Livre blanc de 2013, d'une attaque informatique majeure contre les systèmes d'information nationaux, dans un scénario de guerre informatique, constitue une menace de première importance pour notre souveraineté.

Des actions cyber de sabotage ou d'espionnage contre des réseaux et systèmes d'information jusqu'aux opérations de recrutement et de propagande par le biais d'Internet et des réseaux sociaux, l'espace numérique est un nouvel espace d'affrontement à considérer.

Confronté à cette menace toujours plus complexe, le ministère de la Défense a bien pris la mesure de ce nouvel enjeu. A travers une chaîne de commandement spécialisée et unifiée, rattachée au chef d'état-major des armées, le ministère de la Défense dispose d'une structure dédiée à la cyberdéfense depuis 2011.

Cette dernière soutient la préparation, la planification et la conduite des opérations militaires à travers l'emploi de capacités informatiques défensives ou offensives. Elles assurent l'ensemble de la défense des systèmes d'information du Ministère par une chaine de commandement opérationnelle interarmées et ministérielle spécifique. A sa tête, un officier général « cyberdéfense » est chargé de remplir deux fonctions : l'une opérationnelle au sein du Centre de Planification et de Conduite des Opérations (CPCO) pour planifier, coordonner et conduire des opérations de défense notamment suite à des incidents notables, l'autre transversale pour coordonner les travaux qui permettent nomment le développement des capacités techniques et humaines de la cyberdéfense du Ministère.

Le Centre d'Analyse en Lutte Informatique Défensive (CALID) constitue le bras armé de cette chaîne de commandement. Celui-ci est en charge de la surveillance des réseaux, de la détection des incidents et de la réaction face aux attaques.

Le CALID envoie si nécessaire, des Groupes d'Intervention Rapide sur les théâtres d'opérations pour conduire des investigations supplémentaires ou aider au rétablissement des systèmes. Un Groupe d'Intervention Rapide est déployé actuellement sur le Porte-avions Charles de Gaulle dans le cadre de sa mission au Levant, en appui de la coalition internationale.

Chaque armée a décliné une organisation dédiée à la lutte informatique défensive, en liaison directe avec le CALID.

La Marine nationale a intégré cette nouvelle dimension en prenant en compte ses spécificités de milieu. La Marine est l'armée la plus exposée aux attaques informatiques en ce qu'elle concentre à la fois une composante aérienne à part entière, des forces spéciales, des unités en mer et sous la mer et des infrastructures portuaires à terre. Elle est également dotée de matériels ultra-informatisés et automatisés, tels que les nouvelles frégates multi-missions.

Elle a mis en place une structure dédiée à la cyberdéfense, de l'état-major de la Marine aux unités, en passant par les états-majors de force. Des exercices réguliers lui permettent de tester ses dispositifs de détection, d'analyse et de réaction. L'exercice « Catamaran », conduit par la Marine nationale en octobre 2014, a ainsi intégré une composante cyber dans son scénario. Des attaques les plus proches possibles de la réalité ont été simulées. Elles visaient à désorganiser les bâtiments en affectant leurs réseaux et leur organisation. De la même manière qu'un équipage sait circonscrire un départ de feu ou secourir un blessé, sa capacité à réagir rapidement et à mettre en œuvre les réflexes adaptés à ces menaces cybernétiques a ainsi été éprouvée de manière réaliste.

Par ailleurs, une Chaire de cyberdéfense orienté autour des systèmes navals, créée en novembre 2014 et inaugurée le 6 février 2015, vise à stimuler la recherche et la formation dans ce domaine. Mise en œuvre au sein de l'Institut de Recherche de l'école navale (IRENav), sous le haut patronage de l'Officier Général cyberdéfense, elle est structurée autour de plusieurs composantes : la formation initiale et d'experts de haut niveau, la recherche, garante d'un enseignement supérieur de qualité et le développement d'un tissu industriel de premier plan. Son contenu est fortement orienté vers les aspects techniques de la lutte contre les menaces du cyberespace.

La Chaire s'appuie ainsi sur des plates-formes nécessaires à la formation, l'entraînement à la gestion de cyber attaques navales et l'expérimentation. Pour la Marine nationale, ce projet permet de développer une expertise au profit de la formation des élèves-officiers et des officiers de la Marine nationale tout en renforçant les partenariats dans le domaine de la recherche avec les industriels du monde naval et le domaine du maritime civil.

Plus largement, les réseaux informatiques représentent autant de vulnérabilités qu'il existe de systèmes d'information dans le domaine maritime : des systèmes industriels embarqués en passant par les systèmes liés à la navigation jusqu'aux infrastructures portuaires. Les réseaux informatiques et systèmes d'information ont en effet envahi le milieu maritime dans toutes ses composantes. Un nouveau terme a même été créé pour décrire ce phénomène : la « marétique », définie par le Cluster Maritime Français comme « l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des opérations relatives aux activités maritimes, fluviales et portuaires ».

