CYBERSECURITE : L'AGILITE DES ORGANISATIONS EN QUESTION

Laurent Dubau

CYBERSECURITE : L'AGILITE DES ORGANISATIONS EN QUESTION

CYBERSECURITY: A CHALLENGE FOR THE AGILITY OF ORGANIZATIONS

Laurent DUBAU
Thales
20-22 rue Grange Dame Rose
78141 VELIZY Cedex Société

Résumé
La vitesse d'évolution rapide et l'incertitude en matière de cybersécurité nous fait toucher les limites des moyens techniques, organisationnels et règlementaires actuels. Une réflexion sur un nécessaire changement de paradigme pour s'adapter à ce contexte est proposée dans cette intervention.

Summary
The rapid pace of change and uncertainty in cybersecurity is leading us to the limits of the current technical, organizational and regulatory means. A study on a necessary paradigm shift to adapt to this context is proposed in this paper.

Contexte et objectifs

La transformation numérique modifie nos modes de fonctionnement, en particulier dans les domaines des sciences cindyniques : accélération du rythme du changement, cyberattaques aux contours incertains et évolutifs, enjeux transfrontaliers et phénomène mondial imposant de légiférer entre Etats et à l'échelle internationale. Autant de caractéristiques qui questionnent sur la faculté d'adaptation de nos structures tant en matière de prévention des risques que de gestion des crises. Les cybermenaces doivent donc nous amener à réfléchir sur le juste équilibre entre sécurité réglée et sécurité gérée, et imaginer de modes de fonctionnement en rupture pour faire face au bouleversement induit par cette révolution technologique. Cette communication a donc pour objectif de donner un éclairage sur les limites des moyens techniques, organisationnels et règlementaires dans le domaine de la cybersécurité et de proposer une réflexion sur les outils (organisation au sein des entreprises, réglementation à l'échelle internationale) à mettre en place pour s'adapter à ce contexte qui bouleverse le fonctionnement de nos structures.

Méthode

Nous proposons d'aborder le sujet de la cybersécurité en partant des aspects techniques, puis d'étudier son traitement par les entreprises et les organisations à l'échelle nationale ou internationale, pour finir par des considérations plus générales sur la capacité à règlementer à un rythme adapté à un niveau mondial ainsi que le besoin urgent d'adapter les structures de décision et de gestion des attaques.

1. La limite des moyens techniques et modèles actuels

En matière de cybersécurité les « remparts technologiques » (pare-feu, antivirus, chiffrement, cloisonnement, durcissement des postes informatiques,…) se sont accumulés depuis des années. Cela répond à une des lignes de défense du concept de « défense en profondeur », décrit dans un mémento (ANSSI, 2004, réf.1) et illustré dans le document par les fortifications de Vauban (figure 1).

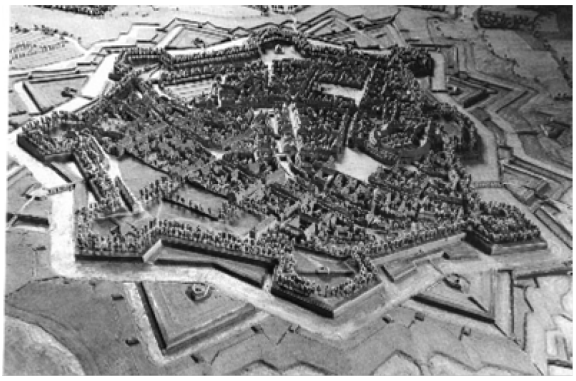

Figure 1 : Fortification de type « Vauban » (Source Image : ANSSI)

Ce concept fait également référence au modèle développé par le psychologue James Reason (Reason, 1990, réf.17) principalement pour décrire les aspects systémiques et socio-organisationnels de la sécurité dans les systèmes industriels.

