Lettre mensuelle – Septembre 2020 – Disponible sur omc.ceis.eu

Table des matières

ANALYSES

1) Un monde « post-digital »… mais à quel prix et à quelles conditions ? 1

2) Cybersécurité du transport maritime : quels enjeux et quelles solutions ? 6

FOCUS INNOVATION

Cosmian : le calcul collaboratif de données chiffrées 11

CALENDRIER

1-31/10 : Cybermoi/s 2020 13

ACTUALITÉ

Lancement du « Diag Cyber », dispositif d'aide à la sécurisation cyber des PME/ETI de la Défense 13

ANALYSES (1/2)

UN MONDE « POST-DIGITAL » ...
MAIS À QUEL PRIX ET À QUELLES CONDITIONS ?

La crise Covid-19 a engendré un véritable « big bang » de la transformation numérique qui s'est inévitablement accompagné de nouveaux défis. Défis techniques et technologiques, (géo)politiques, sociaux et sociétaux, auxquels le « monde d'après » devra répondre pour être pérenne. Pour les Armées, et plus particulièrement le Commandement de la cyberdéfense, l'enjeu est multiple et il est de taille : préparer l'avenir ; comme comprendre le cyberespace de demain et le milieu dans lequel les Armées opèreront ; comprendre à la fois les évolutions de l'écosystème du numérique et leurs répercussions sur le monde physique et vivant, mais aussi les évolutions d'usage et d'emploi des outils numériques ; comprendre et anticiper les bouleversements géopolitiques et sociologiques du cyberespace pour mieux s'y préparer. Tant à court terme, à des fins de prospective stratégique, qu'à long terme, à des fins de préparation opérationnelle, seule une bonne compréhension des conséquences de la crise Covid-19 permettra de relever ces défis.

1. La crise, accélérateur d'une transformation numérique aux effets secondaires encore ambigus

En mettant à l'épreuve la résilience des organisations et des sociétés, forcées de s'adapter à un contexte inédit et imprévisible et d'adopter de nouveaux modes de fonctionnement dans des délais extrêmement courts, la crise a agi comme l'accélérateur d'une transformation numérique déjà bien amorcée. Le temps du confinement, la crise a imposé le « distanciel » comme la nouvelle norme : vidéo-conférences, webinars, salles de réunions virtuelles et solutions de partage d'information sont du jour au lendemain devenus les outils de travail quotidiens de milliards d'individus, tant pour des usages privés que professionnels. Si certaines organisations avaient déjà recours de façon plus ou moins ponctuelle au mode « distanciel », beaucoup d'autres ont dû, en quelques heures, non seulement ajuster leurs façons de travailler et d'interagir, mais aussi tout simplement s'équiper en webcams, ordinateurs portables, écrans, clé VPN… rappelant ainsi notre dépendance à des flux matériaux dans un monde pourtant de plus en plus numérisé. La bascule a sans doute été moins douloureuse pour les organisations qui, comme Véolia, avaient déjà fait des choix technologiques de solutions en mode Saas ou cloud notamment, permettant de décorréler l'accès aux systèmes d'information d'un périmètre géographique donné. La crise Covid-19 a aussi exigé de beaucoup organisations qu'elles revoient leurs modes et process de production, consacrant ainsi certaines technologies émergentes comme l'impression additive ou 3D, les jumeaux numériques...

À bien des égards, cette crise a accéléré certaines évolutions latentes mais inéluctables du paysage et des usages du numérique. C'est même l'un de ses principaux enseignements. Mais si cette digitalisation à marche forcée a été salutaire pour les organisations comme pour les individus, elle a aussi rapidement mis au jour les dangers d'une digitalisation à outrance que ce « monde d'après » de plus en plus digitalisé devra écarter pour survivre au « retour à la normale ». Car le progrès n'est pas uniquement une affaire de technologies, il est d'abord une histoire d'Humains. Or la crise a montré que l'individu était paradoxalement l'un des grands perdants de cette transformation : elle a rappelé d'une part que la digitalisation n'était pas accessible à tous, et d'autre part qu'elle pouvait ne pas être que bénéfique. D'abord, la crise a brutalement rendu bien tangible

la « fracture numérique » et « l'illectronisme » : elle a laissé de côté les individus qui n'avaient pas techniquement accès aux outils numériques (smartphones, postes de travail…) mais aussi ceux qui n'avaient pas les codes et compétences permettant de les utiliser et donc de participer pleinement au mode numérisé. On considère aujourd'hui que 17% des Français sont dans ce cas[1]. Ensuite, le « tout-digital » n'a pas été sans effets secondaires néfastes, comme le rappelait Camille Rabineau dans « Covid-19 ou le big bang de la transformation numérique ». : douleurs physiques, sentiment d'isolement, perte de repères dans le temps, effacement du lien humain et social… Autant de questionnements sur l'éthique et sur la place de l'Humain dans ce monde digitalisé.