Pour autant, ces nouvelles vulnérabilités, susceptibles d'être exploitées par des attaquants, ne sont pas suffisamment prises en compte. L'ENISA (European Network and Information Security Agency) considérait ainsi en 2011 que la sensibilité du secteur au sujet était « faible à inexistante ».

Le monde maritime fait apparaître principalement trois grands secteurs de vulnérabilités en matière de cybersécurité : les systèmes industriels et automates embarqués, omniprésents sur les systèmes de combat, la gestion des plateformes, ainsi que sur les systèmes métiers ; les infrastructures portuaires ; les systèmes liés à la navigation, à son contrôle et à la sécurité nautique, avec des vulnérabilités particulières autour du système de positionnement GPS et de l'Automatic Identification System (AIS).

Des actions de sensibilisation, le développement de formations et l'organisation d'exercices réguliers, doivent permettre de mieux appréhender ces vulnérabilités. L'intégration d'une composante cyber dans des exercices vient notamment d'être expérimentée par le port d'Honolulu, qui a organisé, pour la première fois, une simulation de piratage informatique de son système d'information.

Au-delà de la sensibilisation des acteurs du monde maritime, il est également nécessaire de décloisonner cet enjeu, qui dépasse le seul domaine maritime et peut concerner, par ses impacts, l'ensemble du secteur économique.

Quelques évènements récents ont ainsi permis de porter cette problématique de milieu au-devant de publics non sensibilisés. Le CyberCercle a ainsi décidé de consacrer un cycle de conférences et de débats aux problématiques liées à la cybersécurité maritime.

Ainsi, après un premier « Cybercercle » à Toulon en septembre 2014 réunissant 150 personnes, une conférence workshop à Euronaval le 28 octobre et un numéro spécial de la lettre Cybersécurité & Parlement, les premières Rencontres Parlementaires « Cybersécurité et Milieu maritime » se sont tenues le 12 février 2015 à Paris.

Vice-amiral Arnaud COUSTILLIÈRE
Officier général à la cyberdéfense
Etat-major des armées

La Marine et la cyberdéfense

Chaque jour, la Marine nationale déploie sur toutes les mers du monde des bâtiments, des aéronefs et des sous-marins pour assurer la défense de la France et de ses intérêts. Pour accomplir le large spectre de missions qui lui incombent, la Marine met en œuvre des équipements intégrant les technologies les plus avancées. Dans ce cadre, la maîtrise du cyberespace est gage d'efficacité opérationnelle.

Les navires les plus récents sont armés par des équipages optimisés moins nombreux qu'autrefois. Cela est permis par l'automatisation très poussée de tous les systèmes. Ainsi des réseaux d'automates industriels, pilotés par des SCADA (Supervisory Control And Data Acquisition : systèmes de contrôle et d'acquisition des données) sont présents en grand nombre à bord. De tels systèmes se retrouvent également dans les installations portuaires. On connaît depuis Stuxnet les vulnérabilités potentielles de ces réseaux.

Par ailleurs, les liaisons avec la terre se font le plus souvent par des liaisons satellites, ce qui permet des interconnexions avec les autorités opérationnelles, mais aussi avec l'Internet. Il existe aussi des systèmes comme l'AIS (Automatic Identification System, système d'échange automatique de données) qui relient, entre eux et avec la terre, les navires.

De plus, la navigation aujourd'hui se fait essentiellement sur des moyens informatiques et radioélectriques. La position provient en général du GPS, qui peut subir des cyberattaques (brouillage, spoofing,...) et sa consultation se fait sur des cartes électroniques elles aussi vulnérables. Cette dématérialisation de la navigation laisse imaginer des scenarii d'attaque qui pourraient rappeler dans leurs conséquences les terribles légendes des naufrageurs.

Automatisation, interconnexion, géolocalisation : tous ces apports sont très bénéfiques du point de vue de l'efficacité opérationnelle, mais agrandissent la surface d'attaque offerte aux cyber-attaquants. Cette exposition des navires doit être maitrisée.

Dans ce contexte, la Marine nationale considère que la maîtrise de la mer passe obligatoirement par la maitrise des flots numériques du cyberespace. Pour progresser, la Marine s'est dotée d'une autorité de cyberdéfense, ALCYBER (l'amiral cyberdéfense). Son rôle est de coordonner tous les aspects concourants à la cyberdéfense : les ressources humaines, les structures opérationnelles, la surveillance des réseaux, le maintien en condition de sécurité.

Désormais, toutes les formations des équipages prennent systématiquement en compte la dimension cyber. D'une manière plus académique et avec un haut niveau d'exigence scientifique, l'École navale intègre depuis cette année une chaire de cyberdéfense dédiée aux systèmes navals. En complément, la Marine envoie des officiers suivre le master de gestion de crise cyber du pôle d'excellence Bretagne. Enfin, des cours dédiés à la cybersécurité des SCADA ont été créés.