Cette barrière technique de défense est un préalable nécessaire mais qui ne suffit évidemment pas. Dans cette « guerre de mouvement », selon les termes de Patrice Caine, PDG de Thales, (Caine, 2015, réf.7) qui caractérise l'affrontement dans le cyberespace, les meilleurs boucliers resteront souvent

insuffisants face au glaive du hacker. Ce dernier a en effet l'avantage de l'initiative et la puissance de l'imagination à son service. Les cyberattaques à répétition de ces dernières années (Council on Foreign Relations, 2018, réf.9) témoignent de cette limite. Ce sont ainsi probablement plusieurs centaines de milliards de dollars qui sont perdus pour l'économie mondiale chaque année selon les estimations des cabinets spécialisés. Par ailleurs, ces attaques sont souvent décelées tardivement alors que les pirates ont déjà arpenté le système d'information depuis un moment pour en exfiltrer des données précieuses ou rançonner l'entreprise en les chiffrant comme par exemple à l'aide d'un rançongiciel (voir figure 2 ci-dessous).

Figure 2 : Principale menace actuelle, le « rançongiciel »
(Source image : https://pixabay.com/)

Le développement d'un système plus réactif a donc vu le jour avec des moyens de surveillance et de détection d'intrusion tels que le SOC (Security Operating Center) et le SIEM (Security Information and Event Management), complétés par des moyens d'investigation (dits « Forensics ») ou d'intervention (FIR ou Force d'Intervention Rapide). Nous sommes passés au modèle de l'aéroport (Billois, 2016, réf.5) avec sa tour de contrôle et son radar, ses pompiers, ses enquêteurs et « légistes » du digital. Toutefois ce concept n'est bâti que pour réagir à l'attaque. Un modèle plus récent s'inspire maintenant de la compagnie aérienne (Billois, 2016, réf.6) et intègre la dimension décentralisée des données et du pilotage de la sécurité prenant en compte désormais de nouveaux usages comme le cloud, les outils de mobilité, les prestataires et services à distance. Ce modèle montre néanmoins une limite. Certaines activités peuvent être localisées dans des zones géographiques où les pratiques de sécurité et la règlementation sont moins rigoureuses et nécessitent une vigilance accrue, comme dans le milieu maritime ou aéronautique avec les « pavillons de complaisance ». La disparité des règles de protection des données à caractère personnel à travers le monde (CNIL, 2018, réf.8) par exemple témoigne de ces fossés culturels en matière de cybersécurité avec des zones exemptes de toute réglementation !

Ainsi à l'image d'industries plus matures et mondialisées, la nécessité de légiférer à l'échelle mondiale s'est imposée (paragraphe 3 ci-après).

Synthèse intermédiaire

Difficultés	Voies d'amélioration
Arsenal technique insuffisant pour contrer les attaques	Renforcer la résilience par l'optimisation de l'organisation (FOH[1])
Temps de latence pour la détection des intrusions	Systématiser et élargir la surveillance des systèmes d'information
Maturité et culture cybersécurité disparates à l'échelle mondiale	Promouvoir une convention internationale et un socle commun de bonnes pratiques

2. Des organisations qui s'améliorent et anticipent

Les efforts se sont donc aussi portés sur l'amélioration des organisations et l'anticipation. Les entreprises se préparent en élaborant des plans avec des méthodes inspirées des armées. En effet, une cyberattaque ressemble à une opération militaire avec une phase amont de renseignement, appelée « l'ingénierie sociale », qui consiste à collecter des informations sur les personnes et l'entreprise ciblée : responsables clés, domaines d'activité, systèmes informatiques en place. Ces éléments permettront, par exemple, de mettre en place une attaque de type « spear phishing », hameçonnage ciblé, telle une frappe chirurgicale avec une bombe logique « à guidage laser ». Le renseignement peut être également de nature technique et nécessiter un travail d'agences spécialisées comme cela a été probablement le cas pour Stuxnet (Le Figaro, 2010, réf.12). Les organisations se préparent donc avec des méthodes d'analyse de risque sur les systèmes

[1] Facteurs Organisationnels et Humains

d'information inspirées des états-majors militaires. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) passe ainsi par la formalisation des besoins de sécurité, des scénarios de menaces, des vulnérabilités constatées dans le système d'information et les mesures de remédiation (ANSSI, 2010, réf.2). Autant de similitudes avec des « objectifs militaires », des « modes d'action ennemi » et « ami » qui se concluent par des plans (d'attaque ou de défense). A la différence que nous luttons, dans le cyberespace et notre univers digital, contre des « missiles numériques ».

