Journée des Chaires Cyber Interarmées

Cyberattaques: détection et réaction

Synthèse des interventions

Ecole Militaire, Paris
13/06/2019

Table des matières

Au cours de cette journée interchaires et au fil des conférences sur le thème général de la cybersécurité, les principaux sujets abordés ont été les suivants :

- Enjeux de capacité de réaction et souveraineté nationale
- Importance des partenariats public-privé et des interactions entre les mondes académiques, civils, militaires et de l'industrie
- Enjeux de passage à échelle, de maintien en conditions opérationnelles et de sécurité, et calcul de l'impact des vulnérabilités
- Les sondes souveraines : nouvelles perspectives
- La nécessité d'un système juridique clair et accessible régissant le cyberespace
- Identification et procès des cybercriminels
- Coopération internationale en matière de cybersécurité, répartition des compétences et formation
- Confiance interpersonnelle et collaboration machines/humains
- Fatigue cognitive et faculté d'adaptation en cyber-crise
- Capacité de résilience et de protection des données dans le domaine aérospatial

Matinée

Allocutions d'ouverture

Général de brigade aérienne Didier Tisseyre – Représentant du COMCYBER

Derrière les dysfonctionnements provoqués lors de crises cyber, ce n'est pas l'informatique en lui-même qui est visé, mais l'activité. Il faut être capable de réagir car cette activité nous est essentielle, quel que soit notre environnement. C'est en effet essentiel pour nos activités et, dans certains domaines, essentiel à la souveraineté de l'Etat : ce ne sont donc pas uniquement des enjeux financiers auxquels nous sommes confrontés, mais aussi des enjeux de survie.
Par conséquent, il faut être capable de réagir rapidement, ne pas se laisser imposer le rythme de son adversaire. L'enjeu majeur est donc l'anticipation. Et les échanges entre les différents acteurs, issus de la société civile et militaire, de tous les domaines, sont ce qui est réellement enrichissant et permettra d'avancer dans la résolution des défis auxquels nous faisons face actuellement.

Jean-Paul Laborde – Titulaire de la Chaire Cyber Saint-Cyr, Sogeti, Thales

La détection-réaction est au cœur de la matière cyber. Rien ne peut se faire et tout doit se faire, plus exactement, sous la coordination du COMCYBER. L'objectif ultime est de réagir contre l'impunité et de faire en sorte que les cybercriminels soient détectés et punis. La complémentarité entre chaires peut faire ressortir les éléments et forces de chacun, notamment les interactions entre les scientifiques et les acteurs juridiques. Nous ne pourrons jamais atteindre des avancées dans le milieu en ne mobilisant que des acteurs du public, c'est pourquoi les partenariats avec le privé sont essentiels (en ne se cantonnant pas aux relations de mécénat). Même dans les organisations internationales, des interactions avec le privé se mettent en place et sont primordiales. Le continuum public-privé est nécessaire : en sus de la coordination entre les chaires, les interactions entre public et privé (en respectant les prérogatives et tâches de chacun) sont fondamentales.

Paul Théron - Thales

Le cyber est un engagement de longue durée. Au vu des évolutions actuelles, l'avenir s'annonce complexe (combat en réseau, objets connectés de plus en plus nombreux, IA). Tous ces éléments laisseront l'opérateur humain un peu déconcerté : si aujourd'hui il sait superviser un réseau dont il connait la topologie et reconnaitre des micro-signes d'une attaque en cours, la tâche s'annonce plus ardue dans les futurs réseaux de combat. Dès lors, comment comprendre la complexité d'attaque dans des réseaux complexes et pondérer sa réaction ? L'opérateur humain sera dépassé. Comment l'aider à réagir dans une situation extraordinairement complexe et face à des attaques suivant des trajectoires très différentes de celles actuelles ?

Une piste pourrait être de travailler sur la notion de cyberdéfense autonome, sujet qui commence à intéresser bon nombre d'acteurs (ministère de la Défense américain, Agence européenne de défense, le gouvernement australien entre autres), dont la chaire cyber de l'Armée de l'Air. Cette chaire oriente ses travaux autour de trois axes de travail fondamentaux complémentaires :

- Le défi technologique majeur que représente la cyberdéfense autonome (rien ne surviendra avant 10 ans)

- Cette technologie de cyberdéfense autonome sera peut-être amenée à demander l'aide des « hommes » : il va falloir travailler sur la coopération cyber cognitive entre l'homme et les agents cyber autonomes.
- Il va falloir développer ces technologies, l'embarquer dans des systèmes, pour l'incorporer *in fine* dans les systèmes de défense.

Les coopérations entre le monde académique, la défense et l'industrie sont absolument indispensables : c'est une coopération de long terme qu'il faudra mettre en place.
Face au danger, l'homme est capable de se réadapter en quelques secondes et de prendre des décisions radicalement différentes de celles initialement prévues. Seulement, les agents autonomes n'ont pas cette capacité. Ainsi, si l'on veut éviter une troisième guerre mondiale, il faut travailler sur des mécanismes de *deep decision making* (combinant des mécanismes d'IA, mais pas seulement), ce qu'on ne sait faire à l'heure actuelle, pour que les agents soient efficaces et non dangereux. C'est un des douze défis lancés par la chaire, et ce n'est pas un acteur individuel mais une communauté qui pourra y parvenir.