D'un point de vue technique, un centre de lutte informatique défensive permet de suivre les configurations logicielles des navires. Par ailleurs, un centre support à la cyberdéfense sera inauguré cet été. Ses principales missions seront de consolider une doctrine adaptée au milieu maritime, de capitaliser le retour d'expériences des unités, et d'assurer l'entraînement des forces.

Sur le plan opérationnel, la Marine considère la cyberdéfense comme un domaine de lutte à part entière. Elle fait partie intégrante du processus de qualification opérationnelle des unités navigantes de la Marine nationale. Un bâtiment de combat ne part pas en mission sans avoir suivi des entraînements à quai et à la mer. Pour coordonner les actions au cours des déploiements opérationnels, un « Cyberwarfare Commander » est désigné au sein de chaque force navale.

Ainsi, la Marine s'organise pour avoir la meilleure maîtrise possible du cyberespace avec pour ambition d'obtenir et de conserver la suprématie informationnelle désormais indispensable au succès des opérations aéronavales.

Contre-amiral Anne CULLERRE
ALCYBER - Autorité de cyberdéfense
Marine nationale

La cybersécurité au Grand Port Maritime du Havre

Le port du Havre est l'un des premiers grands ports européens a avoir défini une stratégie propre à la dématérialisation des échanges d'information entre les acteurs portuaires, afin d'améliorer les temps de passage des escales et le transit des marchandises. Cette préoccupation résulte à la fois de sa position géographique comme premier port européen touché à l'import et dernier à l'export, mais est aussi la conséquence de l'accroissement mondial des échanges commerciaux du trafic maritime par conteneur.

Cette stratégie s'est concrétisée par une démarche d'innovation, de développement d'outils informatiques interconnectés à l'ensemble des acteurs professionnels portuaires. Nos processus métiers sont donc devenus très dépendants du système d'information, en particulier dans le domaine de la sûreté, la sécurité ou encore sur le plan des procédures commerciales tel le dédouanement anticipé des droits de ports.

HAROPA-Grand Port Maritime du Havre a donc initié un premier processus de formalisation de l'organisation face au risque de la cybercriminalité, lors de la mise en place du code international ISPS en 2004. Cette étape a permis de mieux appréhender la menace grâce au support de la chaine fonctionnelle SSI des ministères (HFD/FSSI/AQSSI). Pour autant, la position de l'établissement restait assez passive sur le sujet notamment sur le volet organisationnel en matière de risque SI et gouvernance.

C'est donc en 2008, qu'une démarche de certification ISO 28000 (Management de la sûreté pour la chaîne d'approvisionnement) a été entreprise pour positionner HAROPA-Grand Port Maritime du Havre comme un tiers de confiance au sein de la chaine d'approvisionnement logistique (« *supply chain* »). Cette démarche très innovante a permis au Port du Havre d'être reconnu comme l'un des premiers ports au monde certifié dans ce registre. Le système d'information s'est donc retrouvé tout naturellement au coeur de la réflexion.

Pour mieux appréhender l'analyse de la menace cyber vis-à-vis de la sureté, il a été décidé d'initier une réflexion sous l'angle de la norme ISO 27001 (Management de la sécurité de l'information), menée sur un périmètre limité aux processus opérationnels de la capitainerie et la police portuaire. Nous avons utilisé la

Les enjeux de la cybersécurité du transport maritime

Au cours des dernières décennies, les systèmes d'information (SI) ont progressivement envahi le milieu maritime : aide à la navigation et à la propulsion du navire, manutention des conteneurs, pilotage des automates permettant le remplissage et le pompage du pétrole et du gaz, etc. Un terme spécifique – la « marétique » – a même été créé pour désigner « l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'automatisation des opérations relatives aux activités maritimes, fluviales et portuaires. »

Si le secteur a longtemps fait l'impasse sur les enjeux et les risques liés à la cybersécurité, la nécessaire prise de conscience, récente mais bien réelle, semble enfin se produire. En témoignent ainsi la qualité des intervenants et l'affluence lors des 1ères Rencontres Parlementaires Cybersécurité & Milieu maritime qui se sont tenues à Paris le 12 février dernier.

Parmi les éléments du secteur les plus sensibles aux cybermenaces, relevons en premier lieu l'« informatique enfouie » (ou embarquée), constituée des systèmes industriels et des automates omniprésents sur les navires. Si ces systèmes présentent des vulnérabilités intrinsèques souvent connues, le risque s'est cependant fortement accru, notamment au travers de la maintenance en mer réalisée de plus en plus souvent à distance. Ou encore de l'utilisation croissante de systèmes informatiques « sur étagère » s'appuyant sur le protocole Internet « IP » et largement interconnectés pour permettre un traitement en temps réel des données.

