CYBERCERCLE
DÉFENSE & STRATÉGIE

1ÈRES RENCONTRES PARLEMENTAIRES CYBERSECURITE & MILIEU MARITIME

12 FÉVRIER 2015, MAISON DE LA CHIMIE

sous la présidence de

Gilbert LE BRIS
Député du Finistère, Président de la Délégation française à l'Assemblée parlementaire de l'OTAN

Philippe VITEL
Député du Var, Membre de la commission de la Défense nationale et des Forces armées et de l'Assemblée parlementaire de l'OTAN

Ouverture des travaux par **Francis VALLAT**, Président d'honneur du Cluster Maritime Français, Président du Cluster Maritime Européen, et le **vice-amiral Arnaud COUSTILLIERE,** Officier général Cyberdéfense à l'état-major des armées

- « Il y a encore beaucoup à faire concernant la prise en compte des cyber risques. »
- « Les hommes, sans en avoir conscience, peuvent devenir des chevaux de Troie. »
- « Il est beaucoup plus facile de cybersécuriser un navire à sa conception plutôt que par la suite – mais ce n'est pas le seul élément qu'il faut protéger. »
- « La prise de conscience s'accélère, preuve en est du succès des dernières Rencontres, à Toulon en septembre dernier. »

- Il y a beaucoup de points communs entre l'espace numérique et l'espace maritime. Là où la mer véhicule marchandises et richesses, le numérique transporte des données. Et, comme en mer, il y a des routes, des espaces de souveraineté, et des zones grises. On perd une guerre en mer quand on en n'a pas la maîtrise, tout comme dans le cyberespace. Aussi, si le droit est en train de se structurer, nous n'avons que quelques mois pour parcourir le chemin que le monde maritime a fait en 300 ans. Le travail est conséquent, même au sein de l'Union européenne. Pour s'y retrouver, il faut revenir aux fondamentaux et bien comprendre le rôle de tous les acteurs.
- Un bateau est extrêmement dépendant des systèmes informatiques. Il est facilement attaquable, car il utilise de plus en plus d'outils informatiques, alors que les équipages experts en informatique sont trop rares. Aujourd'hui on n'attaque pas une plateforme entière, on fait plus simple : on s'attaque au système de propulsion par exemple. Les plans d'adressage IP des navires sont trouvables sur Internet. Et ils constituent une cartographie pour mener des attaques…
- Le ministère de la Défense a intégré le cyberespace comme un espace de conflictualité. Il faut apprendre à y combattre, ce qui signifie qu'il y a un ennemi capable de manœuvrer et imaginatif. Aujourd'hui la cybersécurité est devenue un enjeu national. Le Livre Blanc 2013 éclaire la posture française dans ce domaine. Au sein du ministère de la Défense, plusieurs outils sont déjà en place : le pacte Défense Cyber - 1 milliard d'€ sur la durée de la LPM - ; le pôle d'excellence Bretagne. On intègre en outre les exercices de cyberdéfense à la qualification opérationnelle des navires. Ceux-ci doivent être résilients quoi qu'il arrive. Pour continuer la mission, même en mode dégradé
- Enfin, si le vecteur de l'arme peut être informatique, il peut aussi être humain. Le social engineering fonctionne très bien. La dimension humaine est prioritaire.

Première table ronde
La cybersécurité des bateaux : des enjeux majeurs

Avec les interventions de :

- **Hugues d'ARGENTRE,** Délégué Général du GICAN
- **Eric BANEL,** Délégué Général d'Armateurs de France
- **ICA Frédéric VALETTE,** Chef du Pôle Sécurité des Systèmes d'Information à la DGA
- **Jean-Charles CORNILLOU,** Chargé de mission auprès de la direction technique du CEREMA
- **Lieutenant-colonel Barnabé WATIN-AUGOUARD,** Chargé de mission au Secrétariat Général de la Mer
- **Capitaine de corvette Nicolas MALBEC,** Adjoint Cyberdéfense, Bureau Systèmes d'Information et de Communication à l'Etat-major de la Marine

« L'étendue des menaces possibles nécessite une approche large et prospective. »

- **Il y a deux types d'enjeux :**
  - La connaissance & l'anticipation, en amont, sur la vulnérabilité et les systèmes critiques...
  - La résilience, en aval, sur les opérations de correction en mer, l'isolement, systèmes d'urgence en mer…

- Pour les armateurs, les enjeux sont commerciaux, et sécuritaires. Cargaison et navigation constituent des données gérées à terre, et qui peuvent être détournées depuis la terre – et cela durablement. Le système d'AIS, qui permet de connaître la position d'un navire en temps quasi-réel, comprend aussi de nombreuses failles que les navires eux-mêmes peuvent exploiter pour leurrer. La sécurisation de l'AIS, qui a été réalisée par la Marine nationale pour les bâtiments militaires ou douaniers, est indispensable à une échelle mondiale.

- Si la piraterie est un danger qui a été pris en compte par l'industrie navale, elle se croyait néanmoins à l'abri des cybermenaces. Contrairement à l'industrie aéronautique ou le milieu médical, elle ne dispose pas d'assurance qualité des logiciels : c'est un terreau de cyberattaques.

- La cybersécurité en milieu maritime est un problème international, car il y a un enjeu souverain de sécurité. Il est en partie traité par l'Organisation maritime internationale, mais celle-ci ne peut pas remplacer l'Organisation hydrographique internationale et l'Organisation internationale des transmissions, en ce qui concerne l'e-navigation.

- La façon dont les systèmes d'information d'un navire communiquent entre eux peut être opaque, si elle n'est pas assimilée dès la conception. Etablir une matrice des flux internes est très laborieux mais indispensable, car il faut connaître l'intégralité de ses systèmes pour en assurer la maîtrise.