Yvon Kermarrec – Titulaire de la chaire de cyberdéfense des systèmes navals

Les bateaux civils et militaires sont soumis à de nombreux aléas de diverses natures lors de la résolution de leurs missions. Pour le marin, la sécurité est un enjeu majeur, si bien d'un point de vue technique que pour les équipages. Les bateaux sont désormais connectés, dotés de différents capteurs et systèmes, qui lui permettent de communiquer avec son environnement et avec les stations au sol, et d'optimiser ses missions. Ces révolutions numériques s'accompagnent de nouvelles vulnérabilités et formes de défaillances. De nombreuses attaques informatiques se sont développées ces dernières années (mauvais signaux GPS orientant les bateaux vers des zones difficiles, informations transmises par les stations au sol falsifiées conditionnant des mauvaises prises de décision).
La marine est une armée technique et scientifique, qui a pris en compte les aspects cybersécurité il y a plusieurs années. Parmi les missions de la chaire, deux missions principales se distinguent :

- Celle de la recherche : moyens de trouver de nouveaux mécanismes pour détecter et protéger de nouveaux équipements toujours plus complexes.
- Celle de la formation, primordiales car les personnes doivent être formées à la cybersécurité

Les formes de coopération entre les divers acteurs permettent d'établir de nouveaux relais et vecteurs pour renforcer les capacités en cybersécurité. Les challenges sont nombreux et la cybersécurité dans le milieu maritime émerge comme un nouvel enjeu, pour assurer la sécurité des personnes et des biens.

Table ronde 1 : Cybersécurité dans le contexte maritime : enjeux et opportunités

Loïc Lagadec – Professeur, adjoint au directeur scientifique, en charge de la cybersécurité, ENSTA Bretagne

Le domaine maritime est particulier à cause de l'environnement mouvant dans lequel évoluent les dispositifs. Cette table ronde permettra donc de se focaliser sur les enjeux et perspectives du domaine.
Les flottes de navires soulèvent des problématiques de passage à l'échelle. Il s'agit d'enjeux importants car représentant des problématiques complexes de systèmes à systèmes, d'enjeu de mobilisation d'acteurs multiples (par leur nombre, leur type, leur rôle dans le processus). Enfin, on va également avoir des problématiques de maintien en conditions opérationnelles (temps plus long dans le milieu militaire que dans

le civil) et en conditions de sécurité, car sans sécurité le maintien opérationnel est impossible. De fait, si l'on arrive à isoler certaines parties du navire, ou à agir sur les dispositifs permettant la gouverne du bateau, cela devient dangereux. Le maintien en condition de sécurité impose donc d'avoir des solutions, alors même que l'on ne solutionne pas des problèmes encore non-identifiés. L'enjeu de cette table ronde est donc de parvenir à cette identification à la fois de problèmes et de solutions *ad hoc*, leurs apports et leurs limites.

Capitaine de Vaisseau Jérôme Augusseau – Marine Nationale, coordinateur cyber et OSSI-C

La Marine compte environ 200 bateaux, dont une centaine de gros bâtiments. Ce qui la caractérise, c'est la variabilité : elle est multiple en termes de tonnage, de nombre de personnes à bord des bâtiments et en termes d'ancienneté.

- ***MCO (Maintien en condition opérationnelle de la flotte) VS MCS (Maintien en conditions de sécurité)***

Le MCO dans la Marine est focalisé sur les périodes à quai, et se concentre globalement sur une période par an (un arrêt technique majeur). On distingue la maintenance préventive de la maintenance corrective, le tout prenant part à un système complexe.
Il a été choisi d'inscrire le MCS dans le MCO, pour ne pas dupliquer les structures. Mais les processus du MCS ne sont pas tout à fait les mêmes que ceux du MCO. On a des problématiques de qualification du MCS, mais aussi des problématiques de traduction des obligations et usages du MCO dans le MCS. Par ailleurs, le MCS et le MCO agissent sur des temporalités différentes : les pratiques se font sur le temps court pour l'un (MCS sur 5 ou 10 ans), beaucoup plus long pour l'autre.
Les pratiques du MCS sont claires et connues, expliquées par l'ANSSI, mais s'appliquent au monde de l'informatique, alors que pour les bateaux la compréhension est beaucoup plus complexe. Des outils sont donc nécessaires pour progresser dans le domaine.

Les bateaux sont des systèmes de systèmes : les navires sont caractérisés par une certaine complexité, et pour des histoires d'économies et d'efficience, l'ensemble des systèmes a été numérisé. Mais en plus de cela, d'autres systèmes peuvent venir se greffer à bord. A-t-on l'assurance que sur de tels bâtiment, on trouve une ségrégation des réseaux ? La marine travaille pour mettre en place des accès aux réseaux, mais il n'y a pas d'interpénétration entre sphères privée et professionnelle. Le sujet reste maitrisé et selon les missions, les téléphones, appareils divers sont autorisés ou non.
A côté de la partie numérique, on trouve des systèmes industriels (pompes, vérins, missiles). On a donc une diversité technologique duale et complexe. La dualité permet de réduire les coûts, mais fait également que toutes les techniques sont connues dans le monde civil : il est donc nécessaire de penser des systèmes de défense pour parer toute attaque, car c'est une source de vulnérabilité supplémentaire.
Enfin, une dernière particularité dans la Marine réside en le fait qu'au-delà de la difficulté technique, on a aussi une difficulté organisationnelle, dans la mesure où les maitrises d'ouvrage varient en fonction du temps et des périmètres.

- ***MCO dans la Marine nationale : cybersécurité dans ces processus ?***

Tout problème complexe se subdivisant en sous-problèmes compliqués, le problème central a donc été découpé en divers processus, afin de détailler le MCO dans la marine et les évolutions à court terme.
Le **premier processus** est la **cartographie** physique (architecture), logique (maitrise des flux) et applicative. Pour avoir ces cartographies, il faut travailler en collaboration avec les industriels, pour partager les mêmes outils dans cette cartographie. Avec l'IA et le big data, il y a des voies de recherche très intéressantes qui s'ouvrent.

