Note n°48/20

10 juin 2020

Nicolas Mazzucchi
Chargé de recherche
Fondation pour la recherche stratégique

Le cyber, domaine particulier de la pensée navale

Cette note a été originellement publiée dans le numéro 17 (janvier 2020) de la revue Etudes marines*, disponible à l'adresse suivante : https://cesm.marine.defense.gouv.fr/index.php/publications/etudes-marines/432-etudes-marines-n-17-strategie*

Pour la première fois en 2019, la grande conférence annuelle DefCon incluait, pour sa 27e édition, un village nommé « Hack the Sea » dédié aux problématiques de cybersécurité dans le domaine maritime. Si ce type de manifestations est bien entendu appelé à se multiplier, c'est qu'il révèle l'importance croissante de la question cyber au sein du monde maritime – spécifiquement dénommée la marétique –, avec l'intégration toujours plus poussée de systèmes communicants dans un nombre croissant de plateformes navales. Cette vision s'étend au domaine maritime civil aussi bien que militaire puisque les navires des différentes marines ne cessent d'être confrontés aux besoins d'émettre et de recevoir des données, aussi bien à longue qu'à courte distances. Même si la problématique des communications navales n'est pas nouvelle, loin s'en faut, elle connaît un tournant majeur depuis quelques années avec la volonté affichée de disposer de capacités de combat en réseau, tant au niveau des groupes navals que des bâtiments eux-mêmes. Ces enjeux de communication trouvent aujourd'hui dans le cyberespace un nouveau domaine, offrant à la fois capacités et menaces.

Il s'agit ici de considérer le cyber dans une acception vaste, à la fois comme domaine de lutte particulier au sein de l'espace maritime mais également comme famille technologique, incluant ses développements vers la robotique autonome, l'intelligence artificielle et les objets

connectés. En effet, l'ensemble de ces technologies reposent sur une base cyber liée à un fonctionnement fondé sur l'échange de données – permanent ou non – entre plusieurs plateformes. En ce sens, de nombreux développements technologiques, actuels ou prospectifs, entrent dans cette définition du cyber au sein des forces armées. L'annonce par l'Amiral Prazuck, Chef d'état-major de la Marine nationale, de l'entrée en service de plusieurs centaines de drones (1 200) en 2030 impose de considérer les enjeux de cybersécurité liés à ceux-ci comme l'un des cœurs de leur intégration au sein des unités de la Marine. Toutefois, au-delà de l'intégration des technologies au sein des navires, la question de l'intégration du domaine cyber dans la stratégie navale se pose avec une acuité d'autant plus grande que si certains éléments semblent similaires, d'autres ouvrent de nouveaux défis.

Le cyber et la mer, les difficultés de l'intégration technologique

Intégrer une couche cyber dans des objets navigants se déplaçant sur et sous les mers est un défi technologique et économique autrement plus grand que le déploiement de réseaux de communication à terre. L'utilisation des technologies cyber a ainsi connu ces dernières années un développement exponentiel à terre, grâce à des avancées logistiques majeures liées aux réseaux à haut débit et à la popularisation des terminaux idoines. Dans certaines régions du monde, comme l'Afrique, c'est véritablement le haut débit mobile qui a permis un usage important du cyberespace sur le continent. En l'espace de dix ans, de 2007 à 2017, la part de la population mondiale utilisant Internet est ainsi passée de 20 % à près de 50 %, corrélativement aux abonnements mobiles haut débit (de 4 % à 62 % dans le même laps de temps) selon l'ONU[1]. Ce sont les réseaux (3G, 4G et bientôt 5G) ainsi que les terminaux, téléphones et tablettes qui ont permis cet essor mondial. Or ceux-ci reposent sur une capacité d'installation d'infrastructures fixes à des distances relativement limitées afin d'assurer une couverture optimale et continue. Ainsi, les antennes relais de téléphonie haut débit ont des rayons d'émission allant de quelques centaines de mètres à une trentaine de kilomètres, ce qui impose un maillage relativement serré des territoires. Identiquement, les autres protocoles de connexion sans fil à distance se voient limités : le Wifi (norme IEEE 802.11) dispose d'une portée de quelques centaines de mètres, le Wimax (IEEE 802.16) d'une dizaine de kilomètres, le Zigbee (IEEE 802.15) d'une dizaine de mètres, etc.

