Le magazine des Ingénieurs de l'Armement

La cybersécurité

caia N°102 Mars 2014

Edito

Cher lecteur,

Face à ce domaine nouveau qu'est la « cyber » avec toutes sortes de suffixes, cyberdéfense, cybersécurité, cybermonde, etc … les ingénieurs de l'armement vous partagent dans ces pages leurs réflexions ainsi qu'une vision sans complaisance. Non la « cyber » n'est pas simplement la perte d'un mail. Oui, elle menace de plus en plus d'aspects de notre quotidien et de l'activité de nos entreprises.

Comprendre et ajuster les réponses de la France aux dimensions nouvelles qui menacent notre défense et notre sécurité, c'est bien notre mission, depuis des siècles

Je reste frappé pour ma part des cas concrets dont je suis témoin : mails de demande d'un proche dont le style est un peu surprenant « j'ai vraiment besoin de ton aide en ce moment… » ; cas de ce chercheur qui recherche les traces de l'apôtre Saint Thomas en Chine, et dont les différents ordinateurs sont régulièrement rendus incapables de recevoir des messages; ils s'affichent quelques secondes puis disparaissent ; cas de nos déplacements au cours desquels nous recevons des SMS et mails visiblement géolocalisés et adaptés à notre profil.

Plus largement, les révélations sur nos pourvoyeurs de services préférés ou sur les vols de données de grands opérateurs montrent combien la menace nous enveloppe.

C'est donc un vrai domaine de développement, dans lequel la DGA va concentrer ses embauches dans les années qui viennent. Pour notre part, nous avons édité en janvier un « shortmag » exceptionnel à l'occasion du forum international de la cybersécurité, pour être mieux vus… à lire ou télécharger sur le site www.caia.net.

Mais tout n'est pas « cyber » ! Nous multiplions les occasions de rencontres véritables pour tisser du lien entre nous. Le gala d'octobre dernier, les clubs, la prochaine assemblée générale, autant de lieux où nous renforcer dans nos missions collectives au service de la défense et de la sécurité de notre nation.

Notre mission s'épanouit aussi à l'échelle de l'individu, et vous trouverez quelques pistes pour vérifier si vous êtes bien aujourd'hui dans votre « vocation professionnelle » ou pour aller plus loin, votre « vocation de service », que ce soit au travail ou ailleurs.

Bonne lecture

Jérôme de Dinechin
Rédacteur en chef

Préface

Jean-Yves Le Drian
Ministre de la Défense

Cyberdéfense : un défi à la mesure de nos ambitions

Fait rare, en l'espace de quelques années seulement, le sujet de la cybersécurité, qui semblait jusqu'ici réservé à une petite communauté d'initiés, s'est élevé au rang de priorité nationale. Ce sujet très technique, qui a pu paraître obscur, est aujourd'hui omniprésent. Il touche à des questions aussi fondamentales que notre sécurité, notre autonomie d'appréciation, de décision et d'action – en un mot, à l'essence de notre souveraineté.

Le livre blanc de la défense et de la sécurité nationale de 2008 avait clairement identifié, pour la première fois, le risque « cyber » qui pèse sur un nombre croissant de systèmes d'importance vitale pour la Nation. Cinq ans plus tard, le nouveau livre blanc n'hésite plus à parler de menaces majeures pouvant aller jusqu'à de véritables actes de guerre. La prise de conscience est brutale ; elle peut être déstabilisante ; à ce titre, elle appelle de notre part une réaction forte et coordonnée.

L'application de ces considérations d'ordre stratégique doit être concrète et efficace.

La loi de programmation militaire, qui vient d'être votée, définit avec clarté l'ambition de la France concernant notre cyberdéfense. Les moyens nouveaux, humains et financiers, qu'elle consacre, vont être à la hauteur des enjeux. Ils se traduisent globalement par un triplement de l'effort, que ce soit en termes de budget d'études amont, de programmes d'armement consacrés à la cybersécurité, ou bien d'effectifs d'experts techniques et de spécialistes opérationnels à la fois.

Une telle croissance, pour être pertinente, doit s'appuyer sur les savoir-faire maîtrisés par le ministère de la défense. La cyberdéfense, c'est-à-dire la prise en compte du cyberespace comme cinquième milieu opérationnel, est désormais pleinement intégrée à la chaîne de commandement des opérations militaires. Elle n'est pas un sujet technique qui serait traité à part, mais bien une composante de cette chaîne, à l'importance croissante, et qui vise à la fois à protéger et soutenir les opérations.

Au sein des programmes d'armement conduits par la direction générale de l'armement, la prise en compte des impacts « cyber » est systématisée, en visant une stricte maîtrise des coûts et des délais, mais sans sacrifier les performances.

Cette intégration de la cyberdéfense au sein de notre appareil de défense a été rendue possible par des femmes et des hommes, civils et militaires, qui ont su s'y adapter rapidement. Elle repose sur des filières d'excellence, comme celle des ingénieurs de l'armement, qui ont justement pour mission de maîtriser des sujets techniques pointus et leur insertion au sein de projets d'une grande complexité.

Comme l'illustrent les articles qui suivent, la prise en compte du « cyber » par le ministère de la défense, ainsi que par les autres composantes de la Nation, ne relève pas de la simple évolution technologique. Il s'agit bien d'une révolution opérationnelle majeure, qui modifie profondément nos doctrines et nos modes d'action. Nous ne faisons que débuter, mais j'ai la conviction que ce défi est à notre portée, et que si nous continuons à nous en donner les moyens, nous en sortirons renforcés à l'échelle internationale.

Excellente lecture !

Sommaire

Rédacteur en chef : Jérôme de Dinechin
Rédacteur en chef délégué :
Guillaume Poupard
Directeur de publication : Philippe Roger
Comité de rédaction : Arnaud Salomon,
Flavien Dupuis, Dominique Luzeaux,
Daniel Jouan, Louis Le Pivain, Denis Plane,
Frédéric Tatout, Jocelyn Escourrou,
Olivier de Vulpillières

Edition et régie publicitaire :
SACOM 01 41 10 84 40,
Ineyret@la-clique.com
Création graphique : La Clique
www.agencesacom.com

CAIA, Bâtiment 158,
24 av. Prieur de la Côte d'Or,
94117 ARCUEIL Cedex
Tél. : 01 79 86 55 12
Télécopie : 01 79 86 55 16
Site : www.caia.net
E-mail : caia@caia.net
numéro de dépôt légal : 2265-3066

Pourquoi consacrer un nouveau numéro de notre magazine à la cybersécurité moins de 4 ans après celui de juin 2010 ?

Le sujet « cyber » est ancien, voire très ancien si l'on tient compte de l'histoire millénaire de la cryptologie, mais son évolution s'accélère très rapidement avec le développement des systèmes d'information, de leurs usages, de leur complexité, de leur interconnexion. En 2008, le livre blanc de la défense et de la sécurité nationale identifiait pour la première fois, avec beaucoup de clairvoyance, une menace potentiellement très grave mais sans oser en définir véritablement l'ampleur. Cinq ans plus tard, l'analyse s'est affinée et le constat s'est considérablement durci puisque le nouveau livre blanc n'hésite plus à parler d'actes de guerre et de priorité nationale !

Vision solarisée d'une salle de supercalcul d'un des plus grands centres Français.

par **Guillaume Poupard,**
ICA

Responsable du pôle sécurité des systèmes d'information de la DGA

X92, docteur en cryptologie de l'Ecole Normale Supérieure, il est d'abord expert puis chef du laboratoire de cryptographie de la Direction Centrale de la Sécurité des Systèmes d'Information. Il rejoint ensuite le Ministère de la défense comme chef de bureau puis conseiller technique en lutte informatique. Depuis novembre 2010, il est responsable du pôle sécurité des systèmes d'information au sein de la DGA.

Qu'on le veuille ou non, le cyberespace est en train de s'imposer comme nouveau milieu opérationnel, le cinquième. Ceci est d'autant plus surprenant et déstabilisant que nous ne sommes même pas capables de nous accorder sur une définition précise à donner à ce néologisme. Son existence, entre réalité physique et virtuel numérique n'en est pas moins incontestable et, si ce milieu peut sembler original, j'imagine que les grandes évolutions technologiques du début du siècle dernier ont certainement dû générer tout autant de scepticisme et de surprises… Citons à ce sujet le secrétaire de la défense britannique, Philip Hammond : « *I'm sure a healthy debate raged 100 years ago about whether to invest in new-fangled tanks and stop buying hay for the horses. Some will have said, "Buy more hay, not tanks."* ».

Le cyberespace existe par lui-même au travers de nos réseaux et de nos systèmes d'information, bien au-delà de l'Internet, mais il interpénètre également de manière très intime les quatre premiers milieux pour la simple raison que nos systèmes d'armes font aujourd'hui un usage important, crucial pour l'atteinte de leurs performances opérationnelles, de systèmes d'information, de calculateurs et d'échange de données.

Maîtriser ce nouveau milieu est une absolue nécessité. Ceci signifie qu'il faut le comprendre, savoir s'y adapter technologiquement mais surtout, si l'on se place dans un mode plus positif, être capable d'en tirer parti afin d'accroître notre efficacité opérationnelle. L'enjeu est clairement, afin de disposer d'un système de défense cohérent et homogène à l'échelle nationale, d'élever au plus vite notre niveau de maturité à la hauteur de celle dont la France peut s'enorgueillir dans les autres domaines. En effet, à quoi bon disposer d'équipements de pointe s'ils peuvent être rendus inopérants ou, pire, retournés contre nous par des attaques à forte composante informatique d'un niveau de complexité accessible à nos adversaires ? Or, si la constitution de véritables armes numériques disposant de toutes les garanties d'efficacité et d'innocuité pour leurs propres concepteurs semble aujourd'hui réservée à quelques nations majeures, force est de reconnaître que de petits groupes compétents, parfois armés de mercenaires, sont aujourd'hui capables d'obtenir des effets opportunistes importants au moyen d'attaques informatiques via l'Internet.

En réponse, il convient de disposer d'experts de très haut niveau dans ce domaine pour lequel il convient d'être très modeste mais où nous n'avons pas non plus à rougir. Mais il importe surtout d'intégrer la question « cyber » dans l'ensemble des programmes d'armement ainsi que dans toute la chaîne de commandement opérationnel de nos Forces. Voilà très précisément l'une des évolutions majeures qui s'est produite en l'espace de quelques années et ce changement est, de mon point de vue, totalement partial et intéressé, majeur et durable. Tous les acteurs sont concernés, qu'ils appartiennent à la recherche académique, à l'industrie ou bien aux services de l'Etat. Les liens étroits qui doivent les unir peuvent s'appuyer sur les modes de travail éprouvés mais nous devons également être capables de les adapter aux spécificités du domaine, à l'image de ce que nous faisons conjointement entre l'EMA et la DGA.

On le voit, le sujet « cyber » est au cœur des préoccupations de souveraineté nationale. Il est particulièrement clivant et va clairement distinguer les pays qui sauront se défendre par eux-mêmes et opérer dans le cyberespace de ceux qui n'auront pas d'autre choix que de rechercher la protection d'un allié plus fort. Sa maîtrise est donc indispensable afin de maintenir la France au premier rang des nations mondiales.

Mais, sans qu'il n'y ait de paradoxe, la cyberdéfense doit également être une priorité en matière de coopération internationale, soit bilatérale avec nos grands alliés, soit multilatérale au sein de l'Europe et de l'OTAN. S'imaginer pouvoir se défendre efficacement seuls par nous-même face à une menace aussi complexe et protéiforme est illusoire. Vis-à-vis d'attaquants de plus en plus organisés, parfois soutenus par des nations puissantes, un renforcement lucide et pragmatique de nos alliances est indispensable. Il ne doit pas traduire un abandon de souveraineté mais bien une démarche collective de lutte face à un ennemi commun.

Mais le phénomène le plus troublant pour beaucoup d'entre nous réside dans le fait que la prise en compte du « cyber » nécessite souvent d'abolir certaines catégorisations structurantes et rassurantes entre applications civiles et militaires et, au sein de ces dernières, entre les domaines classiques. Elle requiert pour ceux dont la sécurité des systèmes d'information n'a jamais été une grande préoccupation de prendre en compte une nouvelle dimension avec tous les risques que cela représente pour le triptyque coût/délais/performance des programmes d'armement.

Le « cyber » est en train de rebattre les cartes à l'échelle internationale. La géopolitique mondiale peut s'en trouver complètement bouleversée. Si nous ne voulons pas rapidement nous transformer en cibles de choix, parées d'un rouge garance numérique, nous devons rapidement évoluer : c'est notre intérêt et c'est à notre portée ! Rendez-vous dans quatre ans pour un premier bilan.

Dans ce magazine, vous trouverez les témoignages complémentaires d'acteurs majeurs de notre cybersécurité. Je tiens à les remercier chaleureusement d'avoir accepté de nous faire partager leur vision, leurs préoccupations mais également leurs ambitions.

Bonne lecture !

Longtemps clairement identifié sous le terme « SSI », la terminologie du domaine a récemment évolué afin de tenir compte de l'évolution du métier, de la menace et de l'organisation. Sans être totalement stabilisé, le consensus actuel tend à regrouper sous le terme général de « cybersécurité » trois aspects connexes :

- la « cyberprotection » en charge du développement et de l'administration des moyens cryptographiques (anciennement simplement appelée SSI) ;
- la « cyberdéfense » responsable de la détection et de la réaction face aux attaques informatiques (parfois également appelée lutte informatique défensive ou LID) ;
- la « cybercontinuité » qui veille au maintien des capacités essentielles lors des attaques et à la résilience des systèmes.