Le **deuxième processus** est la **restauration** : on a besoin de capacité de restauration pour avoir une autonomie à la mer.
Puis, le **troisième processus** est le **durcissement**, pour limiter la surface d'attaque, car plus on restreint le nombre de logiciels utiles, moins on a de MCS à faire.
Le **quatrième point** concerne le **suivi des vulnérabilités**. Globalement, on a 180 000 vulnérabilités, on ne peut donc pas tout traiter manuellement. On peut également les classer par effets : reste uniquement une utilisation d'OS ou d'application contraire à ce qui a été prévu initialement. A l'heure actuelle, la Marine identifie des centaines de vulnérabilités par an : il va donc falloir se focaliser sur les points importants car tout mettre à jour sera impossible (Microsoft, Linux et produits de sécurité).
Le **cinquième point** est la **détection des anomalies**. Elle relève du MCS, et pour la Marine on se focalise sur le cloisonnement des réseaux, la maitrise des flux et la défense en profondeur. Les bateaux sont raccordés à des réseaux de classification différents du Ministère (intradef/intraced/rifan). Toutes les anomalies détectées seront renvoyées à un SOC défense qui va les traiter en apportant une expertise.
Enfin, le **dernier point** est la **mise à niveau logiciel** : avoir un cloisonnement des réseaux, avoir des outils up-to-date, assumer le risque…

Bastien Sultan – Doctorant de la chaire cyberdéfense des systèmes navals

Ce que la chaire propose au niveau prospectif est un processus de maintien en conditions de sécurité ayant pour visée principale le calcul de l'impact que va avoir une vulnérabilité, son exploitation ou une contre-mesure (patch logiciel ou contre-mesure organisationnelle) sur la capacité du système à accomplir ses missions. Car le nerf de la guerre dans ces systèmes est principalement d'assurer la disponibilité des systèmes et leur capacité à accomplir leurs fonctions. Pour cela, la chaire a 3 missions principales :

- L'établissement d'une modélisation la plus fidèle possible, établie *ab initio* et maintenue sur toute la durée de vie du système (documents d'architecture, workflows, topologie des réseaux, qui vont permettre de modéliser les missions et mettre en évidence les liens entre les constituants des systèmes, les fonctions et les missions).
- La création d'un outil de veille des vulnérabilités et contre-mesures. Un robot agrégeant les informations des sources complémentaires en temps réel a été développé, pour permettre de détecter quelles sont les fonctions vulnérables sur les systèmes à tout moment. Cet outil de veille permet d'établir une corrélation entre les vulnérabilités et les processus métier, pour identifier les systèmes vulnérables. C'est moyennant la connaissance de notre système que la veille de vulnérabilité va pourvoir être correctement effectuée.
- L'établissement d'une méthodologie et une métrique pour calculer les impacts que peuvent avoir une vulnérabilité, une attaque, et une contre-mesure sur les missions du système. Le parti a été pris d'établir une mesure comparable, pour faciliter le traitement au niveau des organismes chargés du maintien en conditions de sécurité, car cela permet de hiérarchiser les correctifs entre eux et avec les vulnérabilités, et d'avoir un ensemble d'indicateurs comparables pour faciliter la prise de décision. Ce qui est assez fréquent dans la littérature scientifique concernant les mesures d'impact, c'est l'impact financier.

Ce que l'on obtient à l'issue de la modélisation, ce sont des modèles formels. L'approche est pour le moment semi-outillée, semi-humaine. Enfin, une analyse d'impact de la contre-mesure est également réalisée, pour aider au processus de qualification. En termes de coûts, cela reste une partie inexplorée. Des outils et processus existent déjà en la matière, et il n'a pas été considéré qu'une approche innovante pourrait être apportée.

Patrick Hébard – Naval Group, Responsable recherche et innovation cybersécurité et cyberdéfense

Détection et réaction sont à replacer dans un modèle : le modèle américain ou cybersecurity framework du NIST, construit autour de 5 grands piliers :

1. **L'identification**, des systèmes et des risques. Il est fondamental de définir et d'identifier tous les systèmes numériques.
2. **La protection**, et notamment la défense en profondeur et l'application de la réglementation sur les systèmes de défense. Mais se limiter à la protection n'est pas suffisant.
3. **La détection** (des situations anormales, pas forcément des cyberattaques). Dans ce domaine-ci, l'IA peut aider.
4. **La gestion de crise**, plus compliquée sur des navires, surtout des navires militaires qui peuvent être éloignés.
5. **La remédiation**, c'est-à-dire remettre le système en état, une fois les failles identifiées, matérialisation du système de résilience.

Ces 5 piliers ont permis à un changement de paradigme de s'opérer.

On parle beaucoup d'IA concernant la détection, un sujet à la fois récent et ancien. C'est un vrai sujet de recherche aujourd'hui que d'arriver à utiliser des agents intelligents, avec du *deep learning* ou *machine learning*, pour essayer d'acquérir un modèle intelligent de fonctionnement qui permettrait en temps réel de détecter les déviations par rapport à un modèle de référence. Les puissances de calcul mises en œuvre sont considérables.
On se rend compte que les systèmes de systèmes sont un sujet complexe. Mais on s'aperçoit qu'il faut avoir de la finesse quant aux technologies, car l'application aux systèmes industriels de l'IA fonctionne moins bien que sur l'IT. Un système industriel est un système très déterministe avec des capteurs et des actionneurs, qui effectue toujours les mêmes tâches, et est initialement très peu armé contre les cyberattaques (la logique historique ne prévoyait pas de lutter contre les menaces). Si on veut leurrer le système, on peut leurrer le capteur, ce qui corrompra l'ensemble du système.
On n'est pas seulement dans le monde numérique mais aussi dans le monde réel, et c'est pourquoi il faut être très vigilant aux anomalies, car modifier la température de l'huile ou changer la vitesse de rotation moteurs, in fine, ce n'est pas une attaque cyber, mais cela peut créer un bruitage lors du déplacement d'un sous-marin censé être parfaitement silencieux. Les conséquences opérationnelles peuvent être importantes.
Les outils d'IA ne semblent donc pas particulièrement adaptés compte tenu de l'effet final recherché. En revanche, d'autres études sont en cours mettant en scène des moyens beaucoup plus classiques tels que la modélisation par réseaux de Petri ou par graphes temporels, qui sont très bien adaptés aux systèmes industriels. On cherche donc à combiner les approches IA avec ces approches plus traditionnelles pour atteindre une efficacité maximale dans la détection des anomalies.
Les perspectives sont de continuer la validation des *proof of concept* qu'on a à la fois sur de l'hybridation entre des agents intelligents qui font du *machine* et *deep learning* et de la modélisation par réseaux de Petri, plus souple à faire pour de la détection en temps réel. Les graphes temporalisés semblent par conséquent, pour l'outil, des solutions toute à fait intéressantes.

Philippe Leroy – Thales, Spécialiste senior cyber, chargé de mission PEC et chaires cyber

Le cyber devient un sujet totalement prégnant. Thales est maintenant un grand fournisseur de l'Etat, seule société capable de fournir des produits de protection de données de classe gouvernementale. Thales est très actif pour fabriquer ces produits concrètement qui vont permettre de protéger et de détecter ces attaques au

plus près de l'attaquant. La dimension humaine devient essentielle : des personnes surveillent en temps réel des réseaux face à des incidents surprenants.
L'attaquant, de manière plus ou moins mathématique, a toujours un temps d'avance (dans la mesure où il fait de la veille sur sa cible et de l'exploitation de sources ouvertes, notamment des informations postées sur internet par les industriels eux-mêmes). Aujourd'hui, il faut être assez mature pour ne pas divulguer d'informations qui pourraient faciliter des chemins d'attaque.
Les produits mis au point par Thales à la demande du gouvernement, bien souvent, sont au cœur de la réglementation. Thales est au cœur du *hunting* et s'attache donc à équiper les acteurs en matière de protection, notamment au travers de deux marchés :

- Le marché des sondes souveraines, à savoir des sondes alimentées par des informations de confiance, architecturées pour être installées dans des réseaux et être invisibles tout en remontant les informations requises, et auto-protégées contre des tentatives d'inhibition. Les sondes commandées sont des sondes pour l'IT.
  Ces sondes sont censées observer de façon discrète l'intégralité de ce qu'il se passe dans un réseau pour en remonter les anomalies, ce qui nécessite au préalable une phase de formation.
- La détection maitrisée, qui passe par des produits mais surtout des compétences humaines (pour qu'une fois confrontés aux attaques, les acteurs sachent maitriser les outils).

A la fin de la pyramide de sonde, on voit une obligation de veille et d'analyse permanente et continue de la menace, mais aussi, du côté client, l'obligation d'une certaine visibilité sur leur conception de l'IA (que veulent-ils développer, quels sont leurs moyens ?).

- ***Quel est l'apport de l'IA pour la cyberdétection? Retex d'opération de hunting***

L'IA n'est pas un phénomène nouveau, mais plutôt un phénomène qui fait le buzz, car la puissance de l'IA permet des avancées significatives pour des processus de traitement de base de données géantes, mais aussi permettra d'améliorer les performances, temps de traitement et interprétations potentielles pour l'aide à la prise de décision, vecteur qui facilitera la détection.
L'IA, sur les URL identifiées comme malveillantes, va permettre d'augmenter les capacités de détection et de défense (alors qu'à l'heure actuelle, près des deux tiers de ces URL ne sont pas détectées par les firewall). Il va donc y avoir des modèles d'IA spécifiques à chaque phase de la Kill Chain[1], les sondes révélant les actions que l'attaquant sera en train de mener. Grâce à l'IA, on va pouvoir extraire les flux anormaux, les mettre en exergue, pour qu'ensuite l'humain puisse reprendre la main et matérialiser l'origine de l'attaque. En résumé, l'IA va grandement faciliter la détection d'attaques classiques, grâce aux sondes.

[1] Etapes de la kill chain : reconnaissance, weaponisation, delivery, exploitation, installation, command and control, actions on objective.

Après-midi

Table ronde 2 : Scénario et réponses juridiques

Gilles Guiheux – Directeur du CREC Saint-Cyr

Sciences dures et sociales en cyber sont parfaitement compatibles. La dimension juridique en cyber est un élément clé de la souveraineté. Mais cette approche se fait dans la complexité et le droit. L'intelligibilité requiert un système marqué par la clarté et l'accessibilité, tant en droit interne qu'international. Le problème est que nous sommes très peu armés, parfois même désarmés. Il y a donc une grande conception juridique doctrinale à avoir.