Dans ce contexte, le domaine maritime, par l'impossibilité d'y installer des relais de communication fixes comme c'est le cas à terre, apparaît comme bien plus exigeant pour sa connexion au cyberespace. Les plateformes maritimes vont se reposer essentiellement sur les technologies satellitaires afin de disposer de liaisons de données, que ce soit pour la communication voix et image, pour la navigation, etc. Les liaisons cyber sont ainsi opérées, en France, au travers des systèmes *Inmarsat* pour le civil, *Telcomarsat* ou *Syracuse* pour le militaire. Or les liaisons satellitaires sont, dans le domaine cyber, extrêmement minoritaires – environ 10 % des communications mondiales – du fait, principalement, de leur coût. Le cyber maritime est ainsi bien plus cher, dans la partie communication notamment, que le cyber terrestre, obligeant les systèmes d'information embarqués à traiter autant que faire se peut les informations à bord du navire[2].

[1] Données Banque mondiale et Union internationale des télécommunications.

[2] C'est partiellement cette logique qui explique que le domaine maritime ait vu la mise en service des premiers systèmes d'armes automatisés, tel le système *Aegis* aux Etats-Unis (sur celui-ci voir P. Scharre, *Army of None,* New York, Norton, 2018).

Cette situation n'empêche toutefois pas le développement très rapide d'« objets cyber flottants », bien au contraire. Le cyber, c'est la promesse de l'optimisation du fonctionnement des systèmes par l'utilisation des technologies liées à la collecte et au traitement des données. Dans ce contexte, le monde maritime apparaît comme particulièrement pertinent pour le déploiement de systèmes cyber destinés à optimiser le fonctionnement des navires. Comme tout système « industriel », un navire repose sur la capacité à traiter de la manière la plus automatisée possible un certain nombre de tâches liées à ses missions. Dans le contexte militaire, celles-ci vont de la propulsion aux missions de combat sous la mer et au-dessus de la surface. Le cyber peut, dans ce cadre, jouer un rôle d'autant plus important qu'il est adapté pour l'intégration de multiples sous-systèmes différents – un navire étant avant tout une plateforme d'accueil de systèmes – mais aussi qu'il permet des gains humains, donc des gains de place. Il s'agit ici d'un changement de paradigme fondamental dans le domaine naval puisque celui-ci a été jusqu'ici fondé sur la rareté de la communication et passe maintenant à l'abondance de la communication, du moins en local ou à courte portée. Grâce à l'automatisation poussée, les navires – militaires ou non – ont ainsi gagné en taille pour des fonctionnalités toujours plus importantes. Les FREMM actuelles disposent d'un équipage d'à peine plus de 100 marins pour un rayon d'action de 6 000 nautiques et un spectre de missions extrêmement large. Leurs ancêtres, les frégates de classe *Tourville*, avaient un équipage de près de 300 hommes pour un rayon d'action de 4 500 nautiques. Il est vrai que plus de trente ans les séparent, le temps qu'il a fallu pour entrer dans l'ère numérique. Les derniers navires entrés en service sont donc des systèmes de contrôle industriels flottants, souvent soutenus par de multiples protocoles, faisant du navire un système d'information complexe multi-capteurs ; une sorte d'usine connectée sur mer.

Dans le domaine de l'économie maritime également, les technologies cyber offrent des atouts particuliers qu'il convient de prendre en compte, en particulier quant à la prédictibilité. En effet, l'un des grands avantages de la numérisation des systèmes « industriels » est la capacité d'anticipation offerte par l'usage de données massives, donnant la possibilité de mieux anticiper les mouvements et, par là, d'améliorer la logistique mondiale, qui est essentiellement maritime. Au-delà, le navire autonome, pour lequel les travaux de réflexion sont déjà bien engagés au sein de l'Organisation maritime internationale[3], offre des promesses plus qu'intéressantes en termes de logistique du futur, avec des économies fortes en capital humain et en carburant. Toutefois l'irruption sur les mers de systèmes autonomes de grande taille ouvre de nombreuses questions en termes aussi bien de maturité technologique que de sécurité ou de responsabilité juridique, en particulier avec des systèmes qui embarqueront probablement de l'intelligence artificielle.