Mais cette révolution digitale, si impactante soit elle sur nos modes de vie, semble s'être imposée comme le principal sinon l'unique prisme à travers lequel nous analysons aujourd'hui les conséquences de la crise Covid-19. Or le digital, ou du moins la transformation digitale des organisations et des sociétés, est désormais si avancée qu'elle ne constitue même plus un avantage compétitif durable. À court terme, le digital sera un non sujet, il sera la norme. L'enjeu n'est donc plus tellement la transformation digitale elle-même que ses conséquences et ses impacts. Dominique Turc recommande ainsi de se projeter au-delà du digital en retirant cette « œillère » qui nous empêche de voir et d'étudier les autres forces qui bouleversent de façon durable notre société.

2. La crise, révélateur de profondes mutations politiques et sociétales

Dominique Turc rappelle en effet que crise a aussi accéléré certaines transformations moins visibles, plus profondes, portées par des forces technologiques et sociologiques susceptibles d'entraîner, à court terme, des mutations sociales et sociétales durables.

Retrouvez ici l'intervention de Dominique Turcq

Des technologies prometteuses mais ambivalentes

Parmi ces forces technologiques, **l'intelligence artificielle** (IA) est sans doute celle qui aujourd'hui fait le plus parler d'elle. Véritable *buzzword* de cette décennie, elle est souvent associée, à tort, aux technologies dites « digitales ». Or contrairement à ces dernières, l'IA n'est pas une technologie exacte : elle reste approximative, et là ou bien des technologies digitales remplacent l'action humaine, l'IA ne fait que l'assister. Par exemple, si l'IA constitue une aide (précieuse) à la décision mais ne peut pas (encore ?) prendre elle-même une décision.

[1] https://www.vie-publique.fr/en-bref/271657-fracture-numerique-lillectronisme-touche-17-de-la-population

De la même façon, les technologies de **reconnaissance faciale** qui connaissent aujourd'hui un véritable essor sont encore relativement peu utilisées car encore pas assez fiables et le risque d'erreur trop grand. Autre technologie émergente dont on sous-estime souvent les répercussions à moyen et long terme : les **neurosciences**. Petit à petit, elles se frayent, discrètement et souvent anonymement, une place de plus en plus importante dans nos quotidiens privés comme professionnels, qu'elles soient non-intrusives comme les « nudges » qui nous manipulent parfois insidieusement mais nous permettent aussi d'identifier et comprendre nos biais décisionnels, ou plus envahissantes comme le projet Neuralink, encore au stade de la recherche, d'électrodes implantées dans le cerveau pour permettre la connexion homme-machine. L'enjeu reste donc de comprendre et apprendre à maîtriser ces technologies prometteuses afin qu'elles ne soient pas détournées et utilisées à des fins malveillantes (propagande, fraude…).

Des phénomènes sociologiques préoccupants

À côté de ces forces technologiques, la crise Covid-19 a aussi mis en mouvement un certain nombre de tendances sociologiques et sociétales lourdes mais trop souvent sous-évaluées. La plus manifeste est sans doute l'évolution de notre **relation à l'information**. Les figures qui traditionnellement faisaient autorité (scientifiques, experts, institutions) font aujourd'hui face à une véritable crise de confiance et de crédibilité qui fait le lit des fake news et de la propagande. Le phénomène que Dominique Turc qualifie de « **tripadvisorisation** » y a fortement contribué. *« Aujourd'hui on peut tout mesurer tout de suite et tout publier tout de suite. On est mesurés et évalués à tout moment, à la fois en tant qu'individu et qu'organisation ».* C'est ce qu'ont illustré les débats houleux entre experts médicaux sur l'usage de la chloroquine, et les échanges parfois violents auxquels ils ont donné lieu sur les réseaux sociaux sous formes de posts interposés entre auditeurs pourtant profanes. Sans compter la prolifération de théories du complot sur l'origine du virus voire sur son existence même, à la suite de publications de photos d'hôpitaux vides. Le phénomène n'est pas nouveau et les distorsions et manipulations de l'information sont même à la fois l'une des tendances majeures et l'un des plus grands dangers de ce monde de plus en plus digital, mais la crise Covid-19 a agi comme une fantastique caisse de résonnance qui doit nous forcer à repenser la façon dont on produit et dont on gère l'information. Les défis sont considérables pour les États et presque encore plus pour les Armées : risques politiques et sociaux d'abord, notamment sous forme de populisme et de propagande, mais aussi sécuritaires, avec des enjeux de lutte informationnelle et d'influence d'intensité sans précédent.