La sécurité des systèmes d'information est également tributaire du facteur humain et de l'organisation (politiques et procédures). La construction d'une bonne organisation de sécurité et la mise en place d'une culture de sécurité en sensibilisant le personnel sont donc des éléments décisifs. Les PSSI (Politique de Sécurité des Systèmes d'information) intègrent de plus en plus cette dimension « formation, sensibilisation et information » (Norme ISO 27001 - 2013, Annexe A, objectifs et mesures de référence, A.7 Sécurité des ressources humaines). Toutefois dans le domaine de la cybersécurité la mise en place d'une organisation « apprenante » (Dubau, 2016, réf.10) reste à construire comme dans l'aéronautique, précurseur dans ce domaine, avec la mise en place d'une démarche de « dépénalisation de l'erreur » : permettre aux individus de faire remonter les incidents, améliorer la capacité à apprendre des erreurs et s'adapter en permanence à la menace. Celui qui a ouvert une pièce-jointe douteuse ou cliqué sur un lien suspect dans un mail ne doit pas craindre d'alerter. Il permettra ainsi à l'entreprise de réagir à une attaque informatique avant que des dommages irrémédiables ne soient causés.

Synthèse intermédiaire

Difficultés	Voies d'amélioration
« Organisations apprenantes » à construire dans le domaine de la cybersécurité	Mettre en place une culture de la « dépénalisation de l'erreur »

3. De l'impulsion étatique à la stratégie en alliance

L'obligation de notification d'incident par les OIV (Opérateur d'importance vitale) apparue avec la loi de programmation militaire (LPM) et son article 22 et ses décrets d'applications sectoriels (ANSSI, 2016, réf.3) va dans le sens du partage de l'information à plus grande échelle, facteur décisif de la lutte contre les cybermenaces, notamment via les « Computer Emergency Response Team » (CERT).

Néanmoins, ce travail préalable ne s'accompagne pas encore d'un réel retour d'expérience officiel après des incidents ou cyberattaques touchant les entreprises ou les institutions (en France ou à l'international). Cette formalisation reste limitée, notamment aux failles ou aux vulnérabilités utilisées par les hackers et à des bulletins d'actualités publiés notamment par le CERT. Nombre d'attaques ne font l'objet que d'articles de presse, de publications sur des sites, des blogs spécialisés ou de diffusion sur les réseaux sociaux. Cette situation est compréhensible pour préserver l'image des entreprises ciblées et ne pas dévoiler certaines faiblesses de leurs systèmes d'information. Mais dans un but d'amélioration des analyses de risques, d'apprentissage des organisations et de renforcement de leur capacité de réaction, un mode de partage de l'information rendue « anonyme » doit être envisagé.

Les pirates échangent leurs informations, utilisent l'intelligence collective et le renseignement en accélérant le rythme. Les systèmes de défense, pour lutter à armes égales, intègrent désormais cette dimension (« Threat Intelligence »). Cela va jusqu'à la mobilisation des talents au-delà des limites des entreprises avec des programmes de « Bug Bounties », acteurs extérieurs ou indépendants qui cherchent les vulnérabilités dans les systèmes d'exploitation et les applications pour en améliorer la sécurité contre des rémunérations ponctuelles, faisant d'eux en quelque sorte « les corsaires » dans l'océan numérique luttant contre les « pirates » (figure 3 ci-dessous).

Figure 3 : Les programmes de Bug Bounty
(Source image : eset.co.uk)

Toutefois, malgré les avancées de la LPM en matière de cybersécurité, nulle loi de portée nationale n'est en mesure de couvrir les activités transfrontalières, caractéristiques de certaines infrastructures critiques comme les réseaux de distribution électrique ou les systèmes de contrôle aérien. Ainsi une cyber-offensive sur le point le plus faible au cœur de l'Europe, dans un pays n'ayant pas le même niveau d'exigence que le nôtre, peut avoir des répercussions chez tous ses voisins. Pour contrer ces aspects systémiques, l'Europe s'est dotée d'un outil juridique avec la directive NIS (Network and Information Security), entré en vigueur en mai 2018 (ANSSI, 2018, réf.4). Elle permettra de renforcer la robustesse globale du continent européen en fixant, entre autres, des exigences de sécurisation pour des « opérateurs essentiels » et des obligations d'échanges d'information entre Etats. Elle instaure un cadre de coopération et un réseau d'alerte via les CSIRT (« Computer Security Incident Response Team », terme européen pour les CERT). De ces organismes officiels aux bugs bounties un large écosystème d'information en matière de cybersécurité est désormais disponible dans lequel l'extraction de l'information utile est parfois difficile.