Au-delà du navire lui-même, avec l'évolution des missions et des besoins, l'environnement cyber-naval se conçoit toujours davantage avec l'intégration de plateformes secondaires ou déportées, comme des drones aériens ou sous-marins. Avec ces nouveaux engins, les navires de surface – et les sous-marins dans un avenir plus ou moins proche – tendent à devenir non seulement des systèmes d'information flottants mais également les cœurs d'un mini-réseau local. La multiplication des capteurs déportés dans des plateformes inhabitées, destinés à donner au navire une plus grande visibilité de son environnement, transforme ainsi le futur navire militaire – et civil selon les usages – en une passerelle pour objets connectés. De la même manière que, dans le domaine aérien, les appareils des nouvelles et futures générations (F-35, SCAF, etc.) sont conçus comme le centre d'un système autour duquel évoluent des capteurs/effecteurs autonomes, les navires du futur seront avant tout des passerelles (*gateways*) de traitement de

[3] http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx

l'Internet des Objets, faisant probablement office de *datacenters* également[4]. Cette vision est celle qui se retrouve dans le discours du Chef d'état-major de la Marine nationale quand il évoque le développement rapide des drones embarqués, lesquels peuvent, dans le domaine maritime, être dévolus à de nombreuses missions (ISR, combat, guerre électronique, guerre des mines, etc.). Grâce à des drones – en essaim ou non –, les navires de combat pourraient ainsi devenir des plateformes multi-missions étendues, capables de couvrir un territoire tridimensionnel (air, surface, sous-marin) bien plus important. Cette intégration de nouveaux capteurs-effecteurs aurait un double effet : elle offrirait une réponse – partielle – au dilemme du contrôle territorial, casse-tête de la stratégie navale, et en même temps elle créerait de nouveaux risques et enjeux stratégiques liés à la numérisation.

Stratégie navale et stratégie cyber : de nombreux points communs

Une question de territoire

Les deux milieux de la mer et du cyberespace possèdent un certain nombre de points communs. Parmi ceux-ci, la question de la permanence du contrôle d'un territoire par essence marqué par la fluidité. En effet, dans le cyber comme en mer, il est impossible de disposer d'un contrôle continu sur l'ensemble des territoires, ne serait-ce que parce qu'il est impossible d'y assurer une permanence de la présence humaine. L'immensité du territoire joue ici un rôle fondamental. Il a donc rapidement fallu opérer des choix sur ce qu'il fallait contrôler et ce qui était annexe.

L'histoire de la pensée stratégique navale a ainsi été marquée par la nécessité de défendre des lignes de communication ou des zones précises, avec la possibilité de conduire des actions offensives ponctuelles pour marquer sa supériorité. A la fin du XIX^{e} et au début du XX^{e} siècles, A. Mahan, comme J. Corbett, défend une vision de la supériorité navale fondée sur la maîtrise des lignes de communication, ainsi que sur la force militaire au service de la pérennité de ces lignes. En un certain sens – dans une perspective très historique d'ailleurs, si l'on reprend les travaux de Mahan –, la mer est vue comme un réseau dont il faut protéger les nœuds et les lignes majeures. Le cyberespace, quant à lui, repose également sur cette logique de réseau – en particulier dans la couche physique – qu'il convient de dominer pour disposer d'une supériorité techno-industrielle. Les grandes puissances du XXI^{e} siècle l'ont bien compris, et la confrontation Etats-Unis-Chine dans le cyberespace ne serait sans doute pas la même sans cette lutte pour la technologie des réseaux, illustrée en 2019 par l'épineuse question de l'acceptation de la 5G, laquelle, portée par le chinois Huawei, divise jusqu'au sein des pays de l'OTAN. Une grande différence existe néanmoins à ce stade, le caractère « naturel » (ou quasi) du réseau maritime, opposé au caractère « artificiel » du réseau cyber.