Des dépendances géopolitiques et stratégiques croissantes

Au plan politique et diplomatique, Didier Danet souligne que la crise *« a cristallisé des comportements d'accaparement, ou de conflits durs » :* bataille pour les masques sur les tarmacs d'aéroports, rachats de sociétés pharmaceutiques pour être prioritaires pour les vaccins… Le numérique n'échappe pas à cette dynamique. Une fois encore, la crise a permis de prendre conscience de changements à l'œuvre depuis longtemps et des enjeux et défis associés. Plus particulièrement, elle a mis en lumière la façon dont le numérique a, au cours des dernières décennies, redessiné les relations entre les États et favorisé l'émergence d'un duopole sino-américain. Car malgré quelques alternatives minoritaires, le marché des technologies qui sont au cœur des outils numériques qui permettent aujourd'hui encore aux organisations et sociétés de traverser cette crise est clairement partagé entre la Chine et les États-Unis : réseaux sociaux, solutions Cloud, outils de vidéo-conférences, messageries instantanées, mais aussi technologies de l'IA. Et sans doute, cela sera également le cas de la 5G ou du quantique.

Retrouvez ici l'intervention de Didier Danet

Plus qu'un simple retard technologique ou qu'un désavantage commercial et économique, l'enjeu est celui de notre autonomie stratégique. Ce que la crise a surtout révélé, c'est l'urgence de se doter d'une capacité de décision et d'action autonome, mais aussi de se donner les moyens de rallier d'autres acteurs à nos actions et décisions. Face à un duopole sino-américain, fort de ressources que nous n'avons pas, le constat d'échec et le ralliement à l'un des deux géants n'est pas une option rappelle Didier Danet. C'est ce qu'a tenté de démontrer la France en déployant une application « StopCovid » indépendante des géants américains du numérique, prouvant à la fois la maîtrise des technologies utilisées et l'existence d'un réel savoir-faire.

Autonomie stratégique ou souveraineté numérique ?

Le concept de « souveraineté numérique », souvent associé à une posture défensive, laisse aujourd'hui la place à la notion « d'autonomie stratégique », plus dynamique et volontaire, et qui répond aussi à la définition d'un destin commun et de valeurs communes. La souveraineté numérique, précise le général Jean-Paul Paloméros, ne se décrète pas. Elle se mérite, elle s'acquiert. Elle s'arrête là où commence celle des autres. Elle repose sur l'aptitude à se protéger et à se défendre, mais aussi sur l'aptitude à innover et donc à maîtriser son destin. Véritable enjeu pour l'Europe et pour la France, l'autonomie stratégique prend au fil des crises des formes et des déclinaisons multiples (sanitaire, numérique…), et évolue avec la notion de puissance et de responsabilité.

Plus encore, rappelle Sébastien Bombal, l'autonomie stratégique s'applique à tous les échelons. En matière de numérique par exemple, elle concerne à la fois la base industrielle et l'écosystème du numérique, la gouvernance de l'internet, les législations et la règlementation… et pose une série de question imbriquées et interdépendantes, de la localisation des données, à la nationalité des entreprises, en passant par l'applicabilité de nos législations au-delà du territoire national, la dépendance applicative, la sous-traitance et la délocalisation…

Retrouver l'explication du débat entre ces termes par Alix Desforges ici.

Parmi les solutions à l'étude pour s'affranchir de cette double dépendance, celle du Cloud de confiance demeure, au niveau technologique, la démarche la plus aboutie. Didier Bove rappelle d'ailleurs que ce projet a fait l'objet de débats et réflexions au sein du CIGREF. Le principal enjeu reste celui de l'adéquation entre le niveau de sécurité et la facilitation d'utilisation, clé d'une adoption rapide et massive. Des travaux sont également en cours au niveau européen via le projet GaiaX, qui consiste pour sa part en un socle de standards communs pour un écosystème européen du Cloud.

3. Et maintenant ?

Comment, dans ce contexte, relever les défis du monde post-digital ? Dominique Turcq propose « d'échanger nos armures pour des capes de Jedi ». C'est-à-dire s'adapter à notre nouvel environnement et à nos nouveaux adversaires en faisant évoluer nos structures et nos organisations. Les enjeux sont multiples : enjeux de structure et de fonctionnement d'abord, de hiérarchie et de subsidiarité ensuite, mais aussi de formation et de montée en compétence, d'évaluation et de critères de performances, de culture enfin pour donner aux employés et aux citoyens le bon degré d'autonomie et susciter leur confiance.

Pour le général Jean-Paul Paloméros, il s'agit d'abord de tirer les leçons et de faire un retour d'expérience constructif de cette crise. Car chaque crise est aussi une opportunité et il nous appartient aujourd'hui de la saisir pour construire un « monde d'après » pérenne. Cette crise se distingue par sa durée, son intensité et ses paradoxes. D'une part elle nous a permis de, ou forcé à, tirer tous les bénéfices de l'espace numérique, de ses applications les plus avancées, de ses caractéristiques physiques : hyperconnexion, multiplexage, ubiquité, etc. qui ont permis la communication, la télémédecine, ou encore l'instruction à distance. Mais dans le même temps, la crise a accentué certaines inégalités, a souligné le besoin existentiel d'activité humain, et a rappelé que le monde digital ne pouvait faire qu'au service de l'Humain et non pas à son détriment. Il reste donc aujourd'hui aux parties prenantes à construire cette maturité digitale. Les États, d'abord, devront se recentrer sur leurs fonctions régaliennes dans un double objectif de prospection (anticipation, vision du temps long) et de protection (de nos espaces, de nos intérêts vitaux...). Quant aux entreprises, elles devront se constituer en réseaux, en écosystèmes solides. Les individus enfin, devront être acteurs du changement, formés et instruits pour pouvoir monter en compétence et acquérir les clés de cet avenir post-digital.