En termes d'organisation, au sein du ministère de la Défense et sans entrer dans certaines subtilités, la DGA est en charge, dans les trois domaines, des travaux de recherche et de développement ainsi que des acquisitions. Du point de vue opérationnel, la protection est gérée par une chaîne SSI placée sous la responsabilité du Fonctionnaire de la Sécurité des Systèmes d'Information (FSSI), lui-même dépendant du DGSIC, alors que la défense est une chaîne LID commandée par un officier général de la cyberdéfense au sein de la sous-chefferie opérationnelle de l'EMA.

Comment développer une cyberdéfense européenne dépassant les problématiques de sécurité nationale ?

Jean-Marie Bockel,

Sénateur du Haut-Rhin, ancien ministre

M. Jean-Marie Bockel est l'auteur du rapport d'information sur la cyberdéfense, présenté en juillet 2012 au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat* Il a aussi été le co-rapporteur, avec M. Jacques Berthou, sénateur (SOC) de l'Ain, sur la stratégie européenne de cybersécurité et la proposition de directive de la Commission européenne du 7 février 2013, qui ont fait l'objet d'un rapport et d'une résolution du Sénat du 19 avril 2013**

Parmi les 10 priorités et les 50 recommandations contenues dans le rapport d'information sur la cyberdéfense que j'ai présenté devant la commission des affaires étrangères et de la défense du Sénat en juillet 2012, une partie d'entre elles était consacrée au rôle de l'Union européenne.

En effet, même si la cyberdéfense doit demeurer une compétence première des Etats, car elle touche directement à la souveraineté nationale, il me semble toutefois indispensable, s'agissant d'une menace qui s'affranchit des frontières, de renforcer la coopération européenne dans ce domaine. Or, l'Union européenne a un grand rôle à jouer puisque la plupart des normes applicables aux opérateurs de télécommunications relèvent de sa compétence. Je regrettais toutefois, dans mon rapport, l'absence de réelle stratégie européenne dans ce domaine.

La communication conjointe de la Commission européenne et de la Haute représentante pour les affaires étrangères et la politique de sécurité, Mme Catherine Ashton, du 7 février 2013 répond directement à ce souhait puisqu'elle propose une stratégie européenne de cybersécurité.

D'une manière générale, on peut saluer cette stratégie européenne, qui témoigne d'une véritable prise de conscience de la part des institutions européennes de l'importance des enjeux de cybersécurité. Je pense notamment à l'accent mis sur la lutte contre la cybercriminalité, sur la cyberésilience et la cyberdéfense, sur les aspects industriels, sur la recherche, la formation et la sensibilisation ou encore concernant le rôle international de l'Union européenne.

Dans notre rapport, qui a donné lieu à une résolution adoptée par le Sénat, nous recommandons donc d'approuver les orientations générales de cette stratégie et d'appeler les institutions européennes et les Etats membres à une mise en œuvre rapide de ces priorités.

Nous portons également un regard très positif sur la proposition de directive sur la sécurité des réseaux et des systèmes d'information qui a été présentée par la Commission européenne le 7 février et qui a inspiré certaines dispositions de la Loi de programmation militaire, qui vient d'être adoptée par le Parlement français.

Il en va en particulier de l'obligation, pour les Etats membres de l'Union, de se doter de structures chargées de la cybersécurité, d'élaborer une stratégie nationale en la matière et de disposer d'une structure opérationnelle d'assistance au traitement d'incidents informatiques. Il s'agit là d'un aspect essentiel et qui représentera un progrès car de nombreux Etats membres ne sont pas encore suffisamment sensibilisés à la menace représentée par les attaques contre les systèmes d'information et de communication.

Le deuxième volet de cette proposition de directive porte sur l'obligation, pour plusieurs secteurs d'importance critique, de notifier les incidents informatiques significatifs à l'autorité nationale de cybersécurité.

Le troisième volet concerne le renforcement des obligations des opérateurs d'importance critique en matière de protection de leurs systèmes d'information.

Cette proposition de directive soulève cependant deux réserves

La première porte sur la définition des modalités d'application de ces mesures, qui serait confiée à la Commission européenne, par exemple en ce qui concerne la définition des circonstances dans lesquelles s'appliquerait l'obligation de notifier les incidents ou la liste des opérateurs d'importance vitale concernés. Il serait plus légitime, tant pour des raisons tenant à la souveraineté nationale, que d'efficacité, que les modalités d'application soient confiées aux Etats membres, qui, en définitive, sont les premiers responsables en matière de cybersécurité et sont mieux placés pour prendre les mesures appropriées.

La seconde réserve est plus fondamentale. Elle concerne l'obligation de notifier systématiquement les incidents informatiques, non seulement à l'autorité nationale, mais aussi à la Commission européenne et à l'ensemble des autres pays de l'Union européenne. Outre sa lourdeur bureaucratique, une telle mesure paraît susceptible de soulever des difficultés au regard de la sécurité nationale, notamment dans le cas d'attaques informatiques à des fins d'espionnage.

Dans notre résolution, nous recommandons donc au gouvernement d'œuvrer au sein du Conseil en vue d'une adoption rapide de cette directive, tout en tenant compte de ces deux réserves dans les négociations avec nos partenaires européens.

D'une manière générale, l'Union européenne a, à mes yeux, un rôle important à jouer sur le volet normatif, sur les aspects industriels, la recherche et développement, les mesures de formation et de sensibilisation, qu'il s'agisse des administrations, des entreprises ou des opérateurs d'importance vitale.

L'Europe devrait ainsi avoir l'ambition de parvenir à une souveraineté numérique, ce qui veut dire retrouver la maîtrise de certains composants ou équipements. Cela passe notamment par l'élaboration de normes dans ce domaine, un système de certification, des financements par le biais de programmes européens des efforts de recherche et développement.

Je pense aussi à la prise en compte de la cybersécurité dans les relations extérieures de l'Union européenne, qui mériterait d'être renforcée, notamment dans les relations commerciales de l'Union européenne avec de grands partenaires, comme la Chine ou la Russie.

Mais, dans le domaine de la cyberdéfense, je suis plus réservé.

En matière de sécurité informatique, il existe toujours un risque de « maillon faible » ou de s'aligner sur le « moins disant ». Par ailleurs, la France fait partie des pays les plus avancés dans ce domaine.

On peut toutefois relever, avec intérêt, que la stratégie européenne de cybersécurité évoque la « clause de solidarité », contenue à l'article 222 du traité sur le fonctionnement de l'Union européenne, en cas de cyberincident ou d'une cyberattaque particulièrement sérieux, un peu sur le modèle de l'article V du traité de Washington en ce qui concerne l'OTAN.

La cyberdéfense a fait partie des domaines prioritaires inscrits à l'ordre du jour du Conseil européen des 19 et 20 décembre. Les Chefs d'Etat et de gouvernement de l'Union européenne devaient notamment appeler les institutions européennes à lancer des travaux dans ce domaine pour 2014.

Toutefois, il ne faut pas se faire trop d'illusions. La cyberdéfense est un domaine sensible qui touche directement à la souveraineté des Etats. Comme l'illustre l'affaire Prism, il n'existe pas réellement d'alliés dans le cyberespace !

S'il me paraît indispensable que l'Union européenne renforce la protection et la défense de ses propres réseaux et systèmes d'information et de communication – je pense en particulier aux réseaux du service européen pour l'action extérieure ou à ceux de la Commission européenne – il appartient en premier lieu aux Etats membres d'assurer la protection et la défense de leurs systèmes d'information.

Parallèlement, la France devrait développer ses partenariats bilatéraux avec des pays européens, et en premier lieu avec le Royaume-Uni et l'Allemagne. La cyberdéfense repose, en effet, sur la confiance et il est indiscutable qu'il est plus facile de recourir à la coopération bilatérale qu'à une coopération à vingt-huit pays.

** Disponible sur le site Internet du Sénat à l'adresse suivante : http://www.senat.fr/rap/r11-681/r11-681.html*

*** http://www.senat.fr/rap/l12-491/l12-491.html*

La R&D en cyberdéfense : une nouvelle mission confiée à la DGA

La DGA s'est vu confier l'activité de Recherche et Développement en cyberdéfense, comme le souligne le Livre Blanc pour la Défense et la Sécurité Nationale. Quels sont les enjeux de ce nouveau domaine et de quels moyens la DGA dispose-t-elle pour répondre à ceux-ci ?

De la découverte du logiciel malveillant Stuxnet en passant par les innombrables révélations de l'affaire Snowden, il n'est pas un jour sans que de nouvelles attaques informatiques ne soient dévoilées sur des systèmes aussi variés que les drones, les voitures ou encore les automates industriels. Ces multiples découvertes ne sont malheureusement pas à mettre uniquement au crédit d'une meilleure détection mais bien aussi d'une multiplication du nombre d'attaques et de cibles potentielles.

La convergence des technologies crée de nouvelles vulnérabilités

Sur ce dernier point, deux évolutions technologiques majeures expliquent que de nombreux systèmes autrefois épargnés soient aujourd'hui attaqués. L'interconnexion des systèmes et le nombre croissant de points d'accès facilite la tâche de l'attaquant en lui offrant de multiples possibilités pour pénétrer les systèmes afin de récupérer du renseignement ou de perturber leur fonctionnement. La standardisation de fait de nombreux composants logiciels ou matériels disponibles sur étagère facilite également le travail de l'attaquant en lui permettant de préparer son attaque et d'exploiter très largement les vulnérabilités découvertes. Cette convergence technologique concerne aussi le domaine militaire, où l'on retrouve de plus en plus les mêmes briques matérielles et logicielles que sur les applications civiles.

par **Frédéric Valette,**

ICA

Chef de la division SSI1 à DGA Maîtrise de l'Information

Après un parcours d'expert à l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) puis à DGA Maîtrise de l'Information, il est actuellement responsable des équipes en charge de conduire l'ingénierie du domaine Cybersécurité à Bruz.

De la cyberprotection à la cyberdéfense

Afin de pouvoir contrer ces attaques qui peuvent provenir d'organisations criminelles mais également d'organisations étatiques, il est indispensable de pouvoir disposer de solutions de « cybersécurité » adaptées aux systèmes à protéger. Il convient, dans un premier temps, de mettre en place l'ensemble des dispositifs traditionnels dits de « cyberprotection ». Ces briques telles que le chiffrement des flux ou l'authentification des utilisateurs sont des éléments indispensables sans lesquels il est illusoire de vouloir protéger un système. La DGA équipe depuis longtemps le ministère de la défense mais aussi les autres administrations avec des produits de très haut niveau de sécurité et va poursuivre l'effort réalisé dans ce domaine pour faire développer les solutions souveraines adaptées aux architectures et systèmes de demain. Une fois ces outils mis en place, il faut alors être en mesure de superviser en temps réel le système pour suivre toute évolution ou modification, s'y adapter et détecter les attaques potentielles : c'est le concept dit de la « cyberdéfense ».

Trois fonctions à développer

Dans ce domaine technologique qui n'est pas nouveau, trois grandes fonctions technologiques se développent à grande vitesse et méritent un investissement rapide sous peine de se voir distancer et de ne plus pouvoir rattraper le retard accumulé.

1. Le premier aspect concerne les capteurs qui vont détecter et analyser des évènements, sur les réseaux ou dans les équipements terminaux, qui peuvent être annonciateurs d'une attaque informatique. Ces produits, aussi appelés sondes, commencent à être utilisés à grande échelle mais leur performance est très largement perfectible.
2. Une fois récupérés et traités localement, les évènements sont alors remontés à des centres de supervision qui vont tenter de les corréler afin d'identifier dans cet amas d'informations les quelques signes d'une attaque éventuelle.
3. Enfin, dans un troisième temps, il faut être capable de présenter de manière synthétique les conséquences d'une attaque en cours ou d'analyser l'impact des différents scénarios de réponse sur le fonctionnement d'un système. Le début de prise de conscience des entreprises et administrations sur leur vulnérabilité à des attaques informatiques commence à créer un marché conséquent pour ce type de solutions. De ce fait, on assiste à une multiplication de solutions dans un marché dont les cartes ne sont pas encore distribuées.

Toutes ces technologies doivent pouvoir prendre en compte le « métier » d'application, c'est-à-dire utiliser la spécificité du système supervisé à la fois pour être plus efficace dans la détection mais aussi être capable de réagir de manière adaptée en cas de suspicion d'attaque informatique. En effet, un dispositif de détection d'intrusion d'un réseau de messagerie n'est pas directement utilisable pour protéger des systèmes de distribution d'énergie et les conséquences d'une paralysie de quelques minutes d'une partie du système n'ont bien entendu pas les mêmes conséquences. La DGA, de par sa maîtrise de l'architecture de l'ensemble des systèmes de défense, qu'il s'agisse de plateformes navales, terrestres ou encore aériennes, possède toutes les capacités pour prendre en compte cet aspect « métier ».
Tous ces produits doivent aussi prendre en compte les architectures utilisées pour en tirer profit. A titre d'exemple, un système de supervision d'une infrastructure de type « *cloud* » peut en utiliser les spécificités pour avoir une détection ou une réaction bien plus efficace face à une attaque.