La problématique du droit des conflits armés se pose également dans le cas de l'intégration du cyber dans le milieu maritime. En effet, si l'on considère les débats tant juridiques qu'éthiques autour des systèmes autonomes – armés ou non –, il est intéressant de replacer ces derniers dans le monde maritime. L'un des principaux « freins » à l'utilisation de ces systèmes dans un contexte militaire vient de la difficulté absolue, y compris pour des humains d'ailleurs, de discriminer combattants et non-combattants dans les confits contemporains. Cette problématique, qui est prégnante en particulier sur terre, est beaucoup moins importante dans

[4] Eu égard à la problématique de la connectivité cyber, la question de la pertinence du *cloud* se pose bien plus dans le domaine naval que dans les autres domaines, d'où un traitement au plus près du capteur suivant le modèle dit *fog computing.*

le domaine sous-marin, où la plus grande partie des mobiles y circulant – et des hommes qui les mettent en œuvre – sont militaires. Il est ainsi fort probable que le domaine sous-marin soit le premier à accueillir des systèmes autonomes, éventuellement armés, ne serait-ce qu'à des fins d'expérimentation. En effet, la variété des missions qui peuvent être confiées à ces systèmes (renseignement, lutte sous la surface, guerre des mines, etc.) permet d'augmenter fortement les capacités d'une force navale, en termes si ce n'est de performances, du moins de permanence, permettant par là de résoudre – partiellement – l'un des grands problèmes de la stratégie navale.

Au-delà de cette question du cyber au sein de la stratégie navale elle-même, il appartient également de considérer que le cyberespace repose en grande partie sur un territoire maritime. En effet, l'écrasante majorité des communications du cyberespace transite *via* les câbles sous-marins, dont le nombre ne cesse d'augmenter. En raison de la facilité de mise en œuvre de ces infrastructures, qui permettent de disposer de débits importants à des coûts raisonnables, la mer a très rapidement pris le pas sur l'espace comme territoire de transit des communications mondiales. Il en découle une appréhension maritime – particulière certes – de celles-ci. De fait, l'appréhension stratégique des câbles sous-marins se fait non seulement suivant une logique qui rappelle celle, terrestre, des pipelines – ce sont des infrastructures posées au fond des mers suivant des tracés fixes –, mais aussi suivant une vision navale, avec l'enjeu de la pose et de la protection. Néanmoins, le paradoxe de la communication en mer fait que si le cyberespace s'appuie majoritairement sur le domaine maritime, les navires ont accès à ce même cyberespace au travers des systèmes spatiaux. Cette particularité induit une vision singulière des enjeux de la conflictualité cyber sur ou sous les mers.

Le cyber-combat naval

Avec la numérisation progressive des bâtiments, le cyber-combat naval tend à passer d'une logique de disruption – comme dans le domaine cyber en général – à une logique d'immobilisation/sabotage. Avec des navires – militaires mais aussi civils – à l'automatisation poussée, les risques liés à la perte de l'un ou l'autre des sous-systèmes d'information du bâtiment deviennent de plus en plus critiques. Avec un navire connecté de manière multiple, par plusieurs types de protocoles, eux-mêmes sans fil, il devient théoriquement possible de lancer des attaques ciblées plus pernicieuses.

Les systèmes cyber embarqués obéissent plus, en termes stratégiques, à la logique de l'informatique de production (OT) qu'à l'informatique de traitement (IT). Les plateformes navales sont ainsi des objets industriels complexes, dont la durée de vie se compte en décennies, qui doivent abriter des systèmes cyber de capteurs/effecteurs dont l'obsolescence est bien plus rapide. Il en découle un paradoxe technologique, bien connu dans le monde industriel, entre la structure portante, dont la sécurité vient de sa stabilité, et le système de contrôle, qui est par nature toujours en évolution. L'enjeu de la mise en cybersécurité du système embarqué doit ainsi prendre en compte cette vision spécifique, avec des mises à jour fréquentes, complexes au regard de la connectivité en mer. En outre, la vision du navire comme un ensemble cyber-industriel est également à approfondir avec l'apparition programmée de ces appendices cyber que seront les différents drones aériens, marins ou sous-marins. Ceux-ci, qui utiliseront les protocoles de communication sans fil entre eux ou avec le navire porteur, rapprochent ce dernier d'une usine connectée type 4.0[5].