ANALYSES (2/2)

CYBERSÉCURITÉ DU TRANSPORT MARITIME : QUELS ENJEUX ET QUELLES RÉPONSES ?

En 2017, la cyberattaque NotPetya a considérablement affecté le géant du transport maritime Maersk. Victime d'une interruption contrainte de ses opérations, l'entreprise danoise a subi une perte de productivité, estimée à 300 millions USD[2], et a dû recomposer une partie de son parc informatique[3]. Cet incident a rappelé à grande échelle l'exposition croissante du secteur maritime aux cybermenaces.

La mer est incontournable pour les échanges mondiaux. Avec plus de 50 000 bateaux et un million de marins qui contribuent annuellement aux flux commerciaux, les activités maritimes reposent aujourd'hui en grande partie sur l'informatique, désormais omniprésente dans les ports et à bord des navires.

La filière maritime profite en effet depuis plusieurs années des nouvelles technologies de l'information et de la communication. L'adoption croissante de technologies émergentes telles que le *cloud computing*, le *big data*, l'intelligence artificielle (IA) et l'Internet des objets (IoT) a permis au secteur d'automatiser ses services et ses processus, améliorant ainsi sa rentabilité et sa compétitivité.

Cette dynamique de numérisation repose sur ce que certains appellent la « *marétique* ». Défini par le *Livre Bleu* du cluster éponyme (2013), ce néologisme désigne « *l'ensemble des systèmes informatiques et électroniques utilisés dans la gestion et l'utilisation des opérations relatives aux activités maritimes, fluviales et portuaires*[4] ». Couvrant toutes les marines (marchande, militaire, pêche, plaisance et scientifique), la *marétique* concerne à la fois les navires, les ports, les systèmes de navigation et de communication, ainsi que les outils de gestion et de contrôle du trafic maritime et des cargaisons[5].

La montée en puissance de la marétique s'accompagne d'une interconnexion accrue des technologies de l'information[6] (IT) et des technologies opérationnelles[7] (OT) qui composent les ports et les navires. Or si cette convergence IT/OT favorise par exemple le diagnostic et la maintenance à distance des navires, elle contribue également à augmenter leur surface d'exposition aux cybermenaces. Bien que les dernières années aient été témoins d'une prise de conscience du risque cyber, la réglementation et la législation ne permettent pas en l'état d'y faire face pleinement.

---

[2] Jordan Novet, « Shipping company Maersk says June cyberattack could cost it up to $300 million », *CNBC* [en ligne], 16 août 2017.

[3] Christophe Auffray, « Les 10 nuits en enfer de Maersk pour réinstaller 4000 serveurs et 45000 PC », *ZDNet* [en ligne], 3 mars 2020.

[4] *Livre bleu de la Marétique*, 13 novembre 2013, p. 6.

[5] « Les systèmes de la marétique », *Cyber marétique* [en ligne], 24 octobre 2018.

[6] Comme le Wi-Fi et les systèmes de distraction à bord (Internet, réception et distribution TV, etc.).

[7] Ces « systèmes métiers » sont notamment chargés de la navigation et à la propulsion des bâtiments, ainsi que la gestion de l'énergie, des marchandises, des passagers et des alarmes.

Le maritime : un secteur de plus en plus exposés au risque cyber

Les ports : des infrastructures stratégiques de plus en plus numérisées

En 2018, le transport maritime international a atteint pour la première fois un volume total de 11 milliards de tonnes[8] (contre 10,6 milliards en 2017). Cette hausse s'est accompagnée d'une croissance du nombre d'informations en circulation relatives aux marchandises, aux navires et aux passagers.

Pour rester compétitifs, les ports se sont lancés dans l'automatisation et le traitement de ces flux de plus en plus denses de données. Plaçant la numérisation et l'innovation technologique au cœur de leur modernisation, les *smart ports*[9] (tels que Le Havre, Dubaï, Hong Kong, Los Angeles, Port Elizabeth, etc.) ont automatisé leurs services afin d'optimiser la sûreté de leurs infrastructures, ainsi que la gestion et la planification de leurs opérations (notamment celles des porte-conteneurs et des camions autonomes, la surveillance en temps réel des activités, etc.). Cette numérisation de plus en plus importante accroît dans le même temps l'exposition des ports aux actes de cyber-malveillance.