Une technologie de souveraineté

Ces solutions qui sont dans leur grande majorité à bâtir doivent être maîtrisées au niveau national ou européen. L'actualité récente a illustré à quel point la maîtrise américaine dans les architectures informatiques rendait l'Europe vulnérable et permettait à des tiers d'accéder massivement à des informations sensibles. Les outils de lutte informatique défensive sont là encore des points d'accès privilégiés sur nos systèmes et les rendent vulnérables vis-à-vis de ceux qui les maîtrisent. C'est pourquoi il est indispensable d'avoir une politique nationale de recherche et développement ambitieuse sur ce domaine de la cyberdéfense sans pour autant négliger la cyberprotection.

Le rôle de la DGA

La DGA n'est pas seule sur le sujet. La collaboration étroite qu'elle entretient avec le CALID (Centre d'Analyse pour la Lutte Informatique Défensive), chargé de défendre les systèmes du ministère de la défense, et avec l'ANSSI, chargée des ministères civils ou des opérateurs d'importance vitale, lui permet d'orienter au mieux ses capacités pour répondre aux besoins opérationnels. Pour conduire cette politique d'innovation ambitieuse, la DGA augmente significativement la taille de ses équipes techniques : fin 2017, elle comptera 250 experts de plus dans le domaine qu'en 2010. Ces nouvelles équipes renforcent le pôle d'expertise du centre DGA Maîtrise de l'information situé près de Rennes. Cette politique s'appuie aussi sur une augmentation importante des financements dédiés aux projets scientifiques et technologiques en cybersécurité, qui devraient atteindre 30 millions d'euros annuels fin 2017.
Ces financements vont être utilisés en premier lieu pour lever les verrous technologiques du domaine et permettre à des PME ou des grands groupes de développer des prototypes de solutions pour chacune des thématiques identifiées précédemment sur des applications liées à la défense nationale. Certains prototypes pourront ensuite trouver naturellement un usage dans le monde civil du fait de la convergence des technologies. Cette politique d'innovation doit s'appuyer sur une recherche universitaire de haut niveau, qu'il faut développer à partir d'équipes existantes de très bon niveau mais de taille réduite. L'excellence de ses équipes universitaires qui s'y trouvent et la présence de DGA Maîtrise de l'Information, donnent à la Bretagne tous les ingrédients pour bâtir un pôle de recherche en cyberdéfense de premier plan et créer à terme une « cybreizh vallée ».

Le Pacte Défense Cyber : 1 Milliard d'euros, 6 axes et 50 mesures.

Le « Pacte Défense Cyber » a été annoncé lors du Forum International sur le Cybersécurité (FIC). Il précise les axes concrets d'engagement du Ministère de la Défense sur la période 2014-2019. Ce pacte a été détaillé lors d'un déplacement du Ministre de la Défense à Cesson-Sévigné le 7 février dernier. Élaboré dans le même esprit que le « Pacte Défense PME », il comporte 6 axes et 50 mesures :

- Axe 1 : durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance.
- Axe 2 : préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle.
- Axe 3 : renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés.
- Axe 4 : développer le Pôle d'excellence en cyberdéfense en Bretagne au profit du ministère de la défense et de la communauté nationale de cyberdéfense.
- Axe 5 : cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance Atlantique et dans les zones d'intérêt stratégique. 15
- Axe 6 : favoriser l'émergence d'une communauté nationale défense de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve.

Les 50 actions, distribuées selon ces six axes, sont confiées à des autorités pilotes. Elles sont dotées d'indicateurs et feront l'objet d'un suivi régulier lors du comité ministériel des SIC présidé par le Ministre de la Défense.

La cyberdéfense :
Quelques termes

SOC (*Security Operational center*)
Le terme SOC désigne un centre opérationnel chargé de superviser un ou plusieurs systèmes afin d'y détecter les attaques informatiques et de réagir à ces attaques en temps réel en tentant d'isoler les codes malveillants introduits et de maintenir le système en état de marche.

Capteur/Sondes
Ce qu'on appelle communément une sonde ou un capteur est un élément logiciel ou matériel chargé d'enregistrer et de transmettre au SOC l'ensemble des évènements suspects qui pourraient indiquer qu'une attaque est en train de se dérouler sur le système.

Code malveillant (*Malware*)
Ce terme désigne tout programme développé dans le but de nuire à un système informatique ou un réseau. Les virus, les vers ou les « chevaux de Troie » sont des types de codes malveillants. Les exemples les plus récents et les plus médiatiques sont les malwares STUXNET et FLAME.

Capacité de cybersécurité : une vision globale à 10 ans

Lieu d'affrontement politique, économique et humain, le cyberespace constitue un nouvel espace de confrontation qui est appréhendé par le ministère de la défense selon une approche opérationnelle et capacitaire globale. Le développement de la capacité de cybersécurité associée s'inscrit dans une stratégie nationale (Défense et sécurité des systèmes d'information, Stratégie de la France, Février 2011). Elle repose sur une posture résiliente de protection des systèmes d'information, adossée à une organisation opérationnelle de défense de ces systèmes, coordonnée sous l'autorité du Premier ministre et fondée sur une coopération étroite entre les services de l'Etat pour identifier puis caractériser les menaces.
Le terme « systèmes d'information » doit s'entendre selon une large acception et recouvre trois réalités physiques qui doivent être prises en compte de manière cohérente : les systèmes d'information et de communication (Systèmes d'information opérationnels et de commandement (SIOC), systèmes d'information d'administration générale (SIAG) et systèmes d'information scientifiques et techniques (SIST)), les systèmes d'armes et les systèmes dits industriels (incluant l'informatique des infrastructures opérationnelles du ministère).

par **Alexis Latty,**
Capitaine de vaisseau

Le capitaine de vaisseau Alexis Latty est officier de cohérence opérationnelle du système de forces Commandement et maîtrise de l'information.

par **Jean-François Ripoche,**
ICA

L'ICA Jean-François Ripoche est architecte du système de forces Commandement et maîtrise de l'information.

Face aux enjeux qui sont désormais perceptibles de tous, le ministère met en œuvre depuis 2012 un schéma directeur capacitaire visant à élever progressivement le niveau de cybersécurité de ses systèmes d'information selon une vision directrice à dix ans tenant compte de tous les leviers d'action disponibles : doctrines, organisation, ressources humaines, équipements, soutien et entraînement. Les investissements humains et financiers associés ont été confirmés par la loi de programmation militaire.

Le Livre blanc de la défense et la sécurité nationale confirme des ambitions élevées

Les atteintes aux systèmes d'informations peuvent poser une question de souveraineté majeure en cas de prise de contrôle ou de paralysie de secteurs vitaux pour l'Etat : c'est la raison pour laquelle la maîtrise du cyberespace est désormais érigée en priorité stratégique nationale. Le Livre blanc a développé une doctrine alliant prévention et réaction avec l'ambition d'identifier l'origine des attaques, d'évaluer les capacités offensives des adversaires potentiels et l'architecture de leurs systèmes, et de pouvoir ainsi les contrer.
Pour le ministère, il s'agit avant tout de protéger ses informations sensibles et classifiées, d'être en mesure de continuer à opérer sous agression cybernétique pour garantir l'autonomie d'appréciation de situation et de liberté d'action des forces et, en cas de crise cybernétique nationale majeure, de contribuer à assurer le bon fonctionnement de l'Etat.

Ceci d'autant plus dans un monde où l'interconnexion des systèmes est devenue la norme, y compris dans le domaine militaire où celle-ci est même devenue une nécessité absolue pour garantir la « supériorité informationnelle » sur l'adversaire : meilleure connaissance de l'environnement opérationnel, accélération du tempo de la manœuvre militaire, optimisation de l'efficacité des systèmes d'armes (dans les conflits asymétriques notamment) et maîtrise des effets militaires (précision des armements, identification des cibles, etc.).
La cybersécurité constitue un domaine dans lequel la souveraineté de la France doit s'exprimer pleinement, même si les enjeux de coopération sont réels. Des coopérations opérationnelles ou techniques se développent avec ceux de nos partenaires qui ont un niveau d'ambition similaire. Avec les organisations multinationales (OTAN, UE), également confrontées à la nécessité de mettre en place les moyens de protection et de défense de leurs propres systèmes, il s'agit d'œuvrer en faveur de la coordination des actions (en particulier dans les domaines de la formation et de l'entraînement) et de l'interopérabilité des systèmes susceptibles d'être employés lors des opérations militaires.

La loi de programmation militaire permet de mettre en œuvre cette stratégie

La loi qui vient d'être votée au Parlement consacre le renforcement de la capacité ministérielle de cybersécurité autant sur le plan des équipements que des ressources humaines avec le recrutement de plusieurs centaines de spécialistes sur la période.
L'organisation du ministère en matière de cybersécurité a été revue en 2010. La composante technique est confiée à la DGA. La chaîne opérationnelle de cyberdéfense relève du chef d'état-major des armées, avec un commandement spécialisé exercé à partir du Centre de planification et de conduite des opérations. Cinq autorités qualifiées sont responsables devant le ministre de l'Etat de cybersécurité de leurs systèmes. En matière de cyberésilience, les responsabilités sont réparties entre les autorités d'emploi et les opérateurs, internes ou externalisés (ex. PPP Balard). De manière générale, le ministère poursuit un important processus de réorganisation et d'optimisation visant à concentrer les ressources rares et à les commander de façon efficace.
La recherche amont sera renforcée, particulièrement dans les domaines de la protection (chiffreurs, composants de sécurité, algorithmes de chiffrement, etc.) et de la cyberdéfense (sondes, outils de surveillance des réseaux, etc.) avec pour objectif de contribuer au développement d'une base industrielle et technologique nationale performante et autonome. La dualité du domaine est naturellement prise en compte et les initiatives européennes sont encouragées dans certains domaines ciblés. Citons par exemple, les routeurs réseaux de confiance, les équipements de mobilité sécurisés (tablettes, smartphones, etc.) et la sécurisation d'architectures de « *cloud computing* ».
Pour faire face à l'évolution rapide de la menace et des technologies mises en œuvre, les projets structurants sont conduits de manière incrémentale. La réalisation des moyens techniques de lutte informatique défensive (programme MTLID) suivant ce principe permettra à la fois d'améliorer périodiquement les performances des équipements et d'étendre continûment le domaine supervisé.
Enfin, la capacité de lutte informatique active du ministère s'inscrit dans la capacité nationale de réponse aux agressions susceptibles de peser sur notre pays et enrichit la palette des options possibles à la disposition de l'Etat. Elle concourt à la posture de cybersécurité en contribuant à la caractérisation de la menace et à l'identification de son origine, ainsi qu'en permettant d'anticiper certaines attaques et de configurer les moyens de défense en conséquence.

Les défis à surmonter sont à la hauteur de nos ambitions

L'ampleur des défis à surmonter est inhérente à un domaine qui a qualité de « système de systèmes », celui-ci étant de surcroît particulièrement complexe et en évolution constante. Deux d'entre eux doivent faire l'objet d'une attention particulière.
Le domaine des ressources humaines constitue probablement le principal défi à surmonter dans les années qui viennent. Quatre axes d'effort sont identifiés : formation des personnels non spécialisés (pour réduire les comportements à risques des concepteurs ou des utilisateurs de systèmes d'information), optimisation de la ressource humaine spécialisée (pour viser le bon niveau d'expertise au sein du ministère et le bon niveau de subsidiarité entre compétences civiles et militaires), valorisation des acteurs de la cybersécurité (afin de pérenniser les réservoirs de compétence et d'améliorer la performance de la cybersécurité du ministère) et développement d'un centre d'excellence national dans la région de Rennes.
La maîtrise du cyberespace constitue un enjeu stratégique national qui nécessite la maîtrise de technologies critiques et une forte capacité d'innovation. Le renforcement de la base industrielle nationale du domaine, incluant un accompagnement à l'innovation technologique, est nécessaire car, bien qu'elle présente des atouts avérés, sa situation reste fragile.

L'élan initial est donné, il faut transformer l'essai

Plus personne ne songerait aujourd'hui à nier l'existence de la menace et du risque qu'elle fait peser sur nos capacités militaires. Au-delà d'orientations déterminées, réussir à atteindre ces objectifs nécessite la mobilisation dans la durée des effectifs et des compétences du ministère.
De plus, voir et prévoir à 10 ans dans ce domaine est une gageure : il faudra adapter la cible à l'évolution probablement rapide de l'environnement.
La réussite du ministère dépend aussi de celle de ses partenaires (ANSSI, industriels de défense, opérateurs), lesquels participent d'ores et déjà à l'effort collectif.
La cohérence ne se décrète pas, c'est un combat du quotidien.

La loi de programmation militaire 2014 – 2019 et la cyberdéfense

Source : rapport législatif du Sénat sur le projet de loi.