« Il faut un dialogue technico-opérationnel entre marins et constructeurs. »

- Pour faire face aux cybermenaces en milieu maritime, quelques éléments de réponse ont été apportés :
  - Développer l'analyse de la menace, et des boîtes à outils pour évaluer les risques
  - Faire des audits réguliers pour prévenir et chercher les traces d'une éventuelle attaque

- Encourager les industriels à sécuriser l'ensemble de leurs processus, ensemble
- Former l'humain et établir des relations de confiance avec les sous-traitants
- Agir de concert, au niveau mondial
- Soutenir la recherche

Deuxième table ronde
La cybersécurité des infrastructures portuaires : une dimension fondamentale de sécurité

Avec les interventions de :

- **Guillaume POUPARD**, Directeur Général de l'ANSSI
- **Philippe ROUX**, Adjoint Mer du HFDS adjoint du ministère de l'Ecologie, du Développement durable et de l'Energie
- **Capitaine de vaisseau Henri de FOUCAULD**, Chef du Bureau Systèmes d'Information et de Communication à l'Etat-major de la Marine
- **Jérôme BESANCENOT**, Chef du Service du Développement des Systèmes d'Information du Grand Port Maritime du Havre
- **Paul FRANQUART**, Responsable de la Sécurité des Systèmes d'Information du Grand Port Maritime de Marseille
- **Chef d'escadron Christophe BEGARD**, Adjoint Police Judiciaire et Relations Internationales au Commandement de la Gendarmerie Maritime
- **Luc ALLOIN**, Président Directeur Général de SECURYMIND

« Le piratage d'un navire gazier en entrée portuaire serait dramatique. »

- **On peut décomposer les fonctions portuaires en quatre catégories :**
  - L'activité nautique, qui concerne les mouvements des navires (approche, escale, départ)
  - L'activité logistique, c'est-à-dire la gestion des marchandises (entrée, stockage, départ)
  - L'activité industrielle, qui fait fonctionner le port
  - L'activité humaine, interne ou externe au port

- Ces fonctions portuaires utilisent des systèmes d'information complexes et autonomes, généralement interconnectés et ouverts afin d'en tirer plus de fonctionnalités (circulation rapide et en grande quantité de l'information). Cela a pour conséquence, d'une part, de renforcer le phénomène de « cyberdépendance » des ports, mais surtout de diffuser de l'information en masse à des acteurs pas toujours concernés. Ces quatre domaines d'activités constituent donc autant de fonctions portuaires potentiellement visées et impactées par une cyberattaque.

- Un port est constitué de flux, et sa valeur ajoutée est, en quelque sorte, sa capacité à transférer ces flux, qu'ils soient matériels ou virtuels. L'informatisation des données a donc été naturelle pour les ports, mais leur cybersécurisation n'a réellement été pensée qu'à posteriori. Or, intégrer la sécurité informatique dès la conception d'un projet est aujourd'hui indispensable.

- Le milieu maritime a longtemps ignoré les problèmes de cybersécurité, même si cela tend à évoluer. Rares sont les lignes écrites dans les grands textes internationaux sur le sujet. Par exemple, la plateforme SafeSeaNet, définitivement rendue obligatoire à partir du 1er juin 2015 par la directive UE 2010-65, est un système d'échange d'informations entre les navires, les ports, les administrations et les Etats membres. Elle contient une importante quantité de données sensibles, et n'est pourtant pas pleinement sécurisée.

« Qui est propriétaire de l'information et donc, qui doit la protéger ? »

- Il existe autant de menaces externes et malveillantes, que de menaces internes, principalement dues à la simple négligence. Outre le problème posé par le *Bring Your Own Device*, l'architecture SCADA est aussi particulièrement vulnérable. La gestion des accès, dans un port, est fondamentale pour sa sécurité. Formation du personnel, contrôle des accès, surveillance lors de la maintenance et segmentation des systèmes d'information constituent alors autant d'éléments de travail pour l'avenir.

- En ce qui concerne le cadre juridique qui s'impose aux infrastructures portuaires, la Loi de programmation militaire est le vecteur d'un ensemble de mesures et de directives. Il est en outre imposé aux entreprises d'importance vitale d'avoir une PSSI : il faut connaitre ses systèmes, ses besoins en sécurité, et donc l'impact d'une attaque. enfin, il faut appliquer les principes recommandés par l'ANSSI ; la PSSI actuelle établit un certain nombre de règles basiques mais efficaces qui permettent de contrer les attaques classiques et non ciblées. Il existe aussi des démarches de certification sûreté, comme l'ISO 28000, et des méthodes spécifiques pour « connaitre et maitriser nos SI et les données ».

« Au cœur de la supply chain, le port est potentiellement un maillon faible. »

Fermeture des travaux par **Michel AYMERIC**, Secrétaire général de la Mer

- « Il y a une massification des flux, et donc une intensification de la vulnérabilité. »
- « L'action peut-être juridique, institutionnelle, à l'échelle internationale. »
- « Il faut promouvoir la sécurité lors de la conception, lors de la réception, et du fonctionnement. »
- « Il faut que tous les grands ports, européens et internationaux prennent la mesure du risque. »

Contact : Bénédicte PILLIET, Directeur - Tél : 09 83 04 05 37 - b.pilliet@defense-et-strategie.fr
Pour nous écrire : Défense & Stratégie, 135 avenue de Versailles - 75016 PARIS

LES PARTENAIRES DES #RPCyberMaritime

Cluster Maritime Français
Le Faire-Savoir Maritime
The Maritime Voice

GICAN