> En mai 2020, l'Iran a été la cible d'une cyberattaque contre le port de Shahid Rajaee, l'un de ses principaux terminaux maritimes dans le détroit stratégique d'Ormuz. Téhéran a déclaré que cette attaque n'était pas parvenue à compromettre les systèmes de l'Organisation portuaire et maritime (PMO), autorité nationale des ports iraniens, mais qu'elle avait toutefois compromis et endommagé les systèmes de plusieurs opérateurs privés. La cyberattaque a ainsi eu pour effets d'immobiliser plusieurs conteneurs et navires, ainsi que de créer d'importants embouteillages sur les routes conduisant au port de Shahid Rajaee[10].

Si dans cet exemple les dommages semblent relativement limités, une cyberattaque de grande ampleur contre un port pourrait conduire à la suspension totale de ses activités, susceptible de perturber voire de paralyser totalement la chaîne d'approvisionnement et l'économie du pays ciblé.

De plus, les opérations portuaires sont désormais coordonnées par un *Port Community System* (PCS), qui facilite le fonctionnement des équipements et des services industriels (grues, écluses, ponts, installations de sécurité, etc.), ainsi que les technologies de l'information utiles aux activités d'un port[11]. Le PCS constitue une plateforme d'échange sécurisé d'informations au sein de la communauté portuaire, laquelle se compose d'un grand nombre d'acteurs publics (douanes, police, ville) et privés (transport maritime et ferroviaire, lamanage, avitaillement, gestion des camions, grues, stocks, etc.).

Cette diversité d'acteurs constitue également une vulnérabilité car elle suppose des niveaux variés de sensibilité et de compréhension à la cybersécurité. Le PCS doit ainsi rappeler que la diffusion d'une culture d'hygiène informatique à tous les échelons de la communauté portuaire est essentielle au renforcement de son niveau global de sécurité[12].

---

[8] CNUCED (Nations Unies), *Étude sur les transports maritimes*, 2019, p. 2.
[9] Théo Sinibaldi, *Les Smart Ports*, Wavestone, Juillet 2017.
[10] Ellen Nakashima, Joby Warrick, « Officials: Israel linked to a disruptive cyberattack on Iranian port facility », *The Washington Post* [en ligne], 18 mai 2020.
[11] IAPH, *Port Community Cyber Security*, Chapitre 1.
[12] J. Besancenot, « Le port du futur sera un port « smart » et cyber sécurisé ! », *CyberCercle* [en ligne], Mai 2020.

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a récemment décliné quatre scénarios principaux de cyberattaque contre les ports[13] :

- Une attaque informatique ciblée dans le but d'accéder à des données sensibles pour voler des cargaisons de grande valeur ou effectuer des trafics illégaux ;
- la diffusion de rançongiciels conduisant à un arrêt total des opérations portuaires ;
- la compromission du PCS pour manipuler ou voler des données ;
- la compromission des OT créant un accident majeur dans les zones portuaires.

Les navires : des ensembles complexes hyperconnectés

Autrefois entièrement isolés une fois en mer, les navires sont désormais des ensembles complexes connectés à un réseau d'acteurs et embarquent de plus en plus de SI (communication, automates, systèmes critiques de navigation, de propulsion ou de sécurité). Leur numérisation a considérablement modifié la gestion et le contrôle du trafic maritime. Les échanges entre la mer (bateau et agent maritime) et la terre (port et compagnie) s'effectuent aujourd'hui en temps réel. Les offres de service à distance se multipliant, l'interconnexion accrue des SI à bord, qui permet notamment le diagnostic et la maintenance à distance des navires, étend la surface d'exposition des navires aux cybermenaces et accroit leurs vulnérabilités aux risques cyber, parmi lesquels :

Système	Exemples de risques potentiels[14]
Système de visualisation des cartes électroniques et d'information (ECDIS)	Effet : L'ECDIS est un dispositif embarqué d'information et de visualisation des cartes électroniques de navigation officielles (ENC). En raison de ses interconnexions, il est un élément central de la navigation, en plus d'être de plus en plus relié au système de *command-and-control*. Un ECDIS insuffisamment sécurisé peut faire l'objet d'une cyberattaque.
	Exemple : En 2014, l'entreprise NCC Group publie un livre blanc dans lequel sont exposées les vulnérabilités permettant d'accéder et de modifier de manière non autorisée les ENC contenues dans un ECDIS[15].
Système d'identification automatique (AIS)	Effet : Un AIS permet à un navire de fournir à d'autres navires et aux ports des informations relatives à son identité, sa position et sa route. Les vulnérabilités de son protocole permettent de modifier les données émises par un navire et de le faire passer pour un autre (« émission de faux échos AIS »).
	Exemple : En 2013, le pétrolier iranien Ramtin s'est fait passer pour l'avitailleur Hamoda K (Togo) en piratant son AIS, afin de naviguer au large de Singapour, pour contourner l'embargo américain sur le pétrole contre l'Iran[16].

[13] ENISA, *Port Cybersecurity - Good practices for cybersecurity in the maritime sector*, 26 novembre 2019.
[14] Premier ministre, *Stratégie nationale de sûreté des espaces maritimes*, 10 décembre 2019, p. 25.
[15] « Security vulnerabilities found in technology used by maritime industry "could cause ships to run aground" », *NCC Group* [en ligne], 1er avril 2014.
[16] R. Almeida, « Iranian Tanker Hacks AIS to Disguise Itself Off Singapore », *gCaptain* [en ligne], 25 octobre 2013.

Assistant de navigation (GPS)	Effet : Le GPS est un système de positionnement par satellite qui permet aux navires de se géolocaliser. Vulnérable aux attaques de type brouillage et leurrage, son piratage peut perturber la navigation et le trafic maritime.
	Exemple : En 2016, la Corée du Sud a accusé Pyongyang d'avoir affecté la réception du signal de plus de 700 navires sud-coréens, provoquant une perturbation de son trafic maritime pendant près d'une semaine[17].
Ports USB	Effet : Utilisés pour la mise à jour de systèmes, la réalisation d'opérations de maintenance ou le transfert de fichiers vers ou à partir des OT « hors réseau ».
	Exemple : Un avitailleur a compromis une partie du réseau bureautique de son navire par le biais d'une clé USB infectée. Cela n'a toutefois pas atteint les systèmes de *control-and-command* qui étaient probablement cloisonnées[18].

La plupart des navires en service actif embarquent des SI dont la sécurisation demeure difficile *a posteriori*. Cette réalité souligne la nécessité de sécuriser l'ensemble des technologies de l'information et des technologies opérationnelles dès la phase de conception des bateaux dans une approche « *security by design* ». En parallèle, les réflexions des sociétés de classification sur les normes et les standards techniques qui encadrent la construction navale doivent continuer d'évoluer et d'y intégrer la cybersécurité, afin de faire émerger de nouveaux protocoles de sécurité. De même, la formation cyber des équipages doit se poursuivre. Les recommandations des assureurs du secteur maritime doivent également être prises en compte. En mars 2020, le sud-coréen KR a par exemple délivré la première certification cyber au monde au pétrolier/chimiquier Songa Hawk[19] (îles Marshall).

Un encadrement législatif en progression

Un cadre règlementaire international peu contraignant

Comme indiqué par la *Stratégie nationale de sûreté des espaces maritimes* (2019), la prise de conscience des enjeux cyber par les grands acteurs du secteur maritime est désormais bien réelle[20] .

Plusieurs associations professionnelles ont d'ailleurs publié à l'égard de ces acteurs des guides de bonnes pratiques. Le Baltic and International Maritime Council (BIMCO) a publié en 2016 des *Guidelines on cyber-security on board ships*, mises à jour en 2017 et en 2018. Outre des recommandations, ce guide rapporte plusieurs incidents cyber dans la filière maritime et est cité comme une référence par l'Organisation internationale maritime (OMI). Ces bonnes pratiques sont toutefois non contraignantes. Leur application est de fait laissée à la discrétion des parties concernées et n'est peu voire pas contrôlée.

[17] J. Kim, « South Korea revives GPS backup project after blaming North for jamming », *Reuters* [en ligne], 2 mai 2016.
[18] BIMCO, *The Guidelines on Cyber Security Onboard Ships*, Décembre 2018, p.18.
[19] « KR certifies first cybersecurity compliant vessel », *Safety4Sea* [en ligne], 9 mars 2020.
[20] Premier ministre, *Stratégie nationale de sûreté des espaces maritimes*, 10 décembre 2019, pp. 24-26.

Quant au dispositif règlementaire encadrant la cybersécurité des navires, il est encore peu développé et ne prend pas en compte l'évolution récente des menaces. La cybersécurité des ports ont toutefois fait l'objet d'une attention singulière à l'échelle européenne :

- Entré en vigueur en 2004, le Code International Ship and Port Facility Security (ISPS) relatif à la sûreté des navires et des ports est un premier pas vers la considération du risque cyber à bord. Sa partie facultative mentionne que « *l'évaluation de la sûreté du navire devrait porter sur les* [...] *systèmes de radio et télécommunications, y compris les systèmes et réseaux informatiques*[21] » ;

- en juin 2017, l'OMI a adopté la résolution MSC.428(98) sur « la gestion des cyber-risques maritimes dans le cadre des systèmes de gestion de la sécurité », qui pose le premier cadre règlementaire de la cybersécurité de l'industrie maritime. Cette résolution pousse les navires à évaluer leur risque cyber, au plus tard lors de la première vérification annuelle de l'attestation de conformité des constructeurs après le 1er janvier 2021 ;

- en juillet 2017, l'OMI a voté la circulaire MSC.1-FAL.1/Circ.3 sur la gestion des cyber-risques maritimes qui vise à protéger le transport maritime contre les cybermenaces. Elle promeut une évaluation de la sécurité des SI embarqués qui doit être effectuée en amont et de manière continue en mer pour être efficace. Cette circulaire pose la question de la maintenance à distance et du rôle des sous-traitants pour que l'ensemble de la chaîne de valeur soit conforme et cyber résiliente ;

- en juillet 2016, l'Union européenne a adopté la « directive NIS » qui prévoit que chaque État doit se doter d'une stratégie nationale en matière de sécurité des réseaux et des SI. Les opérateurs de services dits « essentiels » (OSE) doivent prendre des mesures techniques et organisationnelles pour gérer les risques qui pèsent sur la sécurité de leurs réseaux et de leurs systèmes. En vertu de son caractère essentiel, le secteur du transport maritime est directement concerné.

Un arsenal juridique français encore incomplet

En France, la législation se concentre davantage sur la cybersécurité des ports que celle des navires :

- La loi de programmation militaire (LPM) de 2013 pose les jalons en France de la cybersécurité appliquée à la filière maritime. Bien qu'elle ne concerne que les opérateurs d'importance vitale (OIV), la LPM sensibilise ces derniers à la sécurisation de leurs SI, conformément aux orientations du *Livre blanc sur la défense et la sécurité nationale* de la même année.

- un arrêté du Premier ministre précise en 2016 les dispositions de la LPM 2013, en fixant les mesures de sécurité spécifiques aux OIV du secteur « transports maritime et fluvial[22] » ;

- à l'automne 2018, la transposition en droit français de la directive NIS ouvre le cadre réglementaire de la cybersécurité du transport maritime aux autres acteurs que les OIV. Elle dote ainsi les compagnies maritimes, les logisticiens et les transitaires, entre autres, de règles de sécurité.

[21] Partie B, règle 8.3.
[22] « Transports maritime et fluvial », *Journal officiel* [en ligne], 11 août 2016.

La cybersécurité des SI embarqués souffre donc d'un vide juridique qu'il convient de pallier. Des réflexions et des bonnes pratiques ont toutefois déjà été initiées par la direction des Affaires maritimes (DAM) de l'ancien ministère de l'Environnement, de l'Énergie et de la Mer avec la publication en 2016 d'une série de trois guides[23]. À destination des acteurs maritimes, ces guides visent à sensibiliser sur « la prise en compte de la cybersécurité lors des contrôles de sûreté et de sécurité des navires ». L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a également fourni des travaux.

La filière maritime se confronte à des enjeux grandissants en matière de cybersécurité. Afin d'appréhender les nouvelles menaces liées à la numérisation croissante du transport maritime, il est indispensable que le secteur poursuive la diffusion en son sein d'une culture d'hygiène informatique destinée à protéger l'intégralité de sa chaîne de valeur. Outre l'adoption d'un cadre légal dédié à la cybersécurité des navires, les acteurs industriels pourraient de leur côté adopter une approche « *security by design* » des SI embarqués, dont la correction des vulnérabilités doit être effectuée tout au long du cycle de vie du bateau, dans le cadre du maintien en condition opérationnelle.

FOCUS INNOVATION

Cosmian : le calcul collaboratif de données chiffrées

Présentation

Fondée en 2018 par Sandrine Murcia, Raphael Auphan et Bruno Grieder, Cosmian est une startup française spécialisée dans la cryptographie et le calcul collaboratif de données chiffrées. Elle fournit un ensemble de solutions logicielles de « Privacy by Design » destinées à améliorer les processus de partage et de protection de données « sensibles » lors de leur traitement.

La technologie

Ces solutions permettent d'effectuer des calculs avec des données chiffrées. Cosmian en propose deux types :

- Des moteurs de chiffrement fonctionnels et homomorphes, qui permettent d'effectuer des calculs avec des données tout en fournissant, si besoin, le résultat chiffré.
- Une infrastructure sécurisée ou « Secure Enclave », qui permet d'isoler les données et codes du reste d'un système et ainsi de les préserver de toutes attaques extérieures ;

[23] « Cybersécurité maritime », *RP de la France auprès de l'OMI* [en ligne], 21 avril 2017.

Ces solutions rendent possible le calcul collaboratif à base de données chiffrées : les membres d'un réseau peuvent ainsi travailler sur des contenus sans révéler les données fournies par chacun.

Ces solutions sont accessibles principalement via des API et peuvent fonctionner en local aussi bien que dans un Cloud. Leur implémentation reste simple car elle prend la forme d'une brique logicielle intégrée à l'environnement du client et non intrusive. L'ensemble est donc transparent et permet d'avoir, au final, des solutions métiers sécurisées et enrichies (« empowered ») et de résoudre le « paradoxe de la protection des données » : être en mesure d'utiliser les données accessibles tout en respectant leur caractère privé.

Applications

Ces solutions permettent ainsi de protéger les données, algorithmes et codes utilisés lors de ces calculs. Elles peuvent être déployées dans une variété de secteurs :

- Banque et assurance : au sein d'un même groupe, les départements peuvent utiliser les données d'autres services sans enfreindre la confidentialité des données de leurs clients ;
- Finance : les données fournies par des entreprises tierces dans le cadre du processus KYC (know your customer) restent chiffrées ;
- Énergie : le chiffrement des données de consommation utilisées par les fournisseurs d'énergie pour prédire les comportements de consommation permet de renforcer la confidentialité de celles-ci ;
- Industrie : un fabricant d'équipement peut utiliser les données de fabrication de ses clients pour optimiser les chaînes de production de chacun d'entre eux tout en conservant la confidentialité des données de chaque client ;
- SOC : une équipe SOC peut échanger avec d'autres organisations afin de savoir si d'autres sociétés ont été victimes de la même attaque que celle dont elle fait l'objet, sans toutefois révéler aux autres qu'elle en est victime ;
- Technologie médicale : permet d'assurer la confidentialité des données médicales lorsqu'elles sont utilisées pour des analyses prédictives par exemple.
- La société collabore avec de nombreuses institutions de recherche comme l'ENS, le CNRS, l'INRIA ou l'Université Paris Sciences & Lettres.

Perspectives

La crise Covid-19 a mis en exergue le besoin d'espaces de travail interconnectés et sécurisés, que ce soit au niveau d'une entreprise, d'un pays ou à l'international. Les solutions de chiffrement retenues au cas par cas par chaque organisation permettent de garantir l'intégrité de leurs données tout en les partageant.

Le marché du calcul collaboratif de données chiffrées est relativement récent et encore en cours de consolidation. Certaines sociétés, notamment américaines et israéliennes, proposent des solutions similaires, mais adoptent une approche passant par un développement sur mesure, plus onéreuse et complexe qui limite leur déploiement aux entreprises dites stratégiques comme celles du secteur de la défense. Les solutions de

Cosmian ont pour objectifs de s'intégrer dans les environnements de production existants afin de pouvoir être utilisées massivement et par le plus grand nombre.

Actualités

En juin 2020, Cosmian a rejoint le Confidential Computing Consortium (CCC). Ses membres, parmi lesquels Google Cloud, Microsoft, Tencent et Huawei, ont pour objectif de former "une communauté open source dédiée à la définition et à l'accélération de l'adoption du Confidential Computing". Le CCC souhaite ainsi établir des normes et des outils permettant de chiffrer les données en cours d'utilisation, en particulier celles utilisées au sein des applications et des navigateurs web, qu'il considère comme étant les plus sensibles.

Au mois de janvier 2020, Cosmian a participé au CES (Consumer Electronics Show), au sein du Village by CA du Crédit Agricole.

CALENDRIER

1-31/10/2020 : Cybermoi/s 2020

Comme tous les ans, le mois d'octobre est consacré à la sensibilisation du grand public aux dangers du numérique. Projet collaboratif rassemblant une diversité d'acteurs de l'écosystème du numérique et de la cybersécurité, le "Cybermoi/s" met à disposition des internautes des contenus développés pour l'occasion sur les bonnes pratiques en matière de sécurité : hygiène numérique, bons réflexes, nouvelles tendances...

L'édition 2020 sera consacrée au chantage numérique. À travers une série d'événements et de conférences, le Cybermois aborde aussi les grands enjeux du moment et notamment le rançongiciel.

Retrouvez ici le programme de l'événement et la boîte à outils.

ACTUALITÉ

Lancement du « Diag Cyber »
Dispositif d'aide à la sécurisation cyber des PME et ETI de la défense

Géré par la Direction générale de l'armement (DGA), opéré par Bpifrance et financé par le ministère des Armées à hauteur de 4,5 millions d'euros, le Diagnostic Cyber Défense s'inscrit dans le cadre du plan Action PME.

Il se présente comme un ensemble de prestations d'audit et de conseil au profit des PME de la base industrielle et technologique de défense, et a pour objectif de les aider à identifier les risques numériques liés à leurs activités, à évaluer leur niveau de protection, détecter d'éventuelles failles, et si besoin mettre en place un plan de sécurisation. Ce dispositif doit permettre de renforcer la chaîne de valeur de la cyberdéfense de « bout en bout » et de réduire les vulnérabilités de l'écosystème de défense aux cyberattaques.

Les PME et ETI candidates seront présélectionnées sur la base de critères d'éligibilité validés par la DGA, et bénéficieront d'une prise en charge de 50% du coût de la prestation pour un montant maximal de 14 000 euros.

Ce dispositif sera déployé en 3 phases :

1. D'abord un audit d'analyse de risque conduit par l'ANSSI qui permettra d'identifier des objectifs de sécurité et d'élaborer un plan de remédiation ;
2. Ensuite, l'accompagnement à la mise en œuvre du plan de remédiation ;
3. Enfin, un audit final de vérification de la bonne mise en oeuvre du plan de remédiation.

Les entreprises intéressées peuvent déposer une demande sur la plate-forme suivante : www.demarches-simplifiées.fr/commencer/diagnostic-cyber-defense

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction générale des relations internationales et de la stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com