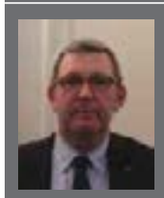
Promulguée le 18 décembre dernier, la loi n°2013-1168 relative à la programmation militaire pour les années 2014 à 2019 élargit le spectre des pouvoirs régaliens en matière de cyberdéfense. Elle définit un cadre juridique nouveau et prévoit des moyens humains et capacitaires renforcés. Elle contient un chapitre entier – le chapitre IV – consacré à la protection des infrastructures vitales contre la cybermenace.
La LPM développe dans un premier temps un cadre juridique qui adapte le droit face aux nouveaux défis de la cybersécurité. On peut distinguer quatre principaux volets :

1. Le premier volet clarifie les compétences au sein de l'Etat en matière de protection et de défense des systèmes d'information et en particulier le rôle majeur du Premier Ministre désormais consacré par une disposition législative.
2. Le second volet énonce des mesures visant à renforcer le niveau de sécurité des systèmes d'information des « opérateurs d'importance vitale » (environ 250 opérateurs issus du secteur public ou privé).
   - La possibilité pour l'Etat d'imposer à ces opérateurs des règles de sécurité
   - L'obligation pour ces opérateurs de notifier tout incident de sécurité
   - Le droit pour l'Etat de recourir à des audits ou contrôles des systèmes d'information
   - La possibilité pour l'Etat d'imposer des mesures techniques aux opérateurs en cas de crise informatique majeure.
3. Le troisième volet porte sur la capacité pour l'Etat de prendre des mesures de lutte informatique défensive avec notamment la possibilité d'accéder à des systèmes d'information assaillants pour étudier leur fonctionnement ou neutraliser les effets de leur attaque.
4. Enfin, un dernier volet concerne les équipements informatiques. Il vise à mieux maîtriser le risque d'espionnage à grande échelle des réseaux de communications électroniques.

Outre la refondation du cadre juridique cyber, La LPM prévoit également un renforcement sensible des moyens humains et financiers consacrés à la cyberdéfense (EMA, DGA et réserve citoyenne cyber). Enfin, le renforcement cyber concerne également le domaine capacitaire : 360 millions d'euros sur la période 2014-2019 alloués à l'acquisition et au fonctionnement d'équipements dédiés à la cybersécurité. De même, les crédits consacrés à la R&D dans le domaine cyber augmenteront sensiblement.

Pour que le cybercrime ne paie pas

La lutte contre la cybercriminalité est, avec la sécurité des systèmes d'information (SSI) et la politique de cyberdéfense, une des composantes qui concourent à la cybersécurité. Tout espace qui s'offre à l'Homme est porteur d'espérances, de liberté, de croissance. Mais il est aussi investi par les prédateurs. Le cyberespace n'échappe pas à la règle. Il est urgent d'y créer un ordre public.



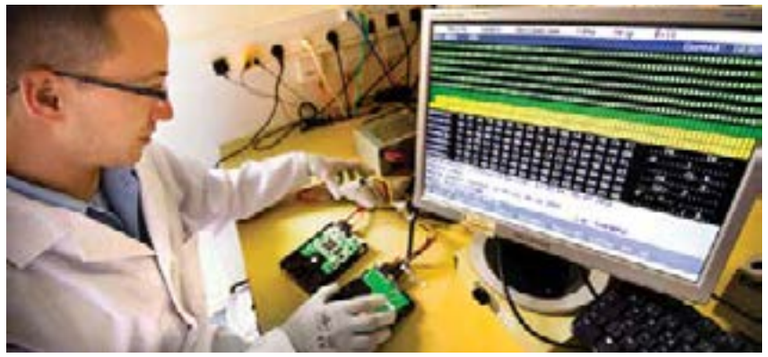
par
Marc Watin-Augouard,
Général d'armée

Ancien inspecteur général des armées – gendarmerie, le général d'armée Watin-Augouard dirige le centre de recherche de l'Ecole des Officiers de la Gendarmerie nationale. Il est membre du comité d'organisation du Forum international de la cybersécurité (FIC), dont il est le fondateur. Il enseigne à Paris II, Paris V, Lille II et Aix-Marseille III. Il est directeur de la rédaction de la Revue de la Gendarmerie nationale.

Dans les années soixante-dix, la crainte d'un développement non contrôlé et d'une utilisation frauduleuse des fichiers de données à caractère nominatif motivent les premières dispositions du code pénal régulant un cyberespace naissant. C'est la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés. Quelques années plus tard, en 1988, la prolifération de hackers animés d'intentions coupables entraîne le vote de la loi « Godfrain » protégeant pénalement les systèmes de traitement automatisé de données contre les attaques pouvant compromettre leur disponibilité, leur confidentialité, leur intégrité.

Puis, l'apparition du web, d'abord « statique », aujourd'hui dynamique, s'accompagne de l'essor d'infractions de « contenu » favorisées par le développement des réseaux sociaux et des blogs : pédopornographie, atteintes à l'image, à la réputation, incitation à la haine, etc. se banalisent. Enfin, la croissance du nombre d'internautes favorise la commission d'infractions, certes classiques, mais avec des résultats d'un tout autre ordre de grandeur : le produit des escroqueries sur Internet est sans commune mesure avec celui obtenu avec les méthodes traditionnelles. D'une manière générale, un transfert de la criminalité et de la conflictualité s'opère aujourd'hui depuis le champ du « matériel » vers celui de « l'immatériel ». Les atteintes aux personnes, aux biens, aux services ont suivi l'apparition successive des secteurs primaire, secondaire et tertiaire de l'économie. A chaque fois, les prédateurs ont procédé à un arbitrage entre l'avantage escompté et le risque pénal. Un secteur quaternaire fait aujourd'hui irruption avec le développement du « tout numérique ». Avec l'interconnexion massive des personnes et des biens, jamais le prédateur n'a été aussi proche de sa victime, puisqu'il peut accéder à son ordinateur, son smartphone, etc. Mais jamais aussi il n'a été aussi loin de son juge ! Les cybercriminels l'ont compris : agir dans le cyberespace peut leur rapporter gros avec un risque pénal faible, car l'entraide judiciaire est moins rapide que la propagation de leurs méfaits dans un cybermonde sans frontière.

Ainsi, au gré de la construction du cyberespace, la cybercriminalité se développe par strates successives, profitant des développements d'Internet. Elle est le fait de délinquants mais aussi de terroristes qui, sans avoir encore commis un cyberattentat, savent exploiter le net pour diffuser leur propagande, échanger des instructions, opérer des transferts d'argent. Depuis 2007, on sait aussi que la cybercriminalité peut être le fait de « guerriers » qui visent un Etat au travers de ses infrastructures critiques. Certains qualifient ces actes de « cyberguerre », mais ils oublient que, sans ennemi déclaré, le droit des conflits armés ne s'applique pas. Qu'ils visent des individus, des entreprises ou des Etats, les comportements illégaux relèvent le plus souvent de la cybercriminalité et donc principalement de l'action judiciaire. Les plus graves d'entre eux, ceux qui ciblent les opérateurs d'importance vitale, entrent aussi dans le champ de la cyberdéfense et justifient alors des mesures



de prévention, des actions diplomatiques, voire des réponses plus « offensives ». La lutte contre la cybercriminalité et la cyberdéfense se composent sans s'opposer. Avec les mêmes armes, sur le même « champ de bataille », la cybercriminalité peut indistinctement viser les individus, notamment dans leur identité, les entreprises dans leur créativité, les Etats dans leur souveraineté. La lutte contre la cybercriminalité et la cyberdéfense s'inscrivent dans un continuum défense-sécurité, particulièrement remarquable dans le cyberespace.

Au regard d'un phénomène ignorant par construction les frontières, une stratégie universelle de cybersécurité aurait été souhaitable. Hélas ! Les enjeux de puissance favorisent les égoïsmes nationaux, tandis que la liberté d'expression n'est pas considérée de la même manière sur l'ensemble de la planète. L'échec de la Conférence de Dubaï (décembre 2012), sous l'égide de l'Union Internationale des Télécommunications (UIT), est révélateur d'un impossible consensus, sauf à opter pour un accord minimaliste inopérant. Le seul instrument normatif existant, à vocation internationale est la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest du 23 novembre 2001). Celle-ci n'a cependant été ratifiée que par une quarantaine d'Etats.

A l'échelle de l'Union européenne, l'année 2013 semble marquée par une évolution positive. La stratégie de cybersécurité, présentée en février, quelques jours après la création d'un Centre européen de lutte contre la cybercriminalité au sein d'Europol (EC3), le renforcement des compétences de l'ENISA, agence européenne dédiée à la sécurité des réseaux, et la directive 2013/40/UE du 12 août relative aux attaques contre les systèmes d'information témoignent d'une volonté plus affirmée de développer une politique européenne.

Mais les Etats devront encore longtemps compter sur eux-mêmes. Depuis le Livre blanc sur la défense et la sécurité nationale de 2008, la France s'est engagée dans une stratégie volontariste que le dernier Livre blanc vient conforter. La loi de programmation militaire, promulguée le 19 décembre, renforce les deux piliers de la cyberdéfense : l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) et le pôle défense (EMA-cyberdéfense et DGA - MI) vont bénéficier d'une augmentation sensible de leurs moyens humains, matériels et juridiques. Il faudra sans aucun doute les revoir encore à la hausse avant le terme de la loi (2019), car les besoins seront assurément croissants dans les prochaines années. Mais l'action régalienne ne peut être équilibrée sans que l'on conforte de manière similaire les capacités de lutte contre la cybercriminalité. La gendarmerie, la police, la douane disposent de compétences déployées au sein de services spécialisés. La cybercriminalité est désormais présente dans les prétoires, mais il n'y a pas encore une véritable politique pénale en la matière, ni de juridiction spécialisée au regard d'un contentieux souvent très technique. Le groupe de travail interministériel, dirigé par le procureur général Marc Robert, devrait présenter des propositions au début de l'année 2014. Conforté, le pôle « cybercriminalité » devra travailler d'une manière plus étroite avec le pôle cyberdéfense, car l'offre régalienne de cybersécurité doit reposer sur le tryptique du « pompier », du « soldat » et du « gendarme ». Il ne servirait à rien de développer les indispensables partenariats public/privé qu'appelle la sécurité du cyberespace si le socle étatique n'est pas solidifié.

L'ordre public dans le cyberespace n'est pas la négation de l'esprit de liberté qui a animé ses fondateurs. Sans ordre, il n'y pas de liberté, car règne alors la loi du plus fort. Aujourd'hui, l'Etat n'a pas le choix, sauf à admettre que les criminels de toute nature deviennent les maîtres de l'espace numérique. Certains avaient parié sur la fin de l'Etat. Le cyberespace donne à ce dernier une nouvelle chance de prouver sa légitimité en contribuant à la sécurité des personnes et des biens, afin que le crime ne paie pas.

La cyberdéfense dans la nouvelle politique de défense de la France

Le livre blanc de la Défense et de la Sécurité Nationale 2013 fait de la cyberdéfense une priorité pour la souveraineté nationale.

Depuis le livre blanc de 2008, la cyberdéfense est montée en puissance au sein du ministère et des armées. Elle est aujourd'hui devenue un nouveau domaine militaire et opérationnel au même titre que les domaines terrestre, aérien, maritime et extra-atmosphérique.

par
Arnaud Coustillière,

Contre-amiral
Etat-major des armées

Le contre-amiral Arnaud Coustillère est actuellement officier général cyberdéfense. Directement rattaché au sous-chef « opérations » de l'état-major des armées, et placé sous la double tutelle du chef d'état-major des armées et du chef de cabinet du ministre, il est responsable de la cyberdéfense du ministère et de sa conduite en situation de crise cybernétique. A l'état-major des armées depuis 2008, il a exercé la fonction d'officier de cohérence opérationnelle en charge du domaine des télécommunications et de la cyberdéfense. Il a également occupé plusieurs postes tant à l'état-major de la force d'action navale (doctrine) qu'à l'état-major de la marine.

Le Livre Blanc sur la Défense et la Sécurité Nationale (LBDSN) de 2013 renforce l'importance stratégique accordée à la cyberdéfense. Il indique notamment qu'une attaque visant la destruction ou la prise de contrôle à distance de systèmes informatisés commandant le fonctionnement d'infrastructures d'importance vitale, de systèmes de gestion automatisés d'outils industriels potentiellement dangereux, voire de systèmes d'armes ou de capacités militaires stratégiques n'est pas à exclure et constitue une menace sérieuse.

Le rôle de l'Etat est central dans ce domaine, que ce soit dans la mise en place d'une capacité de réponse aux attaques, d'un cadre juridique protecteur et adapté, ou de l'incitation au développement d'entreprises de confiance.

Notre capacité à se protéger de ces attaques constitue un élément de la souveraineté nationale. La protection de notre potentiel économique, industriel, militaire et de recherche passe par la mise en œuvre d'une posture globale et robuste de cyberdéfense. La doctrine nationale de réponse permet de pourvoir à cette nécessité. Elle repose sur deux piliers :

1. la mise en place d'une posture robuste et résiliente de protection des systèmes d'information de l'Etat, des opérateurs d'importance vitale et des industries stratégiques, couplée à une organisation opérationnelle de défense, coordonnées sous l'autorité du Premier ministre, reposant sur une coopération étroite des services de l'Etat ;
2. une capacité de réponse gouvernementale globale et ajustée face à des agressions de nature et d'ampleur variées faisant en premier lieu appel à l'ensemble des moyens diplomatiques, juridiques ou policiers, sans s'interdire l'emploi gradué de moyens relevant du ministère de la défense, si les intérêts stratégiques nationaux étaient menacés.

La coopération interministérielle et interarmées au cœur de la cyberdéfense

Le ministère de la Défense est en charge de la défense de ses systèmes d'information et de ceux des armées. Il travaille à la mise en œuvre de la doctrine en liaison étroite avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le ministère de l'Intérieur et le ministère des Affaires Etrangères.

