La cybersécurité du navire de transport : un enjeu essentiel pour l'avenir ?

Sébastien LE VEY
Administrateur principal des Affaires maritimes
Chef de la mission « Sûreté des navires »

De nos jours, tous les moyens de transport évoluent et la technologie ne cesse de nous surprendre. Prendre place à bord d'une voiture autonome pour se rendre d'un point A à un point B n'est plus une utopie. La voiture autonome existe bel et bien et fonctionne. À un détail près! Cette voiture nécessite une sécurisation parfaite de son système d'exploitation afin de ne pas être contrôlée à distance. Et pourtant, c'est ce qui est arrivé en 2016 : un prototype de voiture autonome a été pris pour cible par des « *hackers* ». Ces derniers ont pris la main sur le système d'exploitation, puis télécommandé le véhicule à leur guise. Les images ont fait le tour des réseaux sociaux et ces petites imperfections technologiques ont démontré le besoin de verrouillage de la gestion technique de ce mode de transport.

Plus près de nous, nos véhicules d'aujourd'hui sont désormais connectés aux applications de nos *smartphones* afin d'ouvrir les portières, allumer les appareils auxiliaires, avoir un suvi GPS, démarrer le moteur… La sécurisation de ces applications est-elle aussi mise en question ? Des chercheurs de la société *Kaspersky Lab* se sont penchés sur la question et ont mis en lumière la vulnérabilité de ces applications qui peut déboucher sur la prise en main du véhicule. À ce jour, aucune exploitation de ces applications ni l'existence d'un utilitaire malveillant de type « cheval de Troie » qui permettrait de prendre le contrôle à distance du véhicule par leur intermédiaire n'ont été identifiées. Néanmoins, la gestion de ce type de faille par la cyber criminalité ne serait qu'une question de temps selon les experts.

Le domaine numérique du transport maritime évolue lui aussi rapidement. L'armement suédois *Stena Line* et la société *Rolls-Royce* vont prochainement développer un système de réalité augmentée adapté à une passerelle. Ce concept de superposition de données de synthèse dans un monde bien réel reposera sur la fusion des informations provenant des instruments de navigation et de bases de données. Ce système est en réalité un premier pas pour la société *Rolls-Royce* qui travaille à la conception d'un navire entièrement autonome. Les ingénieurs de cette firme espèrent faire naviguer d'ici dix ans des pétroliers, des porte-conteneurs totalement autonomes en mer Baltique[1].

Le navire autonome serait alors commandé à distance depuis un centre de contrôle. L'équipe de développement « *Ocean Blue* » de *Rolls-Royce* a ainsi mis en place un prototype de centre de contrôle à Alesund, en Norvège, qui simule une vue à 360° de cette tour de contrôle. Celle-ci serait armée par des capitaines et chefs mécaniciens qui suivraient les évolutions d'une flotte de plusieurs navires autonomes au niveau de la conduite et de la maintenance. Cette dernière serait assurée à distance au travers

1. Les Norvégiens *Kongsberg* et *Yara* se sont associés de leur côté pour concevoir et mettre en service à l'horizon 2020 le premier « *feeder* » autonome.

d'outils d'analyse de type drone. La conduite de ces navires répondrait quant à elle aux règles actuelles de navigation avec un plan de route pré-établi à suivre pour l'automate. Ce navire sans équipage et contenant uniquement des marchandises répondra en fait à un objet connecté de type IoT (*Internet of Things*). Sa conception sera bien plus complexe qu'une simple caméra pilotée à distance ou un réfrigérateur qui se remplit automatiquement afin de répondre aux besoins de notre vie courante. Néanmoins, ce navire du futur répondra aux mêmes exigences qu'un simple outil connecté à internet.

Cette prochaine évolution du transport maritime devrait réduire les coûts et augmenter les recettes des armateurs. Il n'y aurait plus aucune charge liée à un équipage et le volume des marchandises à bord du navire augmenterait avec la suppression des locaux qui lui sont dédiés. Vu d'un armateur, le navire autonome apparaît idyllique. Cependant, tout comme notre voiture autonome, il conviendra avant tout de sécuriser les systèmes d'information. Dans le cas contraire, les conséquences pourraient être dramatiques pour la sécurité de la navigation comme pour la protection de l'environnement. À court terme, le contrôle de ces systèmes d'information sera la véritable épine dorsale de notre navire.