Cybermenaces et vulnérabilités

Olivier Kempf – Conseil en stratégie digitale

Qui est menacé et qui menace ? A cette question, une réponse simple : tout le monde. Différentes typologies peuvent être établies (acteurs étatiques, Etats ou organisations internationales, réseaux mafieux, …). Mais on observe une véritable hybridation des acteurs, qui sème le trouble chez les juristes. La cybercriminalité s'est peu à peu imposée comme un nouveau type d'agression. Il y a une continuité dans la menace. En droit interne, le juriste se trouve donc désarçonné car il va devoir organiser un continuum qui n'existait pas auparavant. Avec la mondialisation et la montée en puissance des GAFA, le problème se pose également au niveau international. L'intégration du public et du privé à ce niveau pose elle aussi de nombreux problèmes. Cela fait ainsi 20 ans que l'on essaye de dresser un droit du cyber espace mais les solutions ne se dessinent pas si facilement.

Il y a deux grandes catégories de mobiles :

- Soit l'on mène une attaque cyber car on souhaite en retirer un **avantage personnel**.

D'une part, il existe une sorte de compétition dans le domaine, et ce goût de la compétition est une profonde incitation à réaliser des attaques. D'autre part, la question du savoir et de la connaissance est également un objectif connu. On pourrait alors assimiler cette dimension du cyber au renseignement. Mais cette connaissance n'est pas seulement réservée aux acteurs étatiques. Enfin, une dernière motivation se distingue en la perspective du gain financier.

- Soit l'unique intention est d'**être hostile** et de faire du mal à l'adversaire visé (augmenter sa réputation, son score sur les plateformes de hacking).

On peut très bien penser à des concurrents voulant gagner du terrain sur un marché, ou à des Etats malveillants. A cela s'ajoute les desseins d'influence (de COMEX, ou encore de PDG).

Il n'y a pas de sécurité à 100%. On a toutefois pu observer ces dernières années une montée en puissance de la protection, en parallèle de la recrudescence des agressions.

Enfin, plusieurs enjeux mettent en difficulté la cybersécurité :

- Le manque « d'éducation informatique »
- Les fautes de sécurité
- La crédulité
- La négligence (manque d'actions contre les actions d'influence)
- Le sous-dimensionnement : les PME ne sont pas sensibilisées aux problématiques de cybersécurité.

- Une réactivité excessive : le but de l'attaque n'était peut-être pas de porter préjudice, mais plutôt de tester les réactions pour identifier le type de réponse pouvant être fournie, dans l'optique de préparer une autre attaque de plus grande ampleur.

La riposte juridique aux cyberattaques est-elle pertinente ?

Maitre Cécile Doutriaux – Avocate

La cybersécurité est une catégorie juridique transverse. Il y avait une appréhension au départ autour de ces enjeux, mais désormais, la question des réglementations ne pose plus un problème particulier aux juristes.
Si l'attaquant ne se préoccupe pas du droit, dans le cas des armées, l'aspect juridique est important : jusqu'où peut-on aller, dans quel cadre peut-on agir, à quel moment dépassons-nous les limites ?
Il existe une zone floue, majoritairement en matière de renseignement : tout ce qui n'est pas interdit par la loi est-il autorisé ? Dès lors, ce n'est plus tant une question de droit que de morale. La question de la loi est essentielle et incontournable.
La question de la riposte et de la répression des délinquants a été abordée par le législateur. Cependant, le législateur a évolué, et un fossé s'est créé entre ses attentes et la réalité judiciaire. On a, à 5 reprises, augmenté le quantum de la loi. Toutefois, on ne sait toujours pas réprimer à 100% la fraude informatique et la question de l'identification de l'auteur est toujours ce qui pose problème dans les faits. Cinq lois différentes ont été votées depuis 1988 : le législateur avait donc beaucoup d'ardeur et l'envie de légiférer en la matière mais, en parallèle, les juges n'ont pas suivi et les peines sur le terrain judiciaire sont restées assez légères. Dans les faits, des problèmes restent à régler. Le RGPD a permis une première avancée (la France était à ce moment déjà en avance sur les travaux en cours). La France a eu la possibilité d'ajuster cette réglementation européenne : cela a été fait par la loi du 23 juin 2018.

Par ailleurs, la difficulté est que sur le terrain judiciaire, des solutions existent, mais encore faut-il vouloir les mettre en place. La réalité est que la réponse sera davantage technique que juridique. Le législateur a été en phase avec le terrain dans le cadre de la LPM, en permettant l'utilisation des sondes évoquées plus tôt. Cette réponse réglementaire, en autorisant la pause de ces sondes, permettra aux industriels de continuer à développer des solutions et à avoir recours à l'IA pour détecter ces attaques, tout cela en étant encadré par la loi. Une charte éthique a d'ailleurs été publiée, avec comme objectif de concurrencer la Chine et les USA, en réglementant l'ensemble de ces pratiques. Une des questions principales est donc celle de la qualification stratégique.
L'éthique est une approche positive des comportements que nous aurons à avoir, afin de nourrir notre réponse.

La coopération internationale

Jean-Paul Laborde – Titulaire de la Caire cyber Saint-Cyr, Sogeti, Thales

Le cheminement qui a été fait concernant le terrorisme est similaire à celui que suit aujourd'hui la cyber sécurité. Initialement, personne ne voulait travailler sur le terrorisme, car chacun avait ses intérêts propres. Mais finalement, cela s'est fait : les chefs d'Etats eux-mêmes ont initié le vote de la résolution 2178. Le même scénario s'est dessiné concernant l'usage d'internet par les terroristes. La menace était réellement forte, ce qui a conditionné une action collective.
C'est donc de la même manière qu'il faut travailler la question de la cybersécurité au niveau international, sinon nous n'atteindrons jamais le niveau de coopération souhaité.

La criminalité transnationale organisée génère beaucoup d'argent par le biais de la cybersécurité. C'est aussi, dans ce champ, une question de morale qui se pose, ce que le juge n'apprécie pas. Une vraie politique internationale est nécessaire, afin de pouvoir créer par la suite les outils requis. Seulement, tant que le conseil de sécurité ne sera pas convaincu de cette vision, cela ne fonctionnera pas.

Quelle que soit la menace, on est pris au piège dans notre propre système, car lorsque l'on réprime cette menace, il faut tout de même rester dans le cadre de l'Etat de droit ! L'enjeu serait alors de se mettre d'accord sur les définitions entourant la cybersécurité. Deux textes prévalent en la matière :

- La convention de Palerme
- La convention sur la cybersécurité du Conseil de l'Europe.

Au Conseil de l'Europe se pose la question de la collaboration : un protocole a été mis en place, mais des problèmes techniques se posent. Qui est compétent ? Si les différents acteurs européens sont parvenus à se mettre d'accord, au niveau international, la tâche reste toujours compliquée. Des accords interétatiques et même inter-judiciaires doivent être développés. Mais pour ce faire, le problème majeur (surtout à l'étranger) concerne la formation, l'éducation, même. A partir du moment où ces éléments sont en jeu, le premier effort réside dans la politique internationale de coopération, puis la compréhension des textes et enfin l'éducation des juges.
Certains Etats sont très résistants au Conseil de l'Europe, pourtant ouverts à tous les pays du monde. Dans cette optique, il est improbable à l'heure actuelle de parvenir à une convention internationale. C'est pourquoi il faudrait prendre exemple sur la convention de Palerme, qui a une valeur pratiquement universelle (avec 170 Etats signataires) et a valeur de modèle dans le domaine.

En matière de cybersécurité, un constat assez frappant semble s'imposer, celui que la population est en réalité scindée en deux groupes distincts : ceux qui veulent la gouvernance numérique, et ceux qui veulent la gouvernance du numérique. Aujourd'hui, il n'y a pas de gouvernance mondiale, et celui qui parviendra à l'imposer sera celui qui tapera du poing sur la table.
Nous sommes confrontés à une frontière entre le droit des conflits armées, et le droit commun (droit de la paix). Seulement, dès lors que l'on sort du droit des conflits armés, les acteurs de la cyberdéfense sont vulnérables.

Enfin, il est absolument nécessaire de prendre en compte la notion d'acceptabilité sociale, par les citoyens : à quel moment accepte-t-on l'application du droit ? Il s'agit d'une dimension qui posera problème, car au-delà de la question des normes surgira alors celle de l'utilité.

Table ronde 3 : La cyber-résilience comme capacité d'anticipation et de réaction en situations de cybercrise

Pierre Barbaroux – Ecole de l'air, co-titulaire chaire Cyb'Air

L'une des pistes de recherche de la chaire est de questionner la spécificité de la résilience dans ces milieux de niches. Des cadres sur la fiabilité organisationnelle existent, il faut alors se poser la question de l'applicabilité de ces modèles en ce qui concerne la cyber résilience, sans toutefois prétendre qu'il y ait des spécificités. Les opérateurs immergés dans les systèmes sont les principales cibles dans la mesure où le but final recherché est bien souvent de modifier les capacités cognitives et organisationnelles de ces derniers.

Confiance interpersonnelle, collaboration et cyber-résilience

Florent Bollon – Doctorant, Chaire Cyb'Air

La confiance interpersonnelle est primordiale dans les relations de résolution dans le domaine cyber.
On ne peut pas agir dans le monde cyber sans opérateur humain : c'est toujours un opérateur humain qui prend la décision finale d'agir ou non.
La confiance interpersonnelle désigne l'évaluation de la fiabilité et de la loyauté du tiers. Pour qu'il y ait la mise en place d'un niveau de confiance, il faut à minima trois choses :

1. Une personne qui fait confiance, un opérateur humain. Le *truster*, qui définit le niveau de confiance, et est caractérisé uniquement par ce crédit de confiance qu'il est capable d'accorder à un opérateur
2. Une personne qui est la cible du lien de confiance, autre opérateur humain ou système cyber. Le *trustee* est caractérisé tout d'abord par ses stéréotypes et par l'évaluation de sa fiabilité. Les attributs de la fiabilité sont de trois types : la capacité, l'intégrité et la bienveillance. Est-ce qu'il est capable de réaliser une tâche dans un temps donné, et était-ce la tâche qu'il devait accomplir pour faire augmenter une situation ?
3. Une situation (qui va déterminer un niveau de risque)

Dans la littérature, le niveau de confiance évolue avec le temps, dans la mesure où plus l'on a d'interactions avec une personne, plus l'on a confiance ou non en elle. Seulement, les attaques cyber sont de très courtes durées et doivent être résolues très vite (une journée maximum) : le problème est alors que le niveau de confiance n'a pas le temps d'évoluer. Dans ce contexte, ce niveau de confiance évolue en fonction de deux facteurs uniquement : la propension du *truster* à faire confiance, et les stéréotypes.

<u>Deux types de situations ont été étudiées :</u>

- Une première situation où le trustee et le truster ont relativement les mêmes informations
- Un autre cas de figure dans lequel il y a une dissonance entre les informations

Le but était de savoir lorsqu'il y a dissonance ou concordance, ce qu'il se passe dans le domaine cyber (selon que l'on a confiance ou non en son interlocuteur).
En étudiant ces deux situations différentes, il est apparu que dans le cas d'une concordance des informations, le niveau de confiance ne rentre pas en jeu. Mais lorsqu'il y a une dissonance, le niveau de confiance entre en jeu : quand la personne n'a pas confiance en son interlocuteur elle a du mal à valider ses dires, alors qu'elle a tendance à le faire plus facilement lorsqu'elle lui fait confiance.
Mais les mécanismes de confiance interpersonnelle dépendent également de la spécialité et surtout de l'expérience : les personnes parties en OPEX se méfient plus facilement de leurs interlocuteurs et n'arrivent pas à agir selon les mécanismes de confiance interpersonnelle mis en place.
Ce qui est maintenant envisagé, c'est de voir ce qu'il va se passer dans une situation de dissonance entre ce qui ressort d'un algorithme d'IA ou des sondes, ce que ressort une personne digne ou non de confiance, et l'action de l'opérateur humain.

Fatigue cognitive et résilience des opérateurs en situation de cyber-crise

Mick Salomone – Doctorant, Chaire Cyb'Air

Comment rendre un individu plus résilient dans un cadre de cyber crise, notamment en traitant le problème de la fatigue cognitive ?
Notons d'abord que la résilience est la capacité du système à s'adapter et à gérer une situation imprévue dans le but de continuer une mission. Elle peut être améliorée de différentes façons :

- Dans sa dimension technique : améliorer la défense d'un système afin qu'il soit plus apte à réagir en cas de cyber attaque.
- Dans sa dimension organisationnelle, et donc humaine. L'homme peut en effet être la cible de cyber attaques directement, mais aussi et surtout car il interagit directement avec la machine qui peut être ciblée. Si on veut améliorer la résilience d'un système sociotechnique, il faut aussi prendre en compte cette deuxième dimension.

La fatigue cognitive a donc été identifiée, et définit comme un type de fatigue, comprise en tant que concept multidimensionnel. Il s'agit d'une fatigue mentale présente dès lors que l'on soutient un effort cognitif de manière prolongée. Comment cet effort cognitif peut-il être déclenché, dans une situation opérationnelle ?
L'environnement numérique, originellement, nécessite un effort considérable à cause du nombre d'informations à traiter. De plus, cet effort devient beaucoup plus important dans une situation de cyberattaque, dans la mesure où l'opérateur ne comprend pas le système dans lequel il évolue et a des difficultés à identifier ce qu'il se passe, et aussi car ça va davantage augmenter le nombre d'informations à traiter. S'ajoutent à cela des états limitants les ressources cognitives à disposition de l'opérateur tels que la fatigue et le stress.
Il existe alors trois processus de résilience :

- L'inhibition, ou la capacité à réprimer des comportements automatiques
- La flexibilité mentale, ou la capacité à changer d'idée, de stratégie, de comportement afin d'atteindre un objectif
- La mise à jour, manipulation des informations en mémoire ou la capacité de mémoriser tout en faisait autre chose en même temps.

Ces processus de résilience sont la base de processus cognitifs de plus haut niveau, qu'il faut nécessairement mobiliser lors d'une cyber crise (le raisonnement, la résolution de problèmes, et la planification).

Les objectifs sont alors de parvenir à caractériser les effets de la fatigue cognitive sur les capacités d'adaptation (fonction exécutive) pour mieux comprendre les comportements inadaptés observés sous l'effet de la fatigue. On cherche également à observer les corrélats cérébraux de cette fatigue-là, car il y a une nécessité de les identifier pour savoir quand l'opérateur est réellement fatigué cognitivement. L'intérêt, c'est de pouvoir donner des briques à la création d'interfaces cerveau-machine plus performants, d'adapter l'environnement et de mieux penser l'ergonomie des interfaces afin qu'elle soit adaptée à ce type de situations dégradées.

In fine, ce qu'il ressort de ces études, c'est que même fatigués, les opérateurs humains sont toujours capables de réagir. Seulement, les incapacités d'adaptation sont réelles : même si les opérateurs savent réagir, ils ne savent plus anticiper. Savoir cela permettra dès lors d'orienter les opérateurs sur le comportement à avoir une fois qu'ils sont fatigués cognitivement parlant.

Cyber-résilience aérospatiale : la vision du Groupe Thales

Jean-Pierre Faye – Thales Group

Le RETEX de l'opération ORCHARD (2007), menée par les Israéliens contre la Syrie, a permis certaines avancées. Un des éléments de succès de cette attaque a été le blanchiment des détections syriennes radar au travers d'un logiciel placé dans les centres de commandement, qui a permis que les opérations de détection ne soient pas visibles par les opérateurs. Cela pose des questions sur la méthode. Il n'y a jamais de protection cyber 100% efficace. Néanmoins, lorsque les opérateurs sont confrontés à des situations inédites, ils sont incapables de réagir et ne savent pas ce qu'il se passe. Leurs réactions ne sont pas homogènes : il y a un fort besoin de formation pour qu'ils puissent réagir. Se pose alors la question de l'information à présenter : quel outil mettre à disposition ? Comment organiser le processus de décision à plusieurs ?

Le problème de la protection des données apparait alors en filigrane car les fausses données génèrent de fausses actions. Les mécanismes développés pour assurer des vérifications et corrélations entre données vont donc être importants, tout autant que la formation des agents chargés d'interpréter ces anomalies dans les données reçues.

Cyber-résilience aérospatiale : la vision de Dassault Aviation

Bruno Ramirez – Dassault aviation

Le contexte aéronautique est complexe : il y a l'avion, mais ce dernier n'est pas seul et il est également important de considérer son environnement, c'est-à-dire les équipes au sol, en direct, ou en différé. Un avion est composé des systèmes permettant le pilotage de la machine, le déroulement de la mission, la gestion de l'armement et les communications. Ces systèmes ont vocation à communiquer entre eux. Tout comme dans la Marine, les temps de vie des avions sont longs. Mais ils sont, de base, assez résistants aux failles (pannes, disfonctionnements, pertes d'équipement) grâce à un certain nombre de solutions développées, avec certains cloisonnements et mécanismes d'isolements entre eux qui forment une bonne base de protection.
Quels sont les évènements redoutés en cas d'attaques cyber ?

- La sécurité des vols (perte de l'avion ou de son équipage)
- La non-réussite ou altération des résultats de la mission
- La compromission des données

Le fait est que nous avons toujours besoin de plus d'inter connectivité, de systèmes de plus en plus performants, de reposer sur des technologies grand-public qui offrent davantage de puissance de calcul, où la thématique de la cybersécurité se pose.

Si le pilote d'un avion ne sera pas formé à la cybersécurité, on va toutefois lui enseigner à réagir en cas d'attaque. Les questions sont alors de savoir comment apporter des éléments de décision à un équipage qui se trouve seul face au fait et doit prendre une décision, sans avoir été formé et dans l'urgence. On va donc chercher à augmenter les capacités de robustesse et de résilience.
Un autre point important également est la capacité à estimer les impacts. Dans l'idéal, il faudrait donner à l'utilisateur un moyen lui permettant de savoir sur la base de l'IA et des technologies ce qu'il a observé, l'ampleur des impacts, et ce qu'il est possible de faire en conséquence. Il faut pouvoir proposer une aide synthétique, non binaire, qui va établir un indice de confiance. Il s'agit donc bien d'une relation de confiance entre une machine qui va être capable de faire des prévisions, et un pilote qui a besoin d'un support simple et va adapter sa mission et son comportement à ce rendu.

Les bancs d'intégration peuvent servir pour faire des tests d'intrusion et appréhender une partie de la contribution de cet équipement à la réussite de la défense contre une attaque informatique, en attendant que les jumeaux numériques soient plus accessibles.
En conclusion, l'aide à la prise de décision pour un utilisateur, formé ou non, et l'aptitude à modérer la gravité d'une attaque au vu du contexte informatique dans lequel se trouve l'équipement, sont des axes à développer tout particulièrement. Les notions de connaissance d'ensemble du système, et de rôle d'architecte mais aussi de simulation et d'anticipation sont toutes trois importantes.

Bilan et perspectives

Yvon Kermarrec – Titulaire de la chaire de cyberdéfense des systèmes navals

Les thématiques abordées intéressent si bien les chercheurs que les industriels. Les résultats sont concrétisés avec une visibilité renforcée, et des éléments objectifs en termes de doctorats soutenus et le nombre de thèses en cours à ce jour.
Les perspectives de la Chaire cyber sont diverses :

- Une troisième phase de la chaire sur la période 2020-2023 et les renforcements des liens entre les partenaires de la chaire.
- De nouveaux cours et de nouvelles formations académiques
- Un mastère cybersécurité appliqué à la Marine à venir

Il y a des complémentarités qui apparaissent, les coopérations des chaires militaires sont actées, et parmi les thèmes et les problématiques abordées, on peut voir que les ouvertures peuvent intéresser d'autres groupes, en particulier les grands industriels.

Pierre Barbaroux – Ecole de l'air, co-titulaire chaire Cyb'Air

Les perspectives à court terme de la chaire sont essentiellement d'initier une évolution du programme de recherche pour le faire vivre, d'engager un retour pour financer des travaux de recherche de type doctorat, et de maintenir l'ambition de produire de la connaissance publiable, publiée, et utile pour la communauté académique et les partenaires. Un second volet que la chaire tient particulièrement à développer est de mettre en place une communauté opérationnelle et de chercheurs qui dialoguent autour de ces questions au sein du Ministère. Les acteurs ont en commun de faire le même métier, à savoir de faire de la recherche et de l'enseignement : c'est donc l'occasion de forger un enrichissement mutuel.

Jean-Paul Laborde – Titulaire de la Caire cyber Saint-Cyr, Sogeti, Thales

Ouvrir des recherches et accueillir des doctorants, soit dans le secteur juridique, soit dans celui de l'intelligence artificielle est également une volonté de la chaire et un projet en réflexion.
L'exposition internationale est centrale, en particulier concernant les évolutions politiques, qui semblent particulièrement importantes, surtout en ce qui concerne les questions de souveraineté et leur évolution par rapport aux accords de Tallin. Il est nécessaire de travailler sur des éléments d'ouverture également basés sur notre souveraineté (numérique ou de compétence de nos institutions). C'est un débat important, sur lequel il faut veiller, tout en portant la collaboration au niveau international. Il s'agit d'une position spécifique de la chaire, pour relayer les travaux selon une parole libre.

Contre-amiral (2S) Pascal Verel – Chargé de la coordination inter-chaires, COMCYBER

Les chaires sont des outils à disposition, où chacun peut apporter sa pierre à l'édifice en ce qui concerne ces problématiques communes. Le gros challenge pour un chercheur est de donner de la réalité à sa théorie : l'échange entre professionnels et chercheurs favorisé au sein des chaires permet ainsi de confronter la réflexion des chercheurs à la réalité du terrain, mais permet également aux industriels de concevoir des solutions en adéquation avec celle-ci, en posant les bases d'un enrichissement mutuel.