Une chaîne de commandement interarmées et ministérielle, placée sous l'autorité du chef d'état-major des armées, a été mise en place pour conduire l'ensemble de la défense des systèmes d'information du ministère et des armées, et soutenir les opérations militaires, à travers l'emploi de capacités informatiques défensives ou offensives. Cette chaîne couvre toutes les armes du Ministère de la défense. Elle est unifiée pour gommer les fractures au sein de nos organisations, centralisée pour réagir vite et mobiliser d'entrée les meilleures capacités possibles, et spécialisée car elle demande des procédés adaptés et des compétences particulières.

L'officier général « cyberdéfense » remplit deux fonctions : l'une, opérationnelle, au sein du Centre de Planification et de Conduite des Opérations (CPCO), pour la planification, la coordination et la conduite des opérations de cyberdéfense. La seconde dite « organique », transverse, pour coordonner les travaux relatifs à la montée en puissance de la cyberdéfense des armées.

La chaîne de cyberdéfense s'appuie sur les opérateurs des systèmes d'information des armées et du ministère qui surveillent et défendent les réseaux qu'ils mettent en œuvre. Pour pouvoir répondre aux cyberattaques qui demandent un niveau d'expertise élevé et un temps de réaction très court, le Ministère de la défense dispose en tête de chaîne du Centre d'Analyse et de Lutte Informatique Défensive (CALID) et de Groupes d'Intervention Rapide (GIR).

Le CALID traite des attaques les plus complexes. Il réalise au quotidien un travail de surveillance, d'investigation, de veille et d'analyse. Il travaille étroitement avec son homologue à l'ANSSI, le COSSI. A titre indicatif, le CALID a eu à traiter plus de 500 incidents depuis le début de l'année 2013 alors qu'on en comptait seulement 196 en 2011 et 420 en 2012. Cette augmentation est à la fois le résultat du renforcement de notre niveau de vigilance mais également de la hausse des attaques ciblées.

Les GIR sont des groupes mobilisables très rapidement en cas d'incident cyber, lorsqu'une action spécialisée devient nécessaire sur le terrain. Ils interviennent au côté des opérateurs et apportent l'expertise nécessaire. Les effectifs mobilisés peuvent s'accroître très rapidement en fonction de la gravité de l'attaque, et participent ensuite au rétablissement du bon fonctionnement de l'organisme ciblé.

Le pendant technique de cette mission opérationnelle est confié à la Direction générale de l'armement (DGA), au pôle « sécurité des systèmes d'information », chargé de développer et d'assurer un très haut niveau de protection pour les besoins des forces armées. Ce travail se fait en étroite concertation avec les autres acteurs de la cyberdéfense nationale. Des liens très forts sont recherchés entre entités opérationnelles et techniques, ministérielles et interministérielles ; ils sont une condition indispensable à l'efficacité globale du dispositif de cyberdéfence de la France.

La sensibilisation comme moteur de la stratégie française

La sensibilisation et la formation sont également les piliers d'une posture de cyberdéfense robuste. Ces deux éléments jouent un rôle prépondérant afin d'une part, de préserver la confiance dans la société et l'économie numérique, et d'autre part, de réduire les risques informatiques.

Le rappel des règles élémentaires d'hygiène informatique et des responsabilités de chacun permet de limiter les risques d'infection et de propagation et de sensibiliser les utilisateurs aux risques juridiques liés à une utilisation imprudente ou détournée des systèmes d'information. Ces règles doivent être très largement diffusées et régulièrement rappelées tout en s'accompagnant d'un effort de développement de systèmes d'information résilients produits par des entreprises de confiance.

Pour contribuer à cet effort de sensibilisation, le Ministère de la défense, en liaison étroite avec ses partenaires étatiques, a notamment mis en place un réseau de réservistes citoyens spécialisés en cyberdéfense depuis 2012. Il vise à promouvoir un esprit de cyberdéfense en étroite concertation avec les autorités nationales. Des travaux de réflexion concernant la mise en place d'une réserve à vocation opérationnelle se mettent progressivement en place. Elle permettra de disposer d'une capacité de cyberdéfense démultipliée en cas d'attaque informatique majeure.

Sur l'impulsion du LBDSN de 2013, un pôle d'excellence en matière de cyberdéfense est notamment en train d'être constitué en Bretagne. Des formations seront dispensées au sein de ce pôle, en associant divers partenaires tels que l'Ecole des transmissions (ETRS) ou encore le pôle Maîtrise de l'Information (MI) de la DGA.

Le livre blanc de 2008 a lancé une dynamique ambitieuse pour la cyberdéfense française. Le LBDSN de 2013 poursuit les efforts entrepris et les concrétise pour donner toute sa place à la cyberdéfense en tant que nouveau domaine opérationnel. La loi de programmation militaire vient de plus apporter un cadre nouveau notamment sur le plan juridique. L'année à venir s'annonce riche en évolutions.

Retour sur le FIC 2014

Le 6ème forum international de la cybersécurité (FIC) a eu lieu les 21 et 22 janvier au Grand Palais de Lille. Organisé par la Gendarmerie Nationale, CEIS et le Conseil régional du Nord-Pas-de-Calais, ce forum a l'objectif de nourrir la réflexion et de favoriser les échanges en réunissant l'ensemble des acteurs et des décideurs du monde la cybersécurité. Le thème est d'ailleurs abordé sous tous ses aspects : stratégique, opérationnel, juridique, technologique et industriel. L'allocution d'ouverture du Ministre de l'Intérieur Manuel Valls et le discours du Ministre de la Défense Jean-Yves Le Drian figurent parmi les moments forts du FIC 2014.

Le FIC s'affirme comme événement majeur de la cybersécurité au niveau français et européen avec près de 3500 participants cette année rassemblés sur 1500 m² quand, en 2013, ils étaient 2400 participants sur 800 m². Le succès du forum confirme également l'essor de ce secteur d'activité. Avec 12% de participants étrangers de 58 nationalités, le forum créé par la Gendarmerie Nationale en 2007 rassemble notamment les grandes entreprises, les PME et ETI, les universités et grandes écoles et la fonction publique.

Le ministère de la Défense était bien représenté grâce à la présence de la Direction générale de l'armement (DGA), du Centre d'analyse en lutte informatique défensive (CALID), du Commandement des forces terrestres (CFT) et de la Réserve Citoyenne de Cyberdéfense (RCC).

La réserve citoyenne de cyberdéfense fait des émules

Elle connaît même un franc succès, notamment auprès des jeunes

L'idée d'une réserve citoyenne semble aller à contre-courant de la spécialisation à tous crins des forces armées depuis la fin de la conscription. Cette initiative ambitieuse constitue pourtant une brique fondamentale de la lutte « cyber ». Son succès lui promet un bel avenir. Présentation par le Coordinateur national de la réserve citoyenne de cyberdéfense.

par
Luc François Salvador,
Colonel de réserve, PDG de SOGETI

Propos recueillis par Frédéric Tatout

Luc-François Salvador a passé sa prime enfance en Afrique Equatoriale Française (AEF) où son père servait en tant que sous-officier de l'Armée de l'Air française. En 1976, il rejoint l'Armée de l'air comme engagé volontaire dans le corps des élèves sous-officiers (spécialité informatique). En 1978 il intègre Cap Sogeti Exploitation, alors une société de 40 informaticiens qui deviendra plus tard le Groupe Sogeti dont il assumera la Présidence et la Direction générale en 2000. Auditeur de la 49ème session nationale de l'IHEDN, il devient par la suite membre du Comité Exécutif du Groupe Capgemini.

La CAIA : Quels sont les enjeux et la genèse de cette initiative ?

LFS : La recrudescence de la cybercriminalité faisait entrevoir la possibilité d'un « grand soir » de la sécurité informatique. En 2009 une attaque dirigée contre un Etat, l'Estonie (en lien avec la Bronze Night) a donné corps à cette crainte. Un sursaut devenait clairement nécessaire. Fin 2012, le Président de la République annonce la création d'une « cyber-réserve ». En juin 2013, l'université d'été de la défense, organisée à Rennes, place la cyberdéfense en tête de l'agenda, comme un enjeu mondial et une priorité nationale comme l'a écrit le Sénateur Jean-Marie Bockel dans son rapport. Le Livre blanc va plus loin en donnant corps à une initiative forte.

La CAIA : Pourquoi une cyber-réserve citoyenne ?

LFS : Tout d'abord, l'espace « cyber » constitue une « 5e dimension » sans frontière, à l'instar de la 4e, qui est le spatial. Même limite ténue entre militaire et civil, tant les ramifications entre ces deux sphères sont multiples. De nombreux praticiens de la sécurité informatique voyaient mal comment une cyberdéfense militaire isolée dans sa bulle serait durablement efficace sans ramifications fortes avec le civil. Et si, seules, des attaques hors normes pouvaient toucher la Défense, comment croire que le civil serait épargné ?
Ensuite, la menace est diffuse et difficile à déceler, ses effets sont sans délai ni limite claire. Autrement dit, tout le « raisonnement de défense » est à refaire. De fond en comble c'est-à-dire jusqu'à des concepts fondamentaux tels que la posture de défense et la résilience de la Nation. Dans la perspective de ces concepts, les démarches d'engagement patriotique et l'esprit de défense apparaissent d'emblée comme des facteurs clés du succès. Bien sûr, cela paraît moins naturel en France qu'aux Etats-Unis. Nos débuts sont donc relativement modestes. Ils consistent à accompagner la LPM en étant force de proposition, notamment de la relation entre cette LPM et les industriels, et en posant des fondations solides.

La CAIA : En quoi consiste la réserve cyber-citoyenne ?

LFS : Je commencerai par évoquer le fait que cette organisation est régie par des principes, au premier rang desquels les suivants : y servir représente un engagement patriotique, personnel, humble et bénévole, à ne surtout pas confondre avec l'activité professionnelle. Ces principes constituent notre ADN, ils figurent dans la charte de déontologie signée par tous les membres.
Par ailleurs, il s'agit de la première réserve citoyenne transverse à toutes les armées y compris la Gendarmerie nationale compte tenu des enjeux globaux du sujet.
Sa structure est bicéphale : une tête au cœur de l'institution militaire, animée par l'Officier général cyberdéfense et quelques « étatiques » permanents de son équipe au sein du CPCO, ressource précieuse pour épauler le développement de la réserve ; l'autre tête, constituée de civils, que j'ai l'honneur d'animer. Elles réalisent un premier niveau de synthèse au profit de l'EMA et co-pilotent l'ensemble des travaux.
Forte de ces éléments structuraux, la réserve citoyenne se décline en groupes de travail créés selon ses enjeux opérationnels. Actuellement il y en a 7 :

1. groupe « Relais d'opinion » : il rassemble régulièrement, pour aborder des sujets spécifiques, une cinquantaine d'intellectuels et personnages influents des sphères économique et politique, tous volontaires pour jouer le rôle de caisse de résonnance ;
2. groupe « Elus et journalistes » : il prépare des éléments de synthèse et de communication, ciblés selon les attentes de la presse et les besoins du moment et participent activement à la sensibilisation des parlementaires hors de la commission de Défense ;
3. groupe « Jeunes » : il œuvre à renforcer le lien entre les jeunes compétences dans le domaine de la cybersécurité et les besoins nationaux ; au passage, nous les sensibilisons aux enjeux régaliens de la sécurité informatique. Le degré d'implication des participants nous a surpris. Il dénote une réelle soif d'engagement, qui surpasse les attentes professionnelles ;
4. groupe « *Think Tanks* » : il permet d'inner-ver différents groupes de réflexion, dans une démarche d'enrichissement mutuel ;
5. groupe « Evolution de la réserve » : davantage tourné vers l'intérieur, il réfléchit aux orientations à donner pour déployer et approfondir l'initiative et préciser des modalités d'emploi et de mobilisation en cas d'attaque majeure ;
6. groupe « PME » : il vise à faire mûrir et partager des bonnes pratiques appropriées aux PME, qui constituent une proie facile des attaquants ;
7. groupe « OIV » (Opérateurs d'Infrastructures Vitales). Son objectif est proche du précédent, avec une connotation juridique un peu plus marquée et en lien avec les articles 13 à 16 de la LPM.

Nous avons fait le choix de mettre tout cela en place sous un format limité à 80 personnes environ. C'est peu, mais comme déjà évoqué, la priorité dans un premier temps est de créer des fondations solides.
Et je dois dire que nous disposons déjà de plus de 3 000 candidatures, la plupart très solides, auxquelles nous n'avons pas encore vraiment donné suite, au risque de créer peut-être quelques frustrations. Nous considérons cela comme un potentiel précieux. Il sera exploité le moment venu.

La CAIA : Quelles sont donc les prochaines étapes et les perspectives ?

LFS : Forts d'une base solide, « prouvée » par le succès des opérations que nous avons lancées, nous venons de lancer une deuxième vague de recrutement pour étendre notre noyau dur à la province.
Nous pourrons alors passer au déploiement progressif, sur le long terme.
Pour nous un jalon important est le 6e Forum International de la Cybersécurité (FIC) qui a eu lieu du 22 au 25 janvier 2014 à Lille. Il a été un lieu de rencontre privilégié entre spécialistes et non initiés et entre le secteur public et le secteur privé.

La CAIA : Sous un angle plus personnel, qu'est-ce qui t'a conduit à diriger la tête civile de la réserve cyber ?

LFS : Je n'ai pas connu de carrière militaire, mais j'ai développé, de par mes racines familiales et mon passé d'enfant de troupe, un profond respect pour l'institution. Après un service militaire passionnant, c'est tout naturellement que je suis entré dans la réserve. En proposant d'œuvrer pour la réserve « cyber », j'ai voulu prolonger cet engagement au service des convictions que je porte et en ligne avec mes capacités professionnelles.