[5] Les usines du futur dites, selon l'appellation allemande, « 4.0 » font un usage extensif des données dans la gestion du fonctionnement de l'entité, y compris par le recours à de multiples robots et cobots comme capteurs ou effecteurs.

Eu égard à l'importance des communications sans fil, mais aussi à l'utilisation, pour la transmission de données, du spectre électromagnétique (AIS, GPS, UHF, etc.), il est possible d'envisager une fusion des domaines cyber et guerre électronique au niveau tactique naval. Les capacités de guerre électronique embarquées – y compris au niveau de drones – devraient dans ce contexte devenir prégnantes pour dénier l'accès aux systèmes de transmission de données, offrant une supériorité en termes de *command and control* à celui qui disposerait de telles capacités. L'US Navy encourage depuis de nombreuses années les programmes de drones aériens embarqués (X-47, ScanEagle, etc.) disposant de capacités d'emport modulables, ouvrant la voie à de tels types de systèmes de guerre électronique au sein des flottes.

Les systèmes navals autonomes, civils et militaires, seront des cibles de choix pour les agresseurs cyber. En effet, leur dépendance aux données qu'ils produisent par leurs propres capteurs ou reçoivent (GPS, AIS) les rend sensibles à des formes sophistiquées de brouillage ou de leurrage. L'introduction programmée d'intelligence artificielle pour l'aide à la conduite du navire et à l'accomplissement de ses missions ouvre également des opportunités d'attaque puisque qu'elle peut elle aussi faire l'objet d'attaques spécifiques (injection de code, détournement des schémas de reconnaissance, etc.).

Pirates et corsaires, vers de nouvelles menaces

Au-delà des acteurs étatiques traditionnels de la conflictualité maritime, d'autres dangers menacent les navires militaires ou civils *via* le cyberespace et pourraient modifier l'appréhension de la menace. Depuis quelques années, le domaine cyber a vu apparaître des catégories d'acteurs dont les comportements rappellent l'histoire des conflits navals. Les pirates sont ainsi bien connus des marins, mais jusqu'à présent ils sont limités par une asymétrie de moyens et d'objectifs qui donne l'avantage aux forces régulières. Dans le cyberespace, eu égard à l'apprentissage rapide des techniques d'attaque sophistiquées et aux gains potentiels, les acteurs malveillants non étatiques se multiplient. Les cyber-pirates qui obéissent à une logique financière – ce sont donc en ce sens des cybercriminels ou des cybermafieux suivant leur niveau d'organisation – pourraient être tentés de s'attaquer aux navires de commerce pour les rançonner (détournement, immobilisation, etc.) vu les sommes en jeu dans la logistique maritime mondiale[6]. Même s'ils ne représentent qu'un danger limité pour les forces militaires, leur impact sur le monde maritime pourrait être important dans les années à venir, en cas de mauvaise appréciation des enjeux.

Plus dangereux sont les cyber-corsaires[7] qui œuvrent au profit d'un pays quelconque, ce dernier externalisant ses actions soit pour se cacher, soit par manque de compétences. La mobilisation de cyber-corsaires permet de limiter les risques de rétorsion en cas de découverte de l'origine de l'attaque ; et, paradoxalement, de maintenir un niveau important de conflictualité dans le cyberespace tout en entretenant le brouillard de la guerre par l'incertitude sur les motifs et l'identité réels de l'attaquant. Une hypothèse particulièrement dangereuse serait l'apparition de groupes spécialisés dans les attaques contre les systèmes maritimes – ou même contre les systèmes industriels connectés de manière plus générale – louant leurs services aux plus offrants. Dans ce cas, les agressions cyber sur des points chauds – détroit d'Ormuz, mer Noire,

[6] Des précédents existent dans ce domaine, comme ce fut le cas pour le port d'Anvers, où un piratage a permis à des narcotrafiquants, entre 2011 et 2013, de camoufler leurs activités (« Comment Anvers a été piraté et s'en est sorti », *La Libre Belgique*, 25 octobre 2013).

[7] Ces catégories sont bien évidemment poreuses, il est tout à fait possible qu'un pirate œuvrant par appât du gain un jour soit stipendié par un pays quelconque le lendemain pour conduire des attaques à but géopolitique.

mer de Chine, etc. – pourraient se multiplier, avec comme corollaire une insécurité maritime grandissante.

La prise de contrôle à distance d'un navire connecté, voire autonome, pourrait ainsi provoquer des dégâts importants, si ce n'est critiques. En effet, les navires de grande taille, vraquiers ou chimiquiers géants de plus de 100 000 tonnes, chargés de substances potentiellement nocives ou explosives, voire ceux transportant des milliers de passagers[8], représentent des objets dont l'inertie est telle que s'ils venaient à être détournés à distance et lancés contre les quais d'un port, les arrêter serait une mission plus que périlleuse. La cybersécurité tend ainsi à devenir un enjeu important du monde maritime puisque les risques liés au détournement des plateformes maritimes fixes comme les plateformes pétrolières ou mobiles comme les porte-conteneurs, sont particulièrement dangereux. Le cyber pourrait ainsi créer des menaces particulières dans le domaine du terrorisme maritime[9]. L'enjeu de la sécurisation des systèmes et objets maritimes connectés prend ainsi des allures de problématique critique, eu égard à l'ampleur des risques.

***

La stratégie navale et la stratégie cyber ont de nombreux points communs. Le premier d'entre eux est bien évidemment cette appréhension particulière du contrôle d'un espace où l'omniprésence est par nature impossible, ce qui implique de le considérer comme un réseau avec des pôles, des lignes et des nœuds d'importance. En outre, la question des capacités est également prégnante. Cyber et marine sont ainsi fondés en grande partie sur le croisement entre la technologie, dont la part est prépondérante, et les volontés des acteurs humains. En somme, si le cyberespace est le seul domaine stratégique artificiel, la présence de l'Homme dans l'espace maritime revêt elle aussi une forme d'artificialité. Cette similarité entre le domaine naval et le domaine cyber permet de relever un certain nombre d'enjeux partagés.

Toutefois, alors que le cyber n'a jamais pu faire l'économie de penser son aspect maritime – ne serait-ce que pour la question des câbles –, le domaine maritime doit intégrer plus avant le cyber au sein des réflexions sur les opportunités et, surtout, les menaces. Les plateformes de collecte et de traitement de données, les capteurs et les effecteurs, les systèmes de communication sont autant d'aspects que la pensée stratégique doit considérer afin d'intégrer au mieux les systèmes cyber dans l'ensemble du domaine maritime. Au-delà même de ces sujets immédiats, c'est bien entendu toute une chaîne complexe qu'il s'agit de mettre en mouvement au sein de la Marine – et des entreprises du domaine maritime – puisque la transformation digitale revêt également des externalités humaines (compétences, formation) mais aussi industrielles. A titre d'exemple, l'évolution du besoin énergétique pour faire face à la consommation de la transmission et du traitement de données impose de repenser profondément l'architecture du système électrique (stockage, efficacité, production) des navires, induisant de nouveaux enjeux d'architecture navale. Ainsi, le cyber maritime est loin de ne se limiter qu'à une « simple » question de communications.

[8] Le Symphony of the Seas, lancé en 2018, accueille à son bord plus de 8 000 personnes.

[9] Cette vision reste néanmoins prospective, le cyberterrorisme n'existant pour l'instant pas (Nicolas Mazzucchi, « Le cyberterrorisme à l'épreuve de la réalité », *Cahiers de la sécurité et de la justice* n°35-36, septembre 2016).

Les opinions exprimées ici n'engagent que la responsabilité de leur auteur.

WWW.FRSTRATEGIE.ORG

4 BIS RUE DES PÂTURES 75016 PARIS TÉL : 01 43 13 77 77 FAX 01 43 13 77 78

ISSN : 2273-4643
© FRS—TOUS DROITS RÉSERVÉS