En outre, malgré cet arsenal juridique et règlementaire, certains secteurs exerçant des activités mondialisées comme le transport maritime, aérien, ou l'industrie automobile rencontrent des difficultés à mettre en place des moyens de cybersécurité coûteux et des dispositifs contraignants face à des concurrents moins rigoureux. Tous les acteurs doivent donc suivre le même mouvement pour ne pas créer de « distorsion de compétitivité ». Pour le transport maritime le corpus réglementaire est maintenant du niveau de l'OMI (Organisation maritime internationale) qui déploie avec l'aide de nombreux partenaires une série de normes et guides à l'usage des armateurs (IMO, 2018, réf.11). La cybersécurité est également à l'agenda de l'OACI (Organisation de l'Aviation Civile Internationale) qui va mettre en place des pratiques de cybersécurité dans une annexe de la convention de Chicago (Représentation permanente de la France auprès de l'Organisation de l'Aviation Civile Internationale, 2018, réf.18). Pour l'industrie automobile, une norme ISO (21434) est en cours de rédaction pour harmoniser les pratiques à l'échelle mondiale mais sa première version DIS « Draft International Standard » est annoncée pour mars 2019 ! Alors que les cyberattaques frappent déjà depuis bien des années, ces normes ou exigences ne sont mises en place qu'avec un temps de latence important lié à la nature même de ces institutions (Union Européenne, agences intergouvernementales, organisations internationales) qui ont de longs processus pour élaborer les standards et les règlementations avec souvent la recherche d'un consensus. Pour pallier cette faiblesse il est donc urgent de mettre en place une forme de gouvernance à l'échelle mondiale capable de prendre en compte deux caractéristiques des cybermenaces: l'incertitude et la fulgurance. Une recherche de simplification par l'adoption d'une méthode de réglementation « agile » doit permettre de combler cet écart temporel entre le temps d'évolution des menaces et celles des outils juridiques, légaux ou des normes : simplifier les corpus règlementaires pour aller à l'essentiel, utiliser au maximum les outils collaboratifs modernes (Web conférences par exemple) pour accélérer le processus d'élaboration. Toutefois cette recherche de simplification doit s'accompagner d'une subsidiarité accrue dans la déclinaison des textes.

La métaphore du « virus » informatique doit inspirer un modèle nouveau de gestion des attaques à l'échelle mondiale analogue à celui des pandémies avec, par exemple, un réseau de veille et d'alerte et une véritable capacité de réponse rapide (« task force »).

En outre l'achat sur étagère d'équipements (COTS ou « Commercial On The Shelf ») ou de services auprès de fournisseurs en nombre limité ou parfois unique, et dans certaines zones du monde à moindre coût, conduit à une communauté d'équipement sur les systèmes d'informations et des risques accrus

d'attaque systémique et massive. C'est le mode opératoire utilisé par le botnet Miraï qui a permis la prise de contrôle de 500 000 caméras IP vendues dans le monde par une seule entreprise chinoise et conduire au déni de service à l'encontre de la société Dyn en octobre 2016. Cette tendance devrait ainsi conduire à une méthode d'évaluation du niveau de confiance que l'on peut accorder à certains fournisseurs, tout comme cela a été fait dans l'aérien avec la mise en place de listes noires des compagnies aériennes dangereuses et interdites de vol vers l'Europe. De la même manière, les postures variables de différents Etats en matière de cybersécurité doit être évaluées et diffusées, afin de permettre aux acteurs privés de prendre les décisions d'implantation de systèmes d'information en toute connaissance de cause.

Ces actions ne seront possibles qu'avec la mise en place d'une réelle instance de gouvernance de la cybersécurité à l'échelle mondiale, que certains appellent de leurs vœux mais qui tarde à se mettre en place (SGDN, 2018, réf.19, page 35).