Evénement Epita

Il a été dernièrement organisé une journée d'échange avec l'Epita (école d'ingénieurs en informatique et techniques avancées). Ce fut l'occasion de présenter aux étudiants l'ensemble de la chaîne de cyberdéfense française et de les sensibiliser au sujet. Epita possède déjà une culture de la sécurité informatique et il est important d'être présent dans cette école qui a su anticiper le sujet. Le succès de cette journée nous a étonné, de même que l'enthousiasme des jeunes qui ont été rencontrés. A mes yeux, il s'agit bien plus que d'un succès d'estime. Cela dénote une soif d'engagement pour la noble cause de la cybersécurité.

Réserve opérationnelle et réserve citoyenne, deux outils au service du lien défense nation

- la réserve opérationnelle, 56 000 volontaires dont 20 000 dans la gendarmerie, souvent d'anciens militaires mais pas uniquement, qui effectuent des périodes en uniforme dans les unités. Ils représentent un complément de main d'œuvre pour les forces. Certains réservistes font jusqu'à 180 jours par an d'activités militaires.

- la réserve citoyenne, dont il est question ici, est constituée de 3000 bénévoles (dont 1000 dans la gendarmerie), sans uniforme, plus rarement d'anciens militaires, qui constituent un réseau d'influence pour développer la culture de défense. La réserve citoyenne de cyberdéfense a vocation à y prendre une place croissante.

Que font les Etats-Unis et nos voisins européens ?

Aux Etats-Unis une « *cyberleague* » a été mise en place sous le gouvernement Clinton. Elle présente une forte connotation militaire, par exemple ses membres portent l'uniforme.
Au Royaume-Uni, la stratégie nationale de sécurité de l'information élaborée en 2003 a accouché d'un *National Information Security Coordination Center*, qui a connu un prolongement en 2008 avec la mise en place d'un plan de recrutement de « *ethical hackers* ». Une deuxième vague a été lancée avec la création d'une cyber réserve en 2012, dotée d'un budget de 580 M£.

En Allemagne, les activités de supervision de la sécurité sont incarnées par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) sous le contrôle du Parlement. Par ailleurs, les acteurs industriels se sont fédérés depuis bientôt 20 ans au sein de l'association TeleTrust, qui assure une promotion forte de ses membres, notamment dans les salons internationaux. Il n'existe pas de cyber-réserve citoyenne mais une doctrine de protection des sites sensibles a été élaborée en février 2011, puis en avril 2013 un centre de cyberdéfense nationale forte de 600 membres a été constitué.

La défense des opérateurs d'importance vitale – enjeux et difficultés

L'actualité récente a montré que des entreprises productrices d'énergie, des entreprises de communication ou encore des banques pouvaient être victimes d'attaques informatiques d'envergure, susceptibles de ralentir ou de paralyser l'activité de pans entiers de l'économie d'une nation. Les évolutions technologiques en cours ou prévisibles invitent à une meilleure prise en compte de la sécurité et de la défense des systèmes d'information des opérateurs d'importance vitale afin de préserver notre souveraineté, notre économie et la sécurité de nos concitoyens. La loi de programmation militaire, adoptée le 18 décembre dernier, offre à cette fin de nouveaux leviers.

par **Bruno Marescaux,**
ICA

Chef adjoint du centre opérationnel de la sécurité des systèmes d'information à l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Bruno Marescaux commence sa carrière en 2001 à DGA-Maîtrise de l'information, avant d'occuper des postes en cabinet auprès du Directeur des essais puis du Délégué général pour l'armement. En 2007 - 2008, il prend part à la rédaction du Livre blanc sur la défense et la sécurité nationale et sert jusqu'en 2013 au sein du cabinet du Secrétaire général de la défense et de la sécurité nationale.

Les opérateurs d'importance vitale sont des cibles privilégiées dans le cyberespace, à plus d'un titre

Le code de la défense définit dans son article L. 1332-1 des opérateurs « dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation ». Ces opérateurs, dits d'importance vitale, voient aujourd'hui leurs systèmes d'information exposés à des attaques multiples dans le cyberespace, qui sont susceptibles de constituer de véritables atteintes à la sécurité nationale. Ces attaques sont essentiellement de trois types.

Les attaques à des fins de déstabilisation.

Aujourd'hui, il est possible de louer à bas coût, voire gratuitement, un réseau d'ordinateurs infectés et de piloter ceux-ci à distance depuis Internet afin qu'ils saturent d'informations des réseaux de communication ou des services en ligne. Menées à grande échelle, ces attaques, dites en déni de service, sont susceptibles d'engendrer une paralysie des services essentiels à la vie de la nation. De telles attaques ont par exemple été menées, du 18 septembre 2012 au 2 mai 2013, contre trente-trois des plus importantes institutions financières américaines. Ces attaques auraient coûté plus de 10 millions de dollars à la seule institution Bank of America.

Les attaques à des fins d'espionnage.

Les entreprises françaises de toutes tailles, notamment les plus exposées à la concurrence internationale ou les plus innovantes ainsi que celles évoluant dans des secteurs stratégiques, sont aujourd'hui victimes d'attaques informatiques menées à des fins d'espionnage. Les « attaquants » - services de renseignements, officines, groupes criminels ou entreprises concurrentes - exploitent à leur profit, parfois depuis plusieurs années, les savoir-faire technologiques, industriels ou les facteurs-clés de succès des entreprises visées.

Les attaques à des fins de sabotage, voire de terrorisme.

Les systèmes industriels se modernisent et deviennent progressivement interconnectés et pilotés à distance via Internet, ce qui les rend vulnérables à des attaques informatiques. En août 2012, le sabotage massif du parc informatique de la société saoudienne Aramco - plus de 30 000 ordinateurs mis hors service - a par

exemple perturbé le fonctionnement des activités opérationnelles du premier exportateur mondial de brut pendant plus de quinze jours. Au printemps 2013, le sabotage programmé de l'infrastructure informatique des principales banques et de médias coréens a provoqué la mise hors service des distributeurs automatiques de billets et d'applications bancaires en ligne.

La conscience du danger et les mesures prises par les entreprises, notamment par les opérateurs d'importance vitale, sont encore loin d'être à la hauteur de la menace

La sécurité des systèmes d'information est une question humaine avant d'être une question technique. Sans trop caricaturer et pour fixer les idées, on peut observer que les dirigeants d'entreprises - et le top management des opérateurs d'importance vitale n'échappe pas à cette règle - sont dans l'ensemble trop peu conscients des menaces et des cyber-risques qui pèsent sur leur activité alors même qu'ils numérisent de plus en plus les fonctions de l'entreprise pour en augmenter la qualité de service et la compétitivité et que les produits ou services offerts par celle-ci intègrent de plus en plus de systèmes d'information connectés.

On peut aussi relever que les entreprises, soucieuses du maintien de leur marge, répugnent couramment à engager les investissements proposés par leurs responsables de la sécurité des systèmes d'information qui, bien souvent :

1. ne siègent pas dans les instances dirigeantes et ont parfois du mal à faire entendre leur voix ;
2. sont débordés par des demandes toujours plus importantes d'utilisateurs ou de hiérarchies ignorant les règles de sécurité les plus simples et exigeant d'accéder, dans leur univers professionnel, au même confort et aux mêmes ressources que dans la sphère privée. Les moyens d'action concrets des responsables de la sécurité des systèmes d'information sont en pratique extrêmement limités.

De fait, en dépit de l'action de l'ANSSI en matière de sensibilisation aux risques et de la tenue de multiples colloques visant à évoquer l'impact des attaques informatiques sur la chaîne de valeur de l'entreprise, et même si les révélations d'Edward Snowden ont sans doute amené à une certaine forme de prise de conscience, force est de constater que le niveau de sécurité des systèmes d'information des opérateurs d'importance vitale n'augmente ni significativement, ni rapidement.

La loi de programmation militaire récemment adoptée par le parlement porte des dispositions visant à renforcer la sécurité et la défense des opérateurs d'importance vitale

Adoptée le 18 décembre dernier, la loi de programmation militaire donne à l'Etat les moyens d'imposer aux opérateurs, sous peine de sanctions, des mesures de sécurité efficaces. Quatre dispositions essentielles sont inscrites dans la loi.

Le Premier ministre peut imposer des règles aux opérateurs d'importance vitale concernant leurs systèmes d'information critiques.

Ces règles seront conjointement élaborées avec les opérateurs concernés, sous le pilotage du ministère coordonnateur du secteur d'activité d'importance vitale correspondant. Pour les systèmes d'information les plus sensibles pour l'activité et lorsque la situation l'imposera, elles pourront comprendre l'obligation de mettre en œuvre un système de détection d'attaques informatiques. Un décret d'application précisera en 2014 notamment la procédure de qualification des équipements de détection et des prestataires susceptibles de les opérer, ainsi que les conditions d'exploitation de ces équipements.

Les opérateurs d'importance vitale sont tenus de notifier les incidents significatifs intervenant sur leurs systèmes d'information critiques.

La notification par les opérateurs des incidents significatifs survenus sur les systèmes d'information essentiels à leur activité permettra d'identifier les attaques informatiques nécessitant une intervention de l'ANSSI, d'une autre administration de l'Etat ou d'un prestataire de confiance. Un décret d'application précisera en 2014, par secteur d'activité, le type d'incidents à notifier, les niveaux de gravité et les délais dans lesquels ces incidents devront être déclarés.

Les opérateurs d'importance vitale sont tenus de soumettre à un contrôle ou à un audit de sécurité leurs systèmes d'information, à la demande du Premier ministre.

Il s'agit, par cette mesure, d'étendre à l'ensemble des secteurs d'activité d'importance vitale une capacité de contrôle de sécurité et d'intégrité déjà prévue par le code des postes et des communications électroniques pour les réseaux des opérateurs de communications électroniques. Ces contrôles permettront notamment d'évaluer le niveau de sécurité des équipements, voire de détecter leur éventuelle compromission. Un décret d'application précisera les conditions d'exercice de ces contrôles et audits.

En cas de crise informatique majeure, le Premier ministre peut imposer des mesures aux opérateurs d'importance vitale.

La loi donne une solidité juridique aux mesures techniques que le Premier ministre peut décider d'imposer aux opérateurs d'importance vitale pour réagir dans des délais courts à une crise majeure menaçant ou affectant la sécurité de nos systèmes d'information.

Principaux enjeux juridiques liés à la cyberdéfense

La création d'un corpus juridique qui encadrerait les opérations de cyberdéfense n'en est qu'à ses premiers balbutiements. Elle bute notamment sur des écarts doctrinaux entre états et sur la difficulté de formaliser des concepts opératoires. Le moment est venu pour la France de définir une position cohérente et la faire entendre, sous peine de se laisser imposer une approche qui serait contraire à ses convictions.

par **Eric Turquet de Beauregard,**
Commissaire en chef
Eric Turquet de Beauregard est Chef du bureau du droit des conflits armés à la Sous-direction du droit international et européen de la Direction des affaires juridiques du Ministère de la Défense.

Les implications juridiques liées à la thématique « cyber » entrent de plus en plus dans le champ des préoccupations du ministère de la Défense, comme l'ont rappelé le récent Livre blanc et la loi de programmation militaire (LPM 2014-2019). La France ne réfléchit évidemment pas seule sur ce sujet.

- **Dans le cadre des Nations unies**, un Groupe d'experts gouvernementaux (GGE) a été chargé en 2013 de définir des normes de comportement et de mesures de confiance entre Etats dans le cyberespace. De nombreuses interrogations ont été soulevées : le droit international actuel est-il suffisant pour prendre en compte la montée en puissance du cyberespace ? Peut-on faire contrôler le cyberespace par les Etats sans porter atteinte aux droits de l'homme sur internet ? A partir de quels moments peut-on parler de d'état de légitime défense permettant une réponse, armée ou non ? etc.
- **Un travail de réflexion sur ces mêmes thématiques a également été lancé au niveau de l'OTAN** par le Centre d'excellence « Cyber » de Tallinn. Le résultat de ces travaux a été présenté à Londres le 15 mars 2013 et compilé dans un Manuel dit « de Tallinn » qui présente la somme des réflexions juridiques liées à la cyberguerre.
- **L'UE a de son côté adopté en 2010 une stratégie de sécurité intérieure** qui évoque les aspects « cyber » et une directive conjointe du Parlement européen et du Conseil en date du 12 août 2013 traite plus spécifiquement des attaques contre les systèmes d'information.
- **Il n'existe pas de dispositions dans des traités internationaux qui traitent directement de la cyberguerre.** Et pour cause, c'est une problématique récente. Et, pour la même raison, il est difficile de conclure à l'existence de règles internationales coutumières spécifiquement dédiées au domaine « cyber ». Mais cela ne signifie pas que les cyberopérations sont confrontées à un vide juridique. Les experts de Tallinn ont en effet été unanimes sur le fait que le droit international en l'état actuel des choses pouvait tout à fait s'appliquer aux cyberopérations. Mais il subsiste néanmoins des zones d'ombre et leurs conclusions ne sauraient être reprises in extenso. Ils n'ont d'ailleurs pas toujours été d'accord entre eux, tant sur la notion de recours à la force que sur celle de l'application du droit international humanitaire.

1. Les actions « cyber » considérées comme facteur déclenchant d'un conflit armé (*jus ad bellum*)

1.1 Si l'on évoque le recours à la force stricto sensu, les experts de Tallinn se sont accordés sur le fait qu'il y a emploi de la force si la cyberattaque provoque la mort, des blessures, ou des destructions matérielles significatives (ex. : explosion d'une centrale nucléaire). Mais pour qu'il y ait emploi de la force au sens du droit international, il faut également un armement et un financement par un Etat. Se pose donc la question des acteurs non-étatiques qui seraient à l'origine d'une telle action, voire du hacker isolé. La preuve de l'implication d'un Etat sera difficile à apporter, sans même évoquer l'emploi de la force ayant pour origine des groupes se trouvant sur le territoire d'un Etat failli.

En revanche, pour les attaques « cyber » n'ayant pas d'incidence physique, ou qui ont des effets réversibles, la qualification d'attaque n'a pu être retenue. Et il n'a pas non plus été possible de déterminer un seuil de déclenchement (avec des critères quantifiables) permettant la qualification d'emploi de la force. Cela laisse donc à ce stade une marge d'interprétation assez grande par les Etats selon les circonstances. Ce qui conduit à évoquer la notion de légitime défense (liée à celle d'agression armée).

1.2 L'exercice de la légitime défense, au sens de l'article 51 de la Charte des Nations unies, impose l'existence préalable d'une agression armée. Mais cette dernière n'a pas été définie par la Charte, et c'est l'Assemblée générale des Nations unies (AGNU) qui s'en est chargée (cf. Résolution 3314 du 14/12/1974). La liste des actes d'agression qui s'y trouve n'est pas limitative et a seulement une valeur déclarative. Car seul le Conseil de sécurité est compétent pour qualifier une situation d'agression armée. A titre d'exemples cités par l'AGNU : l'invasion du territoire d'un Etat, l'occupation militaire, ou encore l'envoi par un Etat de groupes armés, de forces irrégulières contre un autre Etat. On revient donc sur les problématiques évoquées précédemment (nécessité de l'action d'un Etat). C'est également la position de la Cour internationale de justice (cf. CIJ, 1986, Nicaragua et 2004, Affaire du Mur).

Cette notion d'agression armée appliquée au domaine « cyber » est problématique : la paralysie de l'économie et l'attaque de systèmes bancaires peuvent-elles être considérées comme

des agressions armées ? Faut-il là aussi avoir recours à un effet de seuil au-delà duquel on peut affirmer qu'il y a agression armée ? Certains experts ont avancé la notion d'effets immatériels suffisamment graves ou la « théorie de l'accumulation des effets ».

Et l'on retrouve dans les réflexions touchant au monde « cyber » les clivages ou les divergences d'appréciation qui ont cours dans le monde « conventionnel ». C'est le cas pour la qualification de la légitime défense en elle-même. Les anglo-saxons parlent volontiers de légitime défense préemptive (dans le cas du « cyber » on parlera alors d'une attaque imminente nécessitant une action immédiate par l'Etat visé. C'est ce que les Américains appellent « *The last window of opportunity* ». Dans ce cas, se pose la question de la faculté des Etats à prévoir une agression cybernétique. Il n'y a pas de consensus sur ce point parmi les experts, comme on peut s'en douter. Il y a en revanche unanimité sur l'interdiction de la légitime défense préventive.

Un dernier point mérite enfin d'être évoqué, celui de la perfidie, proscrite par le DIH.

2. Quid de l'applicabilité du droit international humanitaire au « cyber » (*jus in bello*) ?

2.1 La conduite des opérations est régie par les principes de discrimination et de proportionnalité. Et dans ce domaine aussi, de nombreuses interrogations surgissent. Si l'on examine tout d'abord le principe de discrimination, c'est-à-dire la distinction entre les objectifs militaires et les biens civils, le droit international humanitaire (DIH) prescrit que les attaques ne doivent être dirigées que contre un objectif militaire déterminé ou avec des moyens dont les effets peuvent être limités. Sont également prohibées les attaques qui pourraient causer des pertes en vies humaines dans la population civile et/ou des dommages à caractère civil excessifs par rapport à l'avantage militaire concret et direct attendu.

Il s'agit ici de savoir si les nouvelles technologies peuvent permettre de garantir le respect de ces règles : les cyberopérations peuvent-elles atteindre avec précision l'objectif visé ? Cela soulève la question de l'adéquation des cyberattaques avec la nécessaire protection des établissements et équipements médicaux. Selon les Conventions de Genève, ces établissements doivent être en tout temps respectés et protégés (art. 19, 1re Convention de Genève ; art. 18, 4e Convention de Genève). Pourraient en effet constituer une attaque : une coupure du système électrique ; une infiltration ou une manipulation d'une base de données médicales, causant des transfusions sanguines erronées chez des civils et des soldats.

Est-il possible par ailleurs d'éviter les dommages aux infrastructures civiles (par un virus par exemple), voire les dommages au-delà des frontières de l'Etat visé ? Pour le comité international de la Croix-Rouge (CICR), l'utilisation de tels virus équivaut à une arme frappant sans discrimination. Cela vaut également si l'on s'en prend aux moyens de subsistance de la population civile (si perturbations d'installations de distribution d'eau potable, les systèmes d'irrigations,…), interdit par l'art. 54 du 1er Protocole additionnel aux Conventions de Genève (PA1).

Enfin, est-il possible en pratique d'anticiper les conséquences directes et indirectes qu'aurait ce type d'attaques sur les biens et personnes civils ? Si l'on se réfère à l'art. 57 du PA1, il convient de prendre toutes les précautions quant au choix des moyens et méthodes d'attaque en vue d'éviter, ou de réduire au minimum les pertes et dommages civils causés incidemment.

2.2 Problématique de la distinction civil/combattant.

La définition de la participation directe aux hostilités est particulièrement importante, et plus encore dans le domaine de la cyberguerre. En effet, l'importance de la distinction civil/combattant peut être d'autant plus importante que la participation à une cyberguerre peut avoir une durée extrêmement courte.

Les experts du CICR ont estimé que l'utilisation de moyens électroniques pouvait constituer une participation directe aux hostilités (Guide interprétatif sur la notion de participation directe aux hostilités, 2010). Mais que penser alors de la seule maintenance de systèmes informatiques militaires ? A priori elle ne serait pas considérée comme une participation directe aux hostilités, mais cette notion fait l'objet de nombreux débats.

Un dernier point mérite enfin d'être évoqué, celui de la perfidie, proscrite par le DIH. La perfidie est un acte destiné à tromper la bonne foi de l'adversaire

La raison du plus fort est toujours la meilleure

pour lui faire croire qu'il peut recevoir ou accorder une protection (utiliser une ambulance pour traverser les lignes ennemies ou transporter des armes, utiliser un drapeau blanc ou celui de la Croix Rouge pour attirer l'ennemi dans une embuscade…). Lorsque l'acte perfide entraîne la mort ou des atteintes graves à l'intégrité physique de l'adversaire, il constitue même un crime de guerre.

Se pose donc la question de savoir comment qualifier les manipulations de bases de données de ciblage de l'ennemi, ou les attaques « cyber » visant à faire croire que les véhicules de combat de l'ennemi sont des véhicules médicaux, ou encore l'utilisation du « morphing » pour détourner l'image du chef ennemi en lui faisant lire des déclarations erronées. Peut-on parler de perfidie ? Ou sommes-nous seulement en présence de ruses de guerre qui, contrairement à la perfidie, sont autorisées ? Les ruses de guerre visent à induire l'ennemi en erreur ou lui faire commettre des imprudences (camouflage, leurre, opération simulée, désinformation).

Toutes les questions abordées ici, qui sont évidemment transposables au monde de la robotisation, sont encore loin d'être tranchées. Il nous appartient de :

- suivre l'évolution de l'application pratique du Manuel de Tallin au sein de l'OTAN et également dans les corpus nationaux des nations contributrices ;
- surveiller certaines interprétations parfois restrictives (CICR) ou trop extensives (USA) ;
- nous positionner, en interne France, sur certains des points traités, afin de nous permettre de mieux promouvoir, ou critiquer le cas échéant, les positions émises dans les enceintes internationales. Il reste donc encore du chemin à parcourir… ■

Les opinions exprimées par l'auteur ne sauraient refléter la position officielle du ministère de la Défense.

Un spectre sous contrôle

L'Agence Nationale des Fréquences (ANFr) assure la planification, la gestion et le contrôle de l'utilisation du domaine public des fréquences radioélectriques et représente la France dans les instances internationales traitant de fréquences. Cet EPA, créé en 1997, rassemble plus de 300 collaborateurs.

Les fréquences hertziennes sont une ressource essentielle de la cyberéconomie et le maillon indispensable de tout système de sécurité. Impalpables, elles sont une ressource rare, et leur contrôle est stratégique.

DES ENJEUX CONSIDERABLES

Les fréquences, facteur de développement de l'économie et des services

Evident lorsque l'on parle des télécoms, de l'audiovisuel ou des transmissions par satellites, le recours aux moyens de communication hertziens devenu essentiel pour des secteurs comme le maritime, l'aéronautique, conditionne le développement de nombreux domaines, comme l'énergie, les transports terrestres, la santé, l'automobile, qui dépendent de l'accès au spectre. La révolution des usages engagée autour des objets connectés s'appuie sur la disponibilité des fréquences radios.

Les fréquences sont donc un formidable levier pour la création de valeur d'une société à l'ère numérique. Elle reste un maillon critique de nos systèmes de sécurité : à côté des multiples usages militaires, des moyens des forces de l'ordre, la place des liaisons radios dans la sécurité quotidienne du citoyen va croissant : situations d'urgence et prévention des catastrophes, notamment climatiques (radars météorologiques), contrôle et surveillance d'infrastructures : SNCF, EDF, autoroutes…

Les satellites (ici, Galileo) : presque la moitié des dossiers fréquences au niveau international.

Les fréquences satellitaires, la « nouvelle frontière »

Les systèmes satellitaires desservant de vastes zones géographiques, les ressources fréquentielles qu'ils utilisent sont principalement gérées au niveau international. Les Etats membres de l'Union internationale des télécommunications (UIT) ont convenu de mécanismes d'accès aux ressources orbitales et spectrales, part importante d'un traité appelé Règlement des Radiocommunications, mis en œuvre au niveau national par l'ANFr.

L'agence communique les demandes d'assignations de fréquences satellitaires à l'UIT pour le compte d'organisations intergouvernementales comme l'agence spatiale européenne ou le programme Galileo, d'opérateurs gouvernementaux français (Défense et CNES), et d'une dizaine d'opérateurs commerciaux.

Elle se charge également de la coordination internationale de ces assignations, et instruit pour le compte du ministre en charge des communications électroniques les demandes d'autorisation d'exploitation.

Un nouveau mécanisme prometteur ? Le *Licensed Shared Access* (LSA)

Alors que les opérateurs utilisent aujourd'hui leurs bandes de fréquences sur la base de l'exclusivité, ce nouveau concept technique et juridique vise à introduire, dans les autorisations individuelles pour de nouvelles bandes, des règles de partage permettant aux utilisateurs actuels de conserver leurs usages et leurs droits. Un partage dynamique est aussi à l'étude. On envisage de recourir au LSA pour la bande 2,3 GHz, avec l'accord de la Défense, alors que les usages actuels sont nombreux et sensibles : télémesures, liaisons vidéo et télécommandes de drones, données de vol …

UN MECANISME REGLE… SUR LA BONNE FREQUENCE

Au plan national, le Premier ministre se voit proposer par l'ANFr les actes réglementaires officialisant ces évolutions, une fois assurée la compatibilité avec les accords internationaux, le cadre européen, la loi française.

Les évolutions du spectre à l'échelle mondiale se forgent à Genève. Ce « grand marché » des fréquences est calé sur une périodicité de 4 ans environ, au rythme des conférences mondiales des radio-télécommunications, sous l'égide de l'UIT, agence spécialisée de l'ONU. Cet évènement très professionnel est suivi attentivement par des milliers de responsables publics, industriels, opérateurs du monde entier : il constitue un moment primordial pour finaliser les convergences nécessaires aux nouveaux services, et on y veille sur les marges de manœuvre et les intérêts économiques pour le futur. La négociation d'accords bilatéraux de coordination aux frontières, ou, quand il s'agit de radiocommunications spatiales, d'accords entre pays sur leurs réseaux satellitaires, complètent le dispositif.

par
Jean-Pierre Le Pesteur,
IGA

L'IGA Pesteur (X74 – ENSTA) est président du Conseil d'administration de l'ANFr depuis 2012. Après un début de carrière au GIAT (DGA), il a été sous-directeur au ministère de l'économie, des finances et de l'industrie de 1993 à 2006, chargé de différents secteurs de l'industrie et des services. Il a créé le pôle interministériel de prospective et d'anticipation des mutations économiques. De 2009 à 2012, il a été sous-directeur des politiques d'exportation de la direction du développement international, à la DGA.

Horlogerie suisse et poupées russes : entre Europe élargie et cadre communautaire

Si chaque Etat conserve sa souveraineté (un Etat, une voix) dans le monde des ondes, l'Union européenne a ajouté un étage communautaire à ces travaux : la Commission joue elle aussi son rôle en créant les conditions d'une harmonisation accélérée, en coopération avec les Etats membres, eux-mêmes réunis au sein d'un organisme plus large que l'UE, la CEPT (Conférence Européenne des administrations des Postes et Télécommunications) - entité de coordination entre les organismes des postes et de télécommunications des Etats européens (50 environ à ce jour). Le mécanisme d'harmonisation et de coopération est décrit par la décision « spectre ».

Usages professionnels : sécurité au quotidien.

MIGRATIONS ET PARTAGES : LA METAMORPHOSE DES FREQUENCES

L'histoire et la densité d'usages ont amené des services de nature très différentes à se côtoyer dans certaines parties du spectre. Les besoins évoluant, un travail tantôt de couturière, tantôt de géomètre va permettre de faire une place à de nouvelles applications, de ré-agencer telle partie du spectre. L'objectif permanent est d'aller vers un spectre mieux utilisé, mais ces évolutions prennent des années et la cible est mouvante.

Les gains d'échelle attendus peuvent être considérables : en témoigne la recherche effrénée de bandes de fréquences communes au niveau européen et mondial, pour la transmission de données mobiles à très haut débit (4G/LTE).

Tous les secteurs sont concernés : dans le champ de la sécurité citons l'accord récent défense - intérieur pour les drones des unités d'intervention de la gendarmerie et de la police nationale, en bande UHF, et l'accord défense - aviation civile pour l'insertion des drones militaires dans le trafic aérien général (télécommande et contrôle par satellite dans la bande 5 GHz).

Ces mouvements demandent des outils d'ingénierie financière : le Fonds de Réaménagement du Spectre (FRS), géré par l'ANFr, a ainsi permis le déploiement des réseaux de téléphonie mobile de 4e génération (bandes 790 – 862 MHz et 2 500 – 2 690 MHz), avec la migration d'une dizaine de liaisons hertziennes de la défense, et du réseau gouvernemental RUBIS géré par la gendarmerie nationale, ainsi que le déplacement des fréquences du système intégré de l'Armée de terre FELIN.

Focus sur les brouillages intentionnels

Entre 2009 et 2012, l'ANFr a déployé ses efforts pour faire cesser des brouillages intentionnels en très forte augmentation (1 975 minutes cumulées en 2010, 329 826 minutes en 2012…) dont étaient victimes des satellites commerciaux exploités par la société Eutelsat SA.

Spot de la BBC qui dit tout sur les brouillages dans certaines zones du monde.

Les brouillages délibérés constituent un type particulier de brouillages, avec des caractéristiques très différentes de celles des brouillages non intentionnels : la porteuse « brouilleuse » vise expressément le satellite affecté (de manière à éviter des brouillages préjudiciables à d'autres satellites adjacents), et même certains répéteurs déterminés, n'est modulée par aucun signal d'information, ses paramètres d'émission étant modifiés en temps réel, afin de mettre en échec les techniques d'atténuation des brouillages.

Les moyens de géolocalisation disponibles permettent de déterminer la zone d'où provient le brouillage. Au cours de la période 2010 - 2012, 98,5 % des cas de brouillages délibérés provenaient ainsi du territoire de deux administrations du Moyen-Orient… Fruit des efforts diplomatiques et techniques : il semble que la situation se soit considérablement améliorée depuis mi-2013 (Spot de la BBC sur les brouillages dans certaines zones du monde : http://www.bbgstrategy.com/2012/11/bbc-motion-graphic-satellite-jamming-explained/

Quelle offre industrielle pour assurer la résilience et la souveraineté de la France et de l'Europe

La réalité de l'offre industrielle européenne en matière de cybersécurité est encore extrêmement fragmentée : entre le très haut niveau de sécurité qui reste national avec des volumes très faibles et une déferlante d'offres américaines, l'industrie européenne peine à se consolider pour construire une offre de confiance apte à assurer notre résilience économique et notre indépendance.

par **Hervé Guillou,** IGA

Corporate Executive, Conseiller Défense et Sécurité d'AIRBUS Group
Président du CIS (Conseil des Industries de Confiance et de Sécurité)

Il débute sa carrière en 1978 à la Direction des Constructions Navales de Cherbourg (DCN), puis comme responsable du projet de propulsion nucléaire des Sous-marins Nucléaires Lanceurs d'Engins (SNLE) de nouvelle génération et responsable de la section Nucléaire de DCN Indret (Nantes). De 1989 à 1993, il est Conseiller puis Directeur de cabinet du Délégué Général pour l'Armement Yves Sillard. De 1993 à 1996, il est Directeur du programme international tripartite (UK, Italie, France) de frégates antiaériennes HORIZON et Chef du Joint Project Office à Londres. En 1996, il devient Directeur général délégué de l'entreprise d'ingénierie nucléaire Technicatome, et Président de Principia et de Technoplus Industries. En 2003, il rejoint le groupe EADS comme CEO d'EADS Space Transportation. En 2005, il rejoint EADS/Cassidian en tant que CEO de la business unit Defence and Communications Systems. Enfin, en 2011, il crée Cassidian Cyber Security dont il devient CEO.

La domination de l'industrie nord-américaine n'est pas une fatalité. Il est encore temps de développer une offre de confiance en Europe.

Merci Mr Snowden ! En quelques mois le sujet de la cybersécurité longtemps considéré avec un sourire narquois comme une fantaisie de quelques paranoïaques est au sommet de l'actualité. Mais derrière cette déferlante d'articles sur l'explosion de la menace, qu'elle soit gouvernementale, mafieuse ou terroriste, il convient, plutôt que de se lamenter sur notre sort, de réfléchir et d'agir rapidement pour consolider nos défenses.

Il n'appartient pas à l'industrie de s'exprimer sur les politiques publiques en la matière, mais je ne peux que me réjouir de voir les principaux Etats européens : la Grande-Bretagne, l'Allemagne, la France, mais aussi la Commission européenne prendre le problème à bras le corps. Le vote récent en France d'articles spécifiques dans la LPM, les déclarations du Ministre de la défense, et l'installation de la Filière sécurité par le Premier ministre en octobre 2013 montrent que la prise de conscience est réelle et que les lignes bougent dans le bon sens.

Coté industriel, il convient aussi de faire bouger les lignes sans attendre d'être dans une situation de dépendance totale de l'offre américaine dominant le marché international. Nous sommes en effet face à la nécessité de combler deux faiblesses de notre offre :

- adapter nos solutions aux besoins du monde économique et des services publics (organismes d'importance vitale principalement), au-delà du monde très réservé et restreint de la protection du cœur de nos équipements de défense ;
- créer un socle industriel, pérenne, apte à constituer une base technologique et industrielle de cybersécurité, souveraine et ayant la confiance de nos Etats et de nos citoyens.

Les industriels français doivent développer et compléter leur offre technique et les services associés

D'un point de vue technique, je vois au moins trois priorités :

- développer la capacité de surveillance, d'analyse et de réaction en temps réel : il faut se souvenir en effet que, dans notre domaine, la « Ligne Maginot » est tournée depuis longtemps. Le développement des attaques sophistiquées (APT : *Advanced Persistant Threat*) se poursuit et le temps médian de détection est de l'ordre de 400 jours : que de dégâts entre temps ! Descendre à 40 jours, et pourquoi pas à 4 jours ou 4 heures est très certainement le moyen le plus efficace de limiter les dommages ;
- anticiper l'explosion du nombre de points d'accès dans les systèmes d'information, dus aux terminaux mobiles, mais aussi au développement de l'Internet des objets : 500 millions d'adresses IP en 2003, 15 milliards aujourd'hui, 80 milliards entre 2020 et 2025. C'est demain !

Cette évolution est irréversible car elle résulte de la connexion progressive - via le standard IP – de trois mondes jusqu'ici isolés (pour les nostalgiques, relire l'instruction 1514 !) : l'informatique générale, l'informatique industrielle et l'informatique embarquée. Ceci suppose notamment de développer d'urgence des solutions de confiance pour les SCADA (*Supervisory Control And Data Acquisition*), de renforcer considérablement les méthodes et les outils de chiffrement en ligne, d'authentification des hommes comme des objets, de signature et de traçabilité des échanges.

- développer des réponses à la dématérialisation des infrastructures fixes et mobiles : la notion même de « *cloud* » est à l'évidence totalement orthogonale à la notion de sécurité ou de souveraineté, mais on parle aussi de routeurs ou d'opérateurs virtuels pour nos télécommunications.

Bref, de quoi occuper durablement nos ingénieurs – encore trop peu nombreux – qui s'investissent dans le domaine de la cybersécurité, et que de sujets passionnants pour nos entrepreneurs petits et grands.

COFIS (Comité de la filière industrielle de sécurité)

Des technologies qui évoluent avec une constante de temps inusitée dans le monde des programmes d'armement

Un mot enfin sur cette offre, s'adressant à un lectorat d'Ingénieurs de l'Armement, il ne s'agit pas de construire des programmes sur trente ans ! Nous sommes dans un monde où la menace évolue tous les jours, où les technologies durent au mieux trois ans ! Le cycle de développement et de déploiement des produits et solutions doit plutôt se situer dans la fourchette trois mois à trois ans. Encore un beau challenge pour adopter nos méthodes de R&D de qualification et de mise en service.

Enfin, il ne faut pas oublier que cette offre va s'adresser à une clientèle peu avertie, parfois contrainte de mauvais gré à investir dans sa sécurité, et que l'offre de service sera cruciale pour créer la confiance, depuis l'éveil des consciences des comités exécutifs jusqu'à l'accompagnement par des services opérés dûment reconnus par nos autorités nationales.

Une nécessaire consolidation des PME disposant d'une offre de confiance techniquement certifiée

Le deuxième défi industriel est la consolidation de ce secteur, tant en France que dans les principaux pays européens. A ce jour l'industrie européenne est en effet très fragmentée :

- les grands acteurs de la Défense sont positionnés essentiellement sur des sujets de haut niveau de sécurité, donc plutôt cloisonnés dans des marchés nationaux faibles en volume (50 à 100 M€ par pays/an dans le « high grade », et peinent à élargir leur offre à l'économie générale, à la fois faute de soutien public, et parce que ce ne sont pas leurs clients traditionnels ;
- le marché « hors défense » est complètement submergé par une offre d'origine américaine, promue par une industrie déjà largement consolidée dans des groupes de Défense, ou purement civils de plusieurs milliards de chiffre d'affaires, et soutenue sur son territoire, comme à l'export, par des investissements massifs des agences fédérales : DHS, NSA, DRA… ;
- en Europe, aucun acteur de taille significative n'est visible en dehors des sociétés de Défense, ou des filiales des sociétés américaines.

Ceci ne veut pas dire qu'il n'y a rien, mais plutôt que le paysage industriel est constitué de plusieurs centaines de PME disposant souvent de technologies avancées mais qui peinent à franchir le « plafond de verre » des 5 à 10 M€ de chiffre d'affaire. Souvent sous-capitalisées et ayant du mal à financer leur R&D, peinant à atteindre les bons niveaux de décision chez des donneurs d'ordre 1 000 fois plus gros qu'eux, toujours avec des offres trop étroites pour rassurer les clients qui souhaitent des solutions plus globales et pérennes.

Ces difficultés de croissance des PME pour en faire des ETI ne sont pas spécifiques au domaine de la cybersécurité, mais prennent toute leur importance et leur urgence quand il s'agit de résister à la déferlante transatlantique que l'on connaît.

La France aura du mal à développer seule un écosystème disposant d'une BTIC (Base Technologique et Industrielle de Cybersécurité…) pérenne. Des alliances ciblées avec quelques partenaires européens de confiance doivent être négociées

Dans quel sens aborder cette consolidation de l'offre ? D'abord par pays, ensuite entre pays de confiance, d'abord par métiers puis par pays, je ne sais pas quel est le bon ordre, mais une chose est sûre : c'est urgent !

La Grande-Bretagne s'organise, l'Allemagne se met en route, l'Union européenne prépare des directives spécifiques. L'industrie doit s'y préparer et se montrer proactive, tant vis-à-vis des Gouvernements que des investisseurs, pour faire des propositions.

L'écoute est réelle, le besoin est là, c'est le bon moment…

Le Comité de la filière industrielle de sécurité (CoFIS)

L'Etat et les industriels français organisés de la filière s'engagent dans une politique industrielle concertée

Après la création en septembre dernier du Conseil des industries de confiance et de sécurité (CICS - 10 milliards d'euros de chiffre d'affaire, 50 000 emplois) par les groupements des industries françaises des constructions et activités navales (GICAN), de défense terrestre (GICAT), aéronautiques et spatiales (GIFAS) et la fédération des industries électriques électroniques et de la communication (FIEEC), le 23 octobre 2013 a marqué une nouvelle étape importante dans l'organisation et la visibilité de l'industrie française de la sécurité. En effet, à l'hôtel Matignon, le Premier ministre Jean-Marc Ayrault, conjointement avec Hervé Guillou, président du CICS, Alain Juillet, président du club des directeurs de sécurité des entreprises, Yves Rome, président de la conférence nationale des services d'incendie et de secours (CNSIS), Nicolas Dufourcq, directeur général de la banque publique d'investissement, Jean-Luc Logel, président du cluster EDEN, Jean-Luc Beylat, président du pôle Systematic, Joël Chenet, président du pôle Risque, Jean-Marie Poimboeuf, président du GICAN, Christian Mons, président du GICAT, Marwan Lahoud, président du GIFAS et Gilles Schnepp, président de la FIEEC, signait la charte de création du CoFIS lors d'une réunion rassemblant les signataires et de nombreux ministres.

Une institution visible

Le comité institué comprend le Premier ministre qui le préside, onze ministres, le commissