ILERI - DÉFENSE

La Cyberdéfense dans la Marine Nationale

Florent Corneau - Secrétaire Général d'ILERI Défense - 19 avril 2017

© MARINE NATIONALE

ILERI Défense a assisté à la conférence du 22 mars 2017 du Centre d'Etudes Stratégiques de la Marine (CESM) intitulée *La cyberdéfense dans la Marine nationale : une culture humaine et opérationnelle,* par le Capitaine de Vaisseau Vincent Grégoire, chef du bureau des opérations aéronavales à l'état-major de la Marine. Accompagné d'un officier de marine de la Chaire de Cyber Défense des Systèmes Navals, il a rappelé les menaces auxquelles était exposée la Marine nationale dans le cyberespace, véritable métamorphose de l'approche guerrière contemporaine. Il est aussi revenu sur la réelle prise de conscience de l'Etat dans ce nouveau champ d'affrontements qui a élevé la cyberdéfense au rang de priorité nationale.

Les menaces et les intérêts du cyber

En 2016, 758 millions de cyberattaques ont été relevées, soit une augmentation de 46% en un an, avec une attaque toute les quarante secondes. Plus de 24 000 attaques ont été déjouées cette même année par le Ministère de la Défense, un phénomène qui n'épargne pas la Marine nationale, et dans une plus large mesure, l'espace maritime français.

Que ce soit dans la logistique portuaire, sur les navires commerciaux et militaires, ou encore sur les câbles sous-marins, la menace cyber est partout. Aujourd'hui dans la marine commerciale, 80% des échanges d'informations se font grâce au réseau Wi-Fi ; et 75% des informations internet passent par les câbles sous-marins. Avec des systèmes embarqués et interconnectés, la capacité de nuisance des hackers est grande ; elle peut notamment toucher aux systèmes de communication, à l'aiguillage GPS ou encore aux systèmes vitaux d'un navire de guerre comme celui du refroidissement de l'eau.

La crainte de la Marine est de voir se multiplier les actions cyber liées à des groupes terroristes, comme le démontre la capacité d'action de la mouvance Etat islamique ou

encore la résurgence de la piraterie maritime, là où la Marine française opère. Ces derniers peuvent en effet provoquer la paralysie d'un groupe aéronaval, l'obstruction d'un détroit, un échouage provoquant une marée noire, ou pire, l'explosion d'une bombe cinétique.

Cependant il faut bien comprendre que le choix du cyber ne représente pas seulement une menace, mais que l'intégration des systèmes informatiques est un phénomène inéluctable. Ce n'est donc pas « la lubie d'un ingénieur de DCNS », et le choix de l'informatique a un intérêt hautement pratique permettant d'optimiser les équipages, les équipements, la vitesse et la capacité de frappe, « permettant de disposer de véritables capacités opérationnelles » notamment à bord des navires de nouvelle génération comme les FREMM[1].

Toutefois, « le recours nécessaire et massif aux Nouvelles Technologies de l'Information et de la Communication s'est fait au détriment de la sécurité », s'agissant de choix budgétaires précis et assumés.
Si la Marine française « est l'une des plus exposées, elle a pris très tôt en compte les menaces cyber ».

Quelle cybermarine française ?

L'Etat a bien compris l'opportunité ainsi que la menace que représente le cyber, et a, depuis son *Livre blanc sur la défense et la sécurité nationale* (2013), complété par la Loi de programmation militaire (LPM) de 2015[2], élevé la cyberdéfense au rang de priorité nationale.

[1] Pour plus de détails sur les nouvelles frégates de classe *Horizon* (FDA) et *Aquitaine* (FREMM) voir la note d'Henri Sallé sur note site www.ileri-defense.com

[2] Plus d'informations sur la Loi de programmation militaire de 2015 www.legifrance.gouv.fr

Grâce à la LPM qui couvre la période 2014-2019, l'Etat français a mis en place un Commandement Opérationnel de Cyberdéfense interarmées sur le modèle américain pour prévenir et contourner ces nouvelles menaces. Pour la Marine notamment, le projet a été de mettre en place des organes de réflexion et d'action pour optimiser son opérationnalité.

La mise sur pied d'un Centre Support à la Cyberdéfense (CSC) en 2015 traduit cette volonté de « concrétisation du renforcement des capacités opérationnelles en cyberdéfense »[3] pour la Marine nationale. Le CSC a pour mission de cartographier les systèmes informatiques, de développer la cybersurveillance avec une priorité de Renseignement d'Intérêt Cyber (RIC), et de promouvoir la culture cyberdéfense avec tous les acteurs de la Marine et du renseignement. Cela passe par l'anticipation de cyber attaques, par la constitution de scénarii complexes et d'identification des doctrines et retours d'expérience chez nos partenaires internationaux. Par conséquent, la Marine nationale est la seule armée qui propose de tels mécanismes pour répondre aux menaces. Le CSC devrait avoir sa pleine capacité RH et matérielle avec 54 personnes d'ici 2019.

En effet, le recrutement de personnel qualifié est un enjeu majeur dans la lutte contre les cybermenaces. De fait, la Marine se retrouve en compétition dans ce recrutement avec la société civile. Elle doit notamment former et recruter des agents hautement qualifiés dans ses rangs mais aussi sur le marché du travail. L'Etat a prévu le recrutement de 125 personnes dans ce domaine entre 2016 et 2019, et ce chiffre ne peut qu'augmenter pour répondre à une demande croissante.

Pour répondre à la demande de « réflexion », la Marine via l'Ecole navale a mis en place avec la région Bretagne et des industriels tels que Thalès et DCNS, une Chaire de cyberdéfense des systèmes navals[4]. En bénéficiant de la synergie des acteurs qui

[3] Plus d'information sur le Centre Support à la Cyberdéfense (CSC) www.defense.gouv.fr

[4] Plus d'information sur la Chaire de cyberdéfense des systèmes navals www.ecole-navale.fr

la composent, elle a pour but de fournir la Marine en travaux de recherches et en thèses sur des sujets de cyberdéfense, tout en formant les officiers ou futurs officiers de marine à ces enjeux. Malgré une période initiale allant de 2014 à 2017, le programme de la Chaire a été reconduit pour trois ans jusqu'en 2020.

Aussi, toute une littérature normative a été déployée grâce notamment au travail de l'ANSSI[5] et des différents rapports fournis au Parlement. La directive européenne *NIS*[6] adoptée en 2016 dont la transposition est pilotée par l'ANSSI oblige notamment les différents opérateurs civils comme militaires, de notifier aux autorités tout cas d'attaque cyber, dans le but de pouvoir prendre des mesures cohérentes et efficientes à l'échelle nationale et européenne.

Enfin, il convient de souligner que la Marine s'est mise en ordre de bataille et a mis en place un système vertueux d'études et d'audits SSI au commencement de l'élaboration des nouvelles générations de navires de guerre. Ainsi en intégrant la dimension sécurité du cyber dès la naissance des bâtiments, la Marine entend s'adapter au mieux aux enjeux du cyberespace. Le tout permet une nouvelle fois d'optimiser les navires en hiérarchisant les priorités matérielles en fonction des ordres de missions et de la « priorité du commandant », en adaptant la redondance et le positionnement des équipements. « La cybersécurité n'a [donc] pas un coût mais un prix ».

Par Florent Corneau,
Secrétaire Général d'ILERI Défense
Étudiant en *Bachelor* 2 de l'ILERI.

[5] ANSSI pour Agence Nationale de la Sécurité des Systèmes d'Information.

[6] Plus d'information sur la directive européenne *NIS* www.ssi.gouv.fr