Synthèse intermédiaire

Difficultés	Voies d'amélioration
Retour d'expérience officiel limité	Partage des analyses post-attaques à l'instar des rapports d'accidents des « bureaux d'enquêtes accidents »
Vaste écosystème d'information cybersécurité	Outils technologiques de partage et de tri
Délais pour mettre en place des standards et pratiques recommandées dans les secteurs d'activités mondialisés	Réglementer de façon « agile » en simplifiant les procédures d'élaboration
Améliorer la surveillance et la capacité de réaction à l'échelle internationale	Encourager la mise en place d'un organisme de gouvernance de la cybersécurité à l'échelle mondiale

4. Vers la « sécurité augmentée », une nouvelle perspective pour les cindyniques

Des outils technologiques sont cependant disponibles pour faire face à cet écosystème de plus en plus complexe en matière de cybersécurité, avec des compétences disséminées à l'intérieur de l'entreprise et à l'extérieur (sous-traitants, fournisseurs, spécialistes des agences gouvernementales, chercheurs, bug bounties…) et une quantité d'information massive, conséquence des évolutions citées aux précédents paragraphes.

La « guerre de mouvement » n'existe pas seulement entre les hackers et ceux qui défendent les systèmes d'information des entreprises. Une course de vitesse s'est également établie entre le rythme d'innovation des industries (proposition permanente de nouveaux services numériques qui augmentent d'autant les surfaces d'attaques) et la capacité des organisations et des entreprises à mettre en place les systèmes de défense et de réaction. La maîtrise des risques dans le domaine de la transformation numérique doit donc maintenant utiliser les mêmes moyens et les mêmes outils que ceux qui sont à la disposition aussi bien des innovateurs mais aussi des attaquants.

Pour décrire l'apport de la transformation numérique dans notre quotidien on parle aujourd'hui d'« Homme augmenté » ou de « réalité augmentée ». Une nouvelle étape est à franchir dans le domaine des cindyniques pour aller vers la « sécurité augmentée » et s'approprier davantage l'apport de ces nouvelles technologies. La rupture engendrée par la révolution digitale et la « nouvelle normalité » qu'elle engendre, comme le souligne le SGDN (SGDN, 2018, réf.19, page 31) doit se traduire par un réel changement de paradigme dans le domaine de la maitrise des risques et s'accompagner d'une rupture institutionnelle.

Ainsi le couple « signal – guetteur » tel que décrit dans le livre « La prise de décision agile » (Magne, Pignault, Dubau, 2018, réf.14, pages 64 et 65), aussi bien au niveau de l'entreprise que des organisations internationales, doit maintenant être renforcé par les apports de la technologie. Face à la profusion d'informations disponibles, la complexité des systèmes à surveiller, le guetteur peut être suppléé par la machine, voire simplement être une machine. Cette dernière devra simplement présenter son

diagnostic à un humain de façon claire et précise.

En conséquence la « sécurité augmentée » doit s'appuyer sur des outils qui permettent de démultiplier les capacités des individus et des organisations:

4.1. Des moyens de communication de masse et rapide, des messageries instantanées (type « WhatsApp » ou « Twitter »), équivalents de réseaux sociaux d'entreprise, voire un intranet/extranet dédié à la cybersécurité à l'échelle mondiale. S'il existe un « Darkweb » support de la cybercriminalité, un « BrightWeb » à l'usage des responsables de cybersécurité doit émerger. De plus ces moyens sont à même de soutenir les besoins de règlementation « agile » évoqués au paragraphe 3,

4.2. L'automatisation des tâches de gestion de tri et de filtrage de l'information par le recours à l'intelligence artificielle (IA) pour traiter le volume massif d'information généré par les outils cités précédemment, et le partage du retex évoqué, véritable big data de la « sécurité numérique » ;

4.3. L'apport de l'IA dans les tâches de surveillance, de détection et de réaction (SOC /SIEM, sondes de détection,…) :

- Améliorer la détection (filtrer les informations utiles) ;
- Accélérer la réaction, augmenter la capacité d'adaptation à des environnements avec des changements rapides ;
- Suppléer l'humain pour la perception d'environnements techniques complexes ;
- Robotiser la recherche de vulnérabilité, la réalisation des audits et des tests.

4.4. Le recours massif à la simulation, à la mise en situation des acteurs de la défense des systèmes d'informations (exercices « RedTeam », CyberLab).

Les moyens du 4.4 peuvent être alimentés par ceux des points précédents 4.1 à 4.3 dans la mesure où la boucle d'apprentissage se nourrit du retour d'expérience, d'une analyse augmentée des incidents et attaques ainsi que de la détection des faiblesses ou des vulnérabilités émergentes.