Jusqu'à quel niveau doit-on les sécuriser ? L'inventivité des cybercriminels est débordante et utilise une panoplie d'outils simples ou très complexes selon l'objectif recherché. L'arme ultime étant un ver évolué de type APT (*Advanced Persistant Threat*) dont on a pu découvrir les effets sur le programme nucléaire iranien en 2010[2]. Bon nombre de personnes ont pris conscience à cette occasion que plus aucun système industriel ne semblait être protégé d'une cyber attaque. On peut donc raisonnablement se poser la question de la vulnérabilité numérique du navire : est-il envisageable d'imaginer la prise de contrôle à distance d'un pétrolier autonome et d'amener ce navire à se briser sur une digue pour déverser sa cargaison ? Fiction ? Réalité ?

Les évolutions numériques à bord du navire

La mer est aujourd'hui un maillon essentiel et incontournable pour notre économie : près de 50 000 navires et un million de marins assurent 90 % des échanges en volume.

L'automatisation des navires de commerce a commencé dans les années 1960 avec pour objectif la conduite des moteurs et des installations auxiliaires de façon à libérer le personnel des servitudes du quart traditionnel. Cet objectif a été atteint rapidement

2. En juin 2010, STUXNET, un ver informatique particulièrement complexe a partiellement détruit le programme nucléaire iranien. Il est considéré comme l'une des premières cyber armes.

et, pendant les vingt ans qui ont suivi, l'automatisation s'est étendue peu à peu en dehors du compartiment machine vers la gestion de la conduite, de la cargaison. Les sociétés de classification ont parallèlement adapté leur réglementation aux navires en fonction de leur degré d'automatisation.

La fiabilité des systèmes d'information à bord du navire a permis une réduction spectaculaire du nombre de personnes constituant l'équipage. Ces progrès ont permis d'automatiser tous les domaines-clés du navire de commerce : navigation à travers la carte numérique (*Electronic Chart Display and Information System* ou ECDIS), propulsion *via* la généralisation de la conduite par automate programmable, gestion du chargement… Le monde informatique est désormais omniprésent à bord de notre navire de commerce et il semble aujourd'hui difficile de se passer de cette technologie qui régule les moyens de communication, de gestion de la cargaison et la conduite du navire.

Cette transformation technologique du navire de commerce en a modifié sa gestion. Désormais les échanges sont quotidiens entre le bâtiment, la compagnie, le port, l'agent maritime… Le navire n'est donc plus isolé du réseau des réseaux, il s'intègre naturellement dans le cyber espace et appartient à la toile planétaire du net.

La conduite de ces systèmes n'est malheureusement pas exempte de défauts. Embarqués, ils peuvent ainsi être la clé d'entrée d'un acte de malveillance. Ces trois dernières années, les systèmes de positionnement automatique et par satellite, de cartographie ECDIS et d'enregistrement des données (*Video Data Recorder*) ont fait l'objet d'analyses qui ont révélé plusieurs failles numériques à corriger. Ces simples constats illustrent que le navire peut être vulnérable à un acte de malveillance, d'espionnage, au vol de cargaison et, au bout de la chaîne des menaces, au sabotage et à la prise de commande à distance. Bien que ces actes restent à ce jour très limités contre un navire, il convient cependant d'anticiper car nous n'avons encore rien vu… Protéger le navire consistera à préserver ses moyens opérationnels et organisationnels, l'objectif final étant de garantir qu'aucun acte de malveillance ne puisse mettre en péril la conduite et l'exploitation du navire.

Construire la protection numérique du navire

Pour mettre en place une démarche de sécurité des systèmes d'information du navire, il est important de pouvoir identifier correctement les valeurs et les biens à protéger. Ceci implique une approche rigoureuse en fonction du type de navire et de son exploitation.

À ce jour, la normalisation maritime mondiale n'a pas mis en place un cadre obligatoire pour faire face à ce type de menace. Seul le code international pour la sûreté des navires et des installations portuaires (code ISPS) définit une recommandation en matière de gestion des procédés informatiques. Ce code précise que la vulnérabilité du système informatique devrait faire l'objet d'une évaluation dans le cadre de la sûreté du navire afin de disposer de mesures adaptées à une quelconque menace. Évaluer le niveau de cette dernière est par conséquent essentiel, c'est pourquoi la Direction des affaires maritimes (DAM) a mis en place en 2015 un groupe de travail comprenant l'Agence nationale de sécurité des systèmes d'information (ANSSI) et Armateurs de France (ADF) afin de définir les outils à mettre en place pour faire face à une cyber attaque.

Une phase de recueil d'informations a été réalisée au travers d'une enquête à bord de navires, d'un audit de cyber sécurité auprès d'un navire sensible et *via* l'analyse des vulnérabilités des équipements embarqués. Le recueil de ces éléments permet dès à présent d'en tirer trois enseignements. Le premier porte sur la nécessité de « sacraliser » les systèmes industriels à bord du navire. Ces systèmes resteront par définition fondés sur des technologies qui n'évolueront que très peu après leur construction. Ils sont par conséquent vulnérables. Il est donc fondamental de les isoler et de maîtriser les interconnexions avec d'autres systèmes de gestion du navire. Le second enseignement porte sur le besoin d'élever le niveau de protection du système d'information du navire en disposant d'outils adaptés à son exploitation et d'un système de gestion permettant de faire face à une cyber attaque. Enfin le troisième enseignement concerne le besoin de disposer de marins sensibilisés à cette menace. Ils pourront ainsi mieux détecter une incohérence système.

Ces enseignements permettent dès à présent de définir les outils à mettre en œuvre dans le cadre de la protection de la sécurité de l'information à bord du navire. Ils peuvent être classés en trois catégories :
- les outils de protection : antivirus, pare-feu, connexion « tunnel » (VPN *Virtual Private Network*), logiciel anti-espions (*Anti-spyware*), logiciel de cryptage de messagerie et de Wi-Fi, détection de toute intrusion (IDS), archivage de données (NAS *Network Attached Storage*) ;
- les outils de gestion de la cyber sécurité au travers de normes s'intégrant au niveau des dispositions déjà présentes à bord du navire. Les codes internationaux de sécurité (ISM) et de sûreté (ISPS) permettent de mettre en œuvre rapidement des procédures adaptées au navire. Ces procédures devraient y inclure les références à la politique de cyber sécurité de la compagnie, la gestion d'incident issu d'un acte de malveillance au travers de la reprise du navire, l'autocontrôle du système d'information du navire, la sauvegarde des données, la gestion des échanges entre le navire et les intervenants

extérieurs. Ce dernier aspect est essentiel car un cyber attaquant s'appuiera de façon certaine sur un intervenant extérieur pour contourner les mesures mises en place par la compagnie ;
- les outils de formation : il convient de sensibiliser tous les marins à ce type de menace afin qu'ils puissent mettre en œuvre une « hygiène informatique » à bord du navire. En complément, le navire devrait disposer d'un responsable en charge de la sécurisation des systèmes d'information à bord.

La mise en place de ce cyber triangle doit permettre de disposer d'un cadre afin de traiter une cyber menace.

Un enjeu essentiel ?

Si le seuil de la menace est relativement faible à ce jour, les systèmes technologiques et de gestion adaptés existent pour la contrer. Le monde du « *shipping* » a aussi posé un premier jalon de directives à travers la circulaire 1526 de l'Organisation maritime internationale de mai 2016. Tout est donc en place pour protéger nos 50 000 navires. La faiblesse de la menace n'incite cependant pas les armateurs à investir dans la cyber sécurité. Mettre en place des mesures de sécurisation n'améliore pas la gestion de l'exploitation du navire et oblige à investir dans un domaine qui ne rapporte pas !

La non-prise en compte de cette menace pourrait cependant se révéler catastrophique et bien plus onéreuse qu'un investissement dans ce domaine. Le vol de cargaison apparaît à première vue la menace la plus importante. À titre d'exemple, la société *Verizon* avait mis au jour un projet de vol de conteneurs à bord d'un navire en 2016. Les cyber criminels s'étaient positionnés sur les réseaux d'une compagnie maritime et analysaient le positionnement des conteneurs à forte valeur ajoutée. Il ne restait plus qu'à transmettre ces informations à une équipe en charge de récupérer les conteneurs convoités. Par ailleurs, imaginez les conséquences d'une cyber attaque sur un porte-conteneurs de 18 000 boîtes dont la valeur marchande peut atteindre 1 milliard de dollars ! Et plus les navires se numérisent, plus ils sont exposés. Sensibiliser et accompagner les armateurs pour concrétiser la mise en place d'outils de gestion, d'outils technologiques et d'une formation adaptée est donc essentiel. La DAM a ainsi mis en place un premier triptyque de documents afin de sensibiliser les compagnies. Ces derniers portent sur les moyens d'évaluation/protection du navire, le risque lié aux systèmes industriels du bord et enfin sur les bonnes pratiques en matière d'hygiène informatique[3].

3. http://www.developpement-durable.gouv.fr/surete-des-navires-et-surete-portuaire.

Un deuxième enjeu porte sur la sécurisation globale des systèmes d'information du navire, qu'il soit autonome ou non. Cette sécurisation doit se faire au niveau du navire et de la compagnie, de la gestion de la simple boîte *mails* jusqu'aux systèmes de conduite. Les messageries de société sont en effet une cible privilégiée des cyber-criminels, les données qu'elles sont susceptibles de fournir, directement ou indirectement, à l'attaquant étant plus facilement commercialisables sur le *Dark Web* que les contenus de messageries personnelles. C'est la raison pour laquelle les boîtes professionnelles reçoivent quatre fois plus de *malwares* que les autres. La boîte *mails* d'un navire peut ainsi être la clé d'entrée pour échafauder une prise en main de la cargaison, de l'image de la compagnie ou autre. Aussi, il convient que la direction de la compagnie s'inscrive dans la mise en place d'un cadre normatif à bord du navire pour éliminer tout type de faille système.

La formation des marins du navire constitue le troisième enjeu. Chaque marin devrait au moins connaître et adapter des mesures d'hygiène informatique de base. Ces mesures portent sur la gestion d'un simple mot de passe, d'une clé USB, la prudence sur internet… Un autre degré de formation devrait passer par la mise en place d'un responsable au niveau du navire. Ce dernier aurait pour objectif de piloter les systèmes d'information à bord du bâtiment. Cette tâche pourrait compléter une fonction déjà existante pour ce marin. Dans cet esprit, l'École nationale supérieure maritime et la DAM travaillent à la mise en place d'un référentiel de formation des officiers de marine marchande pour la rentrée 2017/2018.

Enfin, le quatrième enjeu devrait porter sur la gestion croissante de l'internet des objets. Depuis une dizaine d'années, le réseau internet se transforme progressivement en un réseau étendu reliant plusieurs milliards d'êtres humains mais aussi des dizaines de milliards d'objets. L'IoT, grâce à l'omniprésence de ses capteurs et systèmes connectés, fournit au système de pilotage des informations qui permettent d'identifier et de résoudre différents problèmes. Ces systèmes permettront à terme aux compagnies maritimes de bénéficier d'une meilleure rentabilité du navire *via* une baisse des coûts d'exploitation et de maintenance. L'une des prochaines intégrations de l'IoT dans le monde maritime concerne le suivi de conteneurs. En 2017, la société française *TRAXENS* va équiper 200 000 conteneurs d'un boîtier intelligent. Ce dernier permettra le suivi en mer, à terre du conteneur au travers d'outils de communication reliés aux réseaux GSM et satellitaire qui l'environnent. Le navire sera quant à lui pourvu d'un ordinateur central afin de relayer les informations délivrées par le boîtier équipant le conteneur. Pour être pleinement efficaces, ces objets doivent être sécurisés afin d'éviter tout acte de malveillance tel que la prise en main à distance afin de les intégrer à un réseau de machines zombies pour perturber un système (attaque de type DDOS).

Faire face à la cyber criminalité de demain

Qu'il s'agisse d'une voiture, d'une simple caméra pilotée à distance, d'un navire, les systèmes d'information ont envahi notre quotidien. Ils nous simplifient bon nombre de tâches et nous permettent d'être très performants. Chacun d'entre eux doit pouvoir répondre à nos demandes et non pas servir un intérêt criminel. Aussi, il est nécessaire de les sécuriser afin de maîtriser au mieux leur action. Néanmoins, il restera sur chaque système un risque résiduel. Ce dernier doit être évalué en fonction de la menace. S'il est trop important, il convient de mettre en place une contre-mesure. Cette dernière existe pour le navire de transport. Il convient juste de la mettre en place au travers d'un cadre simple et adapté à l'exploitation du navire.

Mais jusqu'où accompagner le navire de charge ?

Cette frontière est fonction de l'évaluation de la menace. Si cette dernière correspond à la gestion de virus paralysant temporairement la cartographie électronique du navire ou la conduite des automates machines, l'équipage devrait pouvoir y faire face avec des procédures adaptées. Si elle prend la forme d'une cyber arme sophistiquée dormante utilisant des failles système de type « *0Day*[4] », il est évident que ni l'équipage ni le support informatique de la compagnie ne pourront y faire face ! Ce genre d'arme fait pourtant partie de la panoplie des outils à disposition d'organisations criminelles, de groupes terroristes ou d'États. En complément, n'oublions pas que le navire représente une excellente vitrine médiatique. Dans ce contexte, on peut raisonnablement questionner le besoin de disposer d'une « cyber flotte maritime stratégique ». À l'image de nos approvisionnements stratégiques qui imposent un quota de navires, on peut s'interroger sur le besoin pour la France de disposer d'un ensemble de navires garantissant un niveau d'exigence en matière de cyber sécurité permettant d'assurer nos approvisionnements stratégiques.

En matière de cyber criminalité, il faut s'attendre à l'inattendu.

4. Une faille « zero day » est une faille de sécurité identifiée par un nombre très restreint de personnes et ne bénéficiant d'aucun correctif connu.