Points nodaux multimodaux, les ports constituent le maillon central du transport de marchandises. Une cyberattaque majeure sur un grand port serait susceptible de désorganiser massivement toute la chaîne d'approvisionnement et, par voie de conséquence, l'économie d'un pays.

Enfin, la navigation et la sécurité nautique reposent sur de multiples dispositifs dont certains semblent particulièrement vulnérables. Ainsi, l'AIS, système universel grâce auquel un navire fournit aux autres navires ainsi qu'aux ports des informations relatives à son identité, sa position et sa route. Les faiblesses de ce protocole permettent de modifier assez facilement les données émises par un navire et de se faire passer pour un autre. Citons également l'ECDIS , dispositif embarqué d'informations et de visualisation des cartes électroniques, qui pourrait présenter des vulnérabilités permettant à un attaquant de provoquer, par exemple, l'échouage d'un navire.

Au niveau national, l'actuelle loi de programmation militaire, même si elle ne concerne qu'une partie des acteurs du transport maritime, constitue une première réponse à ces enjeux. Son article 22 se donne en effet pour objectif de renforcer la sécurité des SI les plus critiques des opérateurs d'importance vitale (OIV). Ces systèmes devront être protégés par des mesures de sécurité et seront soumis à des contrôles. Les incidents affectant ces systèmes devront en outre faire l'objet d'une déclaration à l'ANSSI.

Un arrêté sectoriel du Premier ministre, se basant sur les conclusions d'un groupe de travail réunissant les OIV du secteur, le ministère de l'écologie, du développement durable et de l'énergie, et l'ANSSI, viendra concrétiser cet objectif d'ici la fin 2015. Ambitieuse, cette démarche nationale doit se poursuivre par un travail réglementaire et normatif au niveau international, le domaine du transport maritime étant en effet, comme le cyberespace, peu tributaire des contraintes associées aux frontières nationales.

Profitons dès lors de la prise de conscience du secteur pour engager des actions fortes et durables en impliquant l'ensemble des acteurs maritimes – armateurs, autorités et opérateurs portuaires, industriels, pouvoirs publics – et les instances européennes et internationales, où s'élaborent la réglementation et les obligations applicables au secteur.

Guillaume POUPARD
Directeur général
ANSSI

méthode d'analyse de risques EBIOS et mis en relief une liste d'actifs stratégiques couvrant les moyens de télécommunications, les systèmes d'aide à la navigation, de gestion des escales, des marchandises dangereuses ou des déchets, les automates d'exploitation, les dispositifs de contrôle d'accès et de vidéosurveillance. Des risques ont été identifiés sur ces éléments et classés selon leur criticité.

Nous avons déterminé un plan d'action pour réduire, voire éliminer, les risques critiques ou majeurs, et formalisé un premier champ d'application de la sécurité en système d'information de l'établissement, qui ont permis d'améliorer sensiblement notre capacité à réagir face à la menace cyber. Nous avons bénéficié du soutien appréciable de spécialistes issus de l'ANSSI et de la DRRI qui nous ont aidés à mieux structurer notre démarche en sensibilisant nos utilisateurs et nos informaticiens sur l'existence réelle des menaces. Depuis, nous cherchons à mieux intégrer la réflexion en amont de nos projets informatiques, avec une sensibilisation récurrente de nos personnels en matière de cybercriminalité.

Il reste néanmoins beaucoup d'efforts et de travaux d'harmonisation à mener dans ce domaine, du fait d'un vaste panel d'acteurs, de tailles d'entreprises, d'organisations et des perceptions face au risque immatériel très différentes. La fiabilité d'un port repose donc sur un renforcement de la sécurisation globale des systèmes d'information.

Les systèmes portuaires deviennent d'ailleurs un élément stratégique du dispositif du guichet électronique national pour la dématérialisation des flux déclaratifs d'entrée et sortie des navires des ports européens. Les parties prenantes impliquées dans ces échanges devront rapidement partager la même culture face au risque de la cybercriminalité, y compris à l'échelle européenne et mondiale, pour favoriser l'émergence des bonnes pratiques en matière de sécurisation des échanges d'information internationaux.

Jérôme BESANCENOT
Chef du Service du Développement des SI
Grand Port Maritime du Havre

La cybersécurité selon le Secrétariat général de la mer

Le cyberespace et la mer sont les moteurs de la croissance de demain : il suffit de regarder les efforts consentis par la Chine dans ces deux domaines pour s'en convaincre. Par menace, les marins songent évidemment à la piraterie. Dans le cyberespace, la notion de pirates n'est pas inconnue. Si les attaques y sont virtuelles, elles peuvent néanmoins avoir des conséquences bien réelles et provoquer un préjudice financier ou commercial, mais également humain ou environnemental. Le monde maritime n'a pas connu, pour l'heure, d'attaque cyber majeure mais le risque est bel et bien présent. On peut recenser trois types de menaces. En premier lieu, les vulnérabilités des systèmes d'information, notamment ceux reliés à Internet, permettent le ciblage de navires, de personnes ou de marchandises à des fins criminelles. On peut d'ailleurs s'étonner que certaines informations, comme la position des navires, soient disponibles en source ouverte. Par ailleurs, le manque d'intégrité et de confidentialité de nombreux systèmes permet aisément de les leurrer, de les intercepter ou de les usurper. Il devient alors possible de dissimuler l'identité réelle d'un navire aux autorités de contrôle ou d'approcher un navire ciblé sans attirer son attention. Enfin, la vulnérabilité des systèmes de contrôle et d'acquisition de données n'est plus à démontrer : un cheval de Troie ou une bombe logique placés à l'occasion d'une opération de maintenance peuvent, par exemple, entrainer la neutralisation de l'appareil à gouverner dans les phases portuaires critiques.

Nous avons une occasion unique d'anticiper ces menaces. Pour les navires, et les normes associées, le niveau international semble le plus pertinent. L'OMI s'est saisie des questions de cybersécurité, inscrites à l'ordre du jour de la session de 2015 comité MARSEC. Il s'agit avant tout de renforcer la sécurité des systèmes existants et de promouvoir le *secured by design.* Pour sa part, l'Union européenne aborde ces menaces dans sa récente stratégie de sûreté maritime. Le niveau européen semble d'ailleurs le plus adapté pour la problématique portuaire. En 2011, le rapport de l'ENISA a notamment démontré les vulnérabilités de différents systèmes d'information portuaires. Le cas du piratage du port d'Anvers par des narcotrafiquants en est une parfaite illustration. En proposant un niveau de protection adéquate, les ports fourniraient un gage de sérieux, indispensable dans un monde très concurrentiel. La France ne doit pas demeurer passive et attendre l'arrivée de nouvelles normes, à un horizon plus ou moins lointain. Ainsi, l'ANSSI mène actuellement une étude sur la marétique qui liste les fonctions impliquées, les rares normes existantes et les vulnérabilités potentielles. Cette étude couvre l'ensemble du spectre et permettra d'établir une cartographie précise des risques et de définir des priorités. En parallèle, le SGDSN et le SGMER promeuvent le développement d'une filière des industries de sûreté maritime dans laquelle les SS2I ont toute leur place. En outre, les cybermenaces seront évoquées dans la future Stratégie nationale de sûreté des espaces maritimes annoncée par le Premier ministre lors des Assises de l'économie de la mer en décembre dernier.

Il ne faut évidemment pas exclure les principaux acteurs de la réflexion. Comme cela a été notamment fait pour les équipes privées de protection des navires, il convient de rassembler l'État et ses administrations, mais également les armateurs, les équipages, les industriels, les assureurs... Il s'agit de trouver un compromis entre sécurité des systèmes, viabilité économique et défense de nos intérêts. Si dans le domaine des attaques cyber, tout semble possible, il faut se concentrer dans un premier temps sur le « probable » pour construire progressivement une défense pragmatique et efficace. A cet égard, n'oublions pas que l'humain est souvent au cœur de la problématique cyber. Il convient donc en premier lieu de favoriser la « cyberhygiène » à tous les niveaux de la chaîne. Ne soyons toutefois pas complètement négatifs sur le facteur humain. C'est souvent lui qui permet de détecter les anomalies et d'assurer la résilience en fonctionnant en mode dégradé : suivant la situation, on appellera cela « sens marin » ou « flaire du douanier » !

LCL Barnabé WATIN-AUGOUARD
Chargé de mission sûreté maritime
Secrétariat général de la mer

Quelle menace et quelle protection

Septembre 1997, le dernier né de la flotte américaine, l'USS Yorktown, disparait subitement et ne répond plus aux sollicitations sans que la Marine américaine ne sache ce qui se passe. Après plus de 3 heures de silence, les autorités américaines s'aperçoivent que le navire a été victime d'un bug informatique qui l'a mis dans l'incapacité complète de communiquer. Cet évènement apparait aujourd'hui comme le premier d'une longue série de bugs informatiques qui peuvent toucher les systèmes d'arme modernes. Un navire moderne possède en effet plusieurs millions de lignes de code logiciel, soit autant qu'un système d'exploitation comme Android. Cette part grandissante du logiciel dans ces systèmes améliore certes leur capacité mais les expose aussi à ces erreurs de programmation qui provoquent, dans certaines conditions, des défaillances qui peuvent paraître incompréhensibles et surtout disproportionnées.

De plus, cette informatisation croissante va de pair avec une interconnexion grandissante. Des systèmes comme l'AIS (Automatic Identification System) visent à améliorer le suivi des navires, mais ce faisant, ils les relient à internet d'une façon non sûre, comme l'ont démontré les chercheurs Balduzzi et Pasta en 2013 dans l'article « Attacking Vessel Tracking Systems for Fun and Profit ». De la même façon, les services de télémaintenance permettent de réduire le nombre et les compétences des personnels à bord des navires, mais peuvent, s'ils ne sont pas bien protégés, permettre à un attaquant de prendre le contrôle du bateau à l'insu de l'équipage.

Si aucun navire civil n'a pour l'instant été détourné de cette façon, cette menace apparait aujourd'hui comme plus que plausible. Une plateforme pétrolière au large de l'Afrique aurait ainsi été rendue inopérante après avoir subi une attaque informatique. Ces menaces ne se limitent pas au seul navire mais bien à tout leur environnement. C'est ainsi que des mafieux hollandais auraient mené une attaque informatique sur le port d'Anvers afin de pouvoir prendre le contrôle du dispositif de gestion des containers : ils disposaient alors d'un moyen redoutablement efficace pour suivre les marchandises délictueuses qu'ils cachaient dans ces containers.

Tous ces évènements ne font que confirmer les risques identifiés de longue date par les experts de la DGA. En effet, des systèmes comme les frégates de type FREMM peuvent être vus comme d'immenses réseaux informatiques qui permettent à la fois de se connecter à l'Internet, de recevoir des informations de navigation mais aussi de manœuvrer l'ensemble du navire. Ces systèmes particulièrement complexes sont bien sûr déjà sécurisés mais il est indispensable qu'ils puissent résister à des attaques aujourd'hui inconnues.

LA CYBERSÉCURITÉ MARITIME SELON LE GICAN

Il ne se trouve désormais plus grand monde pour accueillir avec incrédulité le discours cyber-sécuritaire. Il reste bien quelques sceptiques dont l'attitude est moins une marque de défiance à l'égard de la réalité de la menace qu'une forme de paralysie face aux conséquences de l'adhésion à ce constat. C'est notamment vrai dans le domaine des activités maritimes, lequel reste encore très en retrait sur le sujet. Cette attitude est compréhensible car on peut légitimement être pris d'un certain vertige si l'on considère les effets économiques et organisationnels d'une prise en compte globale de la cybersécurité des navires, dès lors que l'on maîtrise peu ou mal ces sujets.

Il y a cependant urgence à prendre concrètement la menace au sérieux. Un nombre croissant d'activités se déploient dans les espaces maritimes, à commencer par le transport, mais aussi la recherche scientifique, l'exploitation des ressources des fonds marins, la valorisation des énergies marines renouvelables, l'exploitation et la protection des ressources halieutiques, sans oublier les opérations de défense et de sécurité. Ces activités ont pour caractéristique commune de mettre désormais en œuvre des outils à haute teneur technologique, incluant une part numérique croissante. Si le logiciel dévore le monde, selon la formule fameuse de Marc Andreessen, il n'oublie pas le monde maritime, qui a forgé pour désigner ce phénomène le terme de marétique, embarquant avec lui l'ensemble des cyber-risques. Ainsi, en quelques années, les cyber-incidents se sont multipliés.

Dès 2011, un rapport publié par l'ENISA, l'agence de sécurité informatique de l'Union européenne, faisait le constat sans appel d'une absence complète de prise en compte du risque cyber dans les activités maritimes. Depuis, la situation a peu évolué, même si plusieurs initiatives ont été engagées par les pouvoirs publics et les organisations professionnelles pour caractériser le risque, améliorer la prise de conscience des acteurs de la filière et proposer des réponses pragmatiques, techniquement atteignables et économiquement défendables.

Le GICAN engage sa réflexion sur les enjeux de la cybersécurité suivant trois pistes principales :

Tout d'abord la formation à tous les niveaux. Il est urgent de hisser l'ensemble des acteurs de la filière à un niveau satisfaisant de compréhension des phénomènes à l'œuvre. Formation des opérateurs et des techniciens à l'hygiène numérique ; formation des officiers à la détection et la gestion d'une crise cyber ; formation des manageurs et des dirigeants aux enjeux de la transformation numérique et des risques associés.

Ensuite la construction navale. Il est indispensable de promouvoir une approche « *Secured by design* » des systèmes embarqués. Il n'est pas envisageable, notamment, de développer des projets comme la « passerelle intelligente » ou le drone maritime sans prendre en compte, dès la conception, la question de la sécurité numérique.

Enfin, la question de la maintenance. Elle est considérée comme le vecteur externe principal des attaques contre les systèmes d'information industriels. Nous avons tous en tête le terrible révélateur que constitua à cet égard Stuxnet, malware découvert en juin 2010 qui s'attaquait aux automates programmables industriels dont sont équipés de nombreux navires. Il convient de définir des normes de contrôle des opérations de maintenance, comme c'est déjà le cas dans l'aéronautique. C'est également par la maintenance évolutive des systèmes numériques embarqués que la restauration progressive de la maîtrise de leur cybersécurité trouvera des réponses. La filière française de la sécurité numérique, et notamment les nombreuses PME innovantes qui l'animent, devraient être associées à ce chantier pour trouver des réponses à très court terme.

Afin de renforcer cette réflexion, le GICAN pourrait proposer l'élaboration d'une feuille de route numérique au profit de l'ensemble de la filière maritime. Ce projet, prenant naturellement en compte la cybersécurité, pourrait s'appuyer sur les travaux du Centre des Hautes Etudes du Cyberespace. En effet, la cybersécurité ne peut ni ne doit être perçue comme une finalité, mais bien comme une condition essentielle de la confiance sans laquelle il n'est pas d'opportunité possible dans le contexte de transformation numérique des activités maritimes.

Hugues d'ARGENTRÉ
Délégué général
GICAN

POUR LES NAVIRES DE LA MARINE NATIONALE ?

C'est pourquoi un double travail est nécessaire. Une première équipe d'experts, férus des dernières techniques d'attaque informatique, réalise un travail d'analyse de la menace en se mettant dans la peau d'un attaquant potentiel et en identifiant les différents chemins qui lui permettraient de prendre le contrôle du bateau. En parallèle, une seconde équipe va s'atteler à améliorer les capacités de détection et de protection du système en confrontant ses idées à celle des « attaquants » afin de s'assurer que les parades imaginées suffisent pour parer de futures attaques. Les résultats de ces analyses conduisent souvent à identifier de nouvelles fonctions de sécurité ou à améliorer celles existantes, ce qui nécessite une souplesse importante et explique le choix de la DGA de travailler autant avec de grands industriels qu'avec des PME.

> « Les frégates de type FREMM peuvent être vues comme d'immenses réseaux informatiques qui permettent de se connecter à l'Internet, de recevoir des informations de navigation mais aussi de manœuvrer l'ensemble du navire. »

Le travail du pôle SSI au sein de la DGA ne s'arrête pas à la sécurisation des systèmes existants et un effort significatif est réalisé pour intégrer dans toutes les architectures des futurs systèmes d'arme la prise en compte au plus tôt des problématiques de cyberdéfense. Ce travail conduit par exemple, par la société DCNS dans le cadre de l'étude amont Maldives, à intégrer dès l'origine du projet la problématique de la cyberdéfense dans la définition de l'architecture des plateformes navales de demain. Ce travail permet par exemple de définir les redondances matérielles ou logicielles à mettre en place, le cloisonnement à effectuer qu'il soit là encore matériel ou logiciel, et l'intégration complète d'une logique de surveillance et de réaction. C'est en maintenant au meilleur niveau cet effort d'innovation permanent que la DGA pourra fournir aux forces des équipements aptes à opérer même en cas d'agression informatique.

ICA Frédéric VALETTE
Chef du pôle Sécurité des SI
DGA

La démarche de cybersécurité au Grand Port Maritime de Marseille

Lors des 1ères Rencontres Parlementaires consacrées à la cybersécurité au sein du monde maritime a été abordée la démarche de cybersécurité au sein des grands ports maritimes français.

La première étape de cette démarche tient du bon sens et consiste à formaliser la cartographie des systèmes d'information d'importance vitale (SIIV) décrits dans l'article 22 de la LPM *« pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation »*. Cette cartographie permet d'identifier les vulnérabilités des biens supports (serveurs, équipements de communication, équipements d'infrastructure) aux biens essentiels (patrimoine informationnel, missions, fonctions) et d'offrir une réaction satisfaisante aux attaques actuelles incessantes mais *« de bas niveaux »*.

Cette indispensable première étape ne suffit pas pour contrer des attaques plus sophistiquées voire plus *« ciblées »*. Une doctrine doit guider les décisions à prendre et les actions à faire réaliser par les unités opérationnelles du département des Systèmes d'Information. C'est le rôle de la Politique de Sécurité des Systèmes d'Information (PSSI) qui constitue LE document de référence qui fait foi en matière de sécurité du système d'information (SSI) et montre l'importance qu'accorde la direction générale à la SSI. La PSSI a pour but de fixer les objectifs de sécurité en offrant un ensemble cohérent de principes et de règles organisationnelles et techniques répondant aux exigences des besoins en sécurité dans l'environnement et le contexte du GPMM : *« Toute réflexion relative à la SSI au sein du GPMM doit être conforme à cette politique »*. La SSI est définie comme *« la capacité d'un système d'information de résister, à un niveau de confiance donné, à des événements accidentels ou malveillants »*. Or le niveau global de sécurité étant défini par le niveau de sécurité du maillon le plus faible, il s'agit *« d'harmoniser »* le niveau de sécurité de chacun des éléments du SI.

> « Toute réflexion relative à la SSI au sein du GPMM doit être conforme à la Politique de Sécurité des Systèmes d'Information (PSSI) »

Au GPMM, 6 préceptes, en complément de la première PSSI, ont permis d'établir une défense adaptée aux menaces et d'assurer une sécurité informatique homogène :

1. Amélioration continue de la sécurité : vieille comme Deming, cette façon de penser la SSI, reprise dans la norme ISO/27001, maintient la vigilance et évite le sentiment de sécurité.

2. Analyse de risque systématique avant toute prise de décision basée sur la méthode offerte par l'ANSSI : EBIOS conforme à ISO/27005 pour traiter le risque et garantir le métier.

3. Responsabilisation de tous les acteurs du SI, c'est une chaîne de responsabilité de bout en bout, de l'utilisateur au responsable-détenteur (toujours métiers) en passant par les informaticiens, permettant de maîtriser le *« facteur humain »*.

4. Chaîne d'alerte interne au GPMM, mais aussi externe, par des relations privilégiées avec des homologues RSSI et la participation à la chaine d'alerte gouvernementale pilotée par l'ANSSI et organisée par les Hauts Fonctionnaires de défense de chaque entité ministérielle. Pour améliorer l'implication et la vigilance des agents, le site Intranet du GPMM contient un sous-site dédié à la SSI commentant, notamment, les faits divers parus dans la presse.

5. Compétences du DSI sans lesquelles rien n'est possible : connaissance parfaite des vulnérabilités par des certifications techniques sur tous les équipements en production. Des certifications ISO/27005 dans les équipes DSI suffisamment étoffées pour superviser et manager les équipements techniques, pour maintenir une surveillance des remontées de ces équipements, pour organiser l'indispensable Hotline pour les utilisateurs pendant les heures ouvrables et les astreintes pour assurer le 24/7/365 des applications métiers.

6. Défense en profondeur : C'est une démarche saine, mise en avant par l'ANSSI depuis plus de 10 ans, qui permet de gérer l'incertitude, de maintenir une inquiétude raisonnée, et surtout d'entretenir une véritable vigilance. Basée sur plusieurs lignes de défense, où chaque ligne participe à la défense globale et a un rôle à jouer : affaiblir, gêner, retarder. Chaque ligne, autonome, indépendante, dispose de ses propres moyens pour résister. Il faut 3 lignes de défense au minimum, si la première barrière est affectée par une agression, et que la seconde est défaillante pour une raison fortuite alors les conséquences sont limitées « à *coup sûr* » par la troisième ligne de défense.

Les 3 barrières du GPMM, ont été choisies : l'infrastructure, qui, pour procurer une sécurité périmétrique efficiente, doit être constamment mise à jour et dotée de moyens de contrôle de ses actifs ; le poste de travail, qu'il faut protéger, durcir mais aussi surveiller par l'utilisation d'un outil, validé par la CNIL, dédié à l'analyse comportementale du poste de travail ; et enfin l'utilisateur, averti sur l'ingénierie sociale et les comportements à risques (mot de passe fragile ou non secret, clics de curiosité), qui doit adopter une attitude professionnelle.

Les règles de sécurité, affirmées dans la PSSI, sont pertinentes pour consolider les barrières identifiées dans la défense en profondeur. Mais le « *facteur humain* » vient souvent perturber les scénarios les plus étudiés.

La mise en œuvre de la première PSSI du GPMM a souligné l'intérêt de réduire les risques induits par ce « *facteur humain* ». Outre, la chaîne de responsabilité de bout en bout, un document, destiné aux informaticiens, intitulé « *Conditions d'utilisation du Système d'Information* » décrit les cas d'usage des autorisations spécifiques pour chaque intervention dont celles depuis l'extérieur et impose, par des habilitations, l'engagement de confidentialité pour les agents disposant de pouvoirs particuliers. Ainsi chaque acteur du SI dispose des documents SSI le concernant, doit les avoir compris, doit les avoir signés pour être pleinement conscient de ses droits et devoirs. Et puisqu'il faut sans cesse reformuler pour obtenir un comportement professionnel, chaque jour, pour obtenir l'ouverture de sa session Windows, l'utilisateur accepte de respecter la charte informatique et se voit rappeler les bonnes pratiques de bases.

Il faut s'attendre au pire et s'y préparer. Cela arrivera, on ne sait pas quand, c'est tout. Les recommandations de l'ANSSI, les normes auxquelles on se conforme, les outils et les formations que l'on met en place permettent de retarder et d'amoindrir le pire. Alors on applique, on respecte, en misant sur la lâcheté de l'attaquant qui choisira une cible plus facile ou sur son impatience qui le conduira à préférer un autre chemin que celui du Système d'Information.

Paul FRANQUART
Autorité Qualifiée en Sécurité des SI
Grand Port Maritime de Marseille