Toutefois l'apport de la technologie doit rester sous un contrôle humain et, comme tout principe de subsidiarité, s'appuyer sur la confiance (Magne, Pignault, Dubau, 2018, réf.14, page 165). A ce titre, l'usage des automatismes et de l'IA doit s'accompagner des précautions suivantes :

- S'assurer régulièrement que le niveau de filtrage de l'information est exercé au bon niveau ;
- Vérifier que le « machine learning » et « deep learning » n'est pas détourné par des attaquants.

5. La « sécurité augmentée » outil pour la « sécurité agile »

Si l'on considère que les trois principaux ennemis de la sécurité sont la complexité, l'incertitude et le changement, l'apport des outils technologiques et de la « sécurité augmentée » doivent permettre de :

- Lutter contre la complexité en **simplifiant** (par exemple l'élaboration de la règlementation « agile » et en utilisant les moyens modernes de communication décrits au 4.1),
- Réduire l'incertitude en améliorant **l'analyse** des situations (permettre la confrontation des idées et la capacité d'innovation par la mise en réseau des compétences grâce aux outils du 4.2 et 4.3),
- S'adapter au changement en **accélérant** (par l'usage des outils d'aide à la décision et en améliorant sa capacité de réaction grâce au RETEX et à l'entrainement, 4.4).

« Simplifier », « analyser » et « accélérer », trois leviers qui, au niveau des cindyniques permettent de répondre aux voies d'amélioration tracées dans les paragraphes précédents et d'élaborer les bases d'un changement de paradigme dans la conception de la sécurité, adaptée au monde mouvant et incertain de la sécurité numérique.

Synthèse générale

Voies d'amélioration	Leviers cindyniques
Renforcer la résilience par l'optimisation de l'organisation (FOH[2])	Simplifier Analyser Accélérer
Systématiser et élargir la surveillance des systèmes d'information	Analyser
Promouvoir une convention internationale et un socle commun de bonnes pratiques	Simplifier
Mettre en place une culture de la « dépénalisation de l'erreur »	Analyser
Partage des analyses post-attaques à l'instar des rapports d'accidents des « bureaux d'enquêtes accidents »	Analyser
Outils technologiques de partage et de tri de l'information	Analyser Accélérer
Réglementer de façon « agile » en simplifiant les procédures d'élaboration	Simplifier Accélérer
Encourager la mise en place d'un organisme de gouvernance de la cybersécurité à l'échelle mondiale	Simplifier Analyser Accélérer

De plus, les outils technologiques permettent d'agir sur l'ensemble des activités de sécurité comme décrit dans le tableau ci-après, et d'ouvrir la perspective nouvelle d'une sécurité dite « agile », nourrie à la fois de la sécurité réglée et de la sécurité gérée. En dégageant des ressources disponibles pour le traitement des signaux utiles et la prise de décision, l'apport de la technologie permet d'envisager cette nouvelle piste où le prescrit et le réel peuvent cohabiter grâce à la capacité d'interaction de l'Homme et de la machine. Ce domaine est celui où l'Humain est dans l'action tout en étant suppléé par des moyens technologiques puissants, ce qui lui permet de prendre du recul et de prendre des décisions plus pertinentes.

Domaine d'action	Activités de cybersécurité	Apport de la sécurité augmentée
« Sécurité numérique réglée »	Règlementations	Outils collaboratifs
	PSSI	Outils collaboratifs
	Dispositifs de protection (anti-virus, pare-feu,…)	Automatisation et IA
	Audits, tests d'intrusion	Automatisation et IA
« Sécurité numérique gérée »	Gestion des vulnérabilités	Automatisation et IA Outils collaboratifs
	Gestion des incidents	
	Force d'intervention rapide	
« Sécurité agile »	Surveillance, SOC/SIEM	Outils collaboratifs Automatisation et IA
	Analyse des environnements complexes	Automatisation et IA
	Apprentissage : sensibilisation, entraînement en simulation	Outils collaboratifs Moyens de simulation

La sécurité « augmentée » permet donc d'agir sur les trois composantes de la sécurité comme présenté en synthèse dans la figure 4 ci-après.

[2] Facteurs Organisationnels et Humains

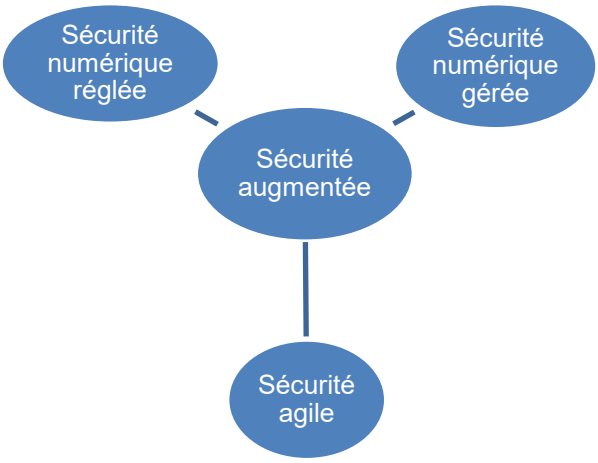

Figure 4 : La « sécurité augmentée » au service des cindyniques

6. Conclusion

Pour les entreprises et les institutions, une perspective d'amélioration de l'organisation et de gestion de la cybermenace passe donc par le développement et l'utilisation de nouveaux outils technologiques afin de pouvoir rapidement caractériser une attaque, identifier et localiser les expertises puis les mobiliser. Ainsi de nouveaux modes de gestion plus réactifs et plus fluides sont dorénavant à rechercher.

Le combat dans le cyberespace est aussi une lutte de moyens. Les ressources financières que les entreprises peuvent consacrer à la cybersécurité ne sont souvent pas à la hauteur des moyens déployés par certaines organisations criminelles ou mafieuses. Dans un cadre budgétaire contraint, la réflexion doit amener à l'établissement d'un juste équilibre entre la « sécurité réglée », dont le rythme d'élaboration et d'adaptation peut être en décalage avec l''incertitude et la fulgurance qui caractérisent les cyberattaques, et la « sécurité gérée » plus en mesure de s'adapter aux conditions réelles des attaques. La sécurité « agile » apparait comme une perspective nouvelle en mesure de relever ce défi.

Le cyberespace, univers de liberté où les flux d'information circulent comme le trafic maritime sur les océans, a pour un marin et un militaire, de frappantes ressemblances avec l'espace maritime. Ainsi, comme pour la haute mer, qui échappe à la souveraineté directe des Etats, il aura fallu mettre en place des conventions, des coalitions, des task-forces internationales pour éviter que cet espace ne devienne le lieu de trafics illicites, et lutter contre cette tendance au « côté obscur » du « Darknet ». L'humanité a progressé dans le passé en mettant en place des modes de gestion des crises, en créant des liens et des échanges entre anciens pays belligérants après des ruptures parfois brutales telles que deux conflits mondiaux. De la même manière un nécessaire changement de paradigme à l'échelle internationale va s'imposer pour le cyberespace avec le nécessaire avènement d'un organisme de gouvernance. Les pirates informatiques échangent leurs informations, utilisent l'intelligence collective et le renseignement en accélérant le rythme. Leur puissance de destruction ne fera que s'amplifier avec la rupture technologique en cours de l'internet des objets (ou IoT « Internet of Things ») et la perspective de 25 milliards d'objets connectés en 2020. Cette dernière annonce une interaction grandissante entre le monde physique et logique avec des risques accrus pour les systèmes industriels. La nature de la menace, comparée parfois à l'arme nucléaire (Lewis, 2015, réf.13) s'approche, en réalité, davantage de la menace bactériologique.

Associée à l'avènement de l'intelligence artificielle (des systèmes de recherche des vulnérabilités informatiques s'autocorrigent), la crainte de la perte de maîtrise du système existe : des « chatbot » échappent déjà au contrôle de leur créateur ! (mashable.france24.com, 2017, réf.15). L'attaque par déni de service massive (DDoS) par le Botnet Mirai du 21 octobre 2016 puis celle qui a frappé l'entreprise GitHub le 28 février 2018 (Numerama, 2018, réf.16) préfigure les dommages colossaux que ces réseaux de robots pourront causer. Une alerte récemment publiée fait même craindre un effondrement d'internet (Silicon.fr, 2017, réf.20). Pour garder le contrôle de ce « feu prométhéen » et éviter un « cyberarmageddon », une réflexion urgente doit être impérativement lancée sur une nouvelle forme d'organisation internationale pour accélérer le rythme de décision et anticiper les attaques du futur face à des menaces qui évoluent de plus en plus vite. La capacité de « prise de décision agile » et la faculté à des organisations à renforcer le couple « signal – guetteur » (Magne, Pignault, Dubau, 2017, réf.14) par l'apport de la technologie et la faculté d'adaptation des futures structures seront les facteurs déterminants de la victoire dans cette course de vitesse.

Références

1. ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), 2004, Mémento sur le concept de défense en profondeur appliquée aux systèmes d'information, https://www.ssi.gouv.fr/entreprise/guide/la-defense-en-profondeur-appliquee-aux-systemes-dinformation/
2. ANSSI, 2010, EBIOS — Expression des Besoins et Identification des Objectifs de Sécurité https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
3. ANSSI, 2016, Publication des premiers arrêtés sectoriels relatifs à la sécurité des systèmes d'information des opérateurs d'importance vitale, https://www.ssi.gouv.fr/publication/publication-des-premiers-arretes-sectoriels-relatifs-a-la-securite-des-systemes-dinformation-des-operateurs-dimportance-vitale/
4. ANSSI, 2018, Adoption de la directive Network and Information Security (NIS) : l'ANSSI, pilote de la transposition en France https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/
5. Billois, 2016, L'évolution du modèle de sécurité : du château-fort à l'aéroport, https://www.riskinsight-wavestone.com/2016/05/levolution-modele-de-securite-chateau-fort-a-laeroport/
6. Billois, 2016, Le modèle de sécurité du futur n'est-il pas celui d'une compagnie aérienne ? http://www.lemagit.fr/tribune/Le-modele-de-securite-du-futur-nest-il-pas-celui-dune-compagnie-aerienne
7. Caine, 12/06/2015, La Tribune https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/aeronautique-le-modele-economique-est-aligne-avec-l-interet-ecologique-patrice-caine-pdg-de-thales-483355.html
8. CNIL, 2018, Data protection around the world https://www.cnil.fr/en/data-protection-around-the-world
9. Council on Foreign Relations, 2018, https://www.cfr.org/interactive/cyber-operations#Timeline
10. Dubau, 2016, Cybersécurité : Quelle place pour l'humain et quelle organisation ? https://www.riskinsight-wavestone.com/2016/02/cybersecurite-quelle-place-pour-lhumain-et-quelle-organisation/
11. IMO, International Maritime Organization, 2018, http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/cyber-security.aspx
12. Le Figaro, 2018, Cyberattaques en Iran : une unité israélienne suspectée http://www.lefigaro.fr/international/2010/10/05/01003-20101005ARTFIG00697-cyberattaques-en-iran-une-unite-israelienne-suspectee.php
13. Lewis (James A), 2015, Tallinn paper, page 2 https://ccdcoe.org/multimedia/role-offensive-cyber-operations-natos-collective-defence.html
14. Magne, Pignault, Dubau, 2017, « La prise de décision agile », https://www.dunod.com/entreprise-economie/prise-decision-agile-anticiper-risques-grace-aux-signaux-precurseurs
15. Mashable http://mashable.france24.com, 2017, Une intelligence artificielle de Facebook a accidentellement inventé son propre langage http://mashable.france24.com/medias-sociaux/20170620-intelligence-artificielle-facebook-messenger-chatbots-langage
16. Numerama, 2018, « GitHub a subi ce qui semble être la plus grosse attaque DDOS enregistrée jusqu'ici » https://www.numerama.com/tech/333329-github-a-subi-ce-qui-semble-etre-la-plus-grosse-attaque-ddos-enregistree-jusquici.html
17. Reason, 1990, « Human Error », Chapter 7, page202, Cambridge University Press.
18. Représentation permanente de la France auprès de l'Organisation de l'Aviation Civile Internationale, 2018, https://oaci.delegfrance.org/Dossier-Cybersecurite-et-transport-aerien#t2-L-OACI-accelere-ses-travaux-dans-le-domaine-de-la-cybersecurite
19. SGDN, 12 février 2018, Revue stratégique de cyberdéfense
20. Silicon.fr, 2017, Un nouveau botnet IoT prêt à faire éclater une cyber-tempête https://www.silicon.fr/nouveau-botnet-iot-eclater-cyber-tempete-187895.html/?inf_by=5a16cfab671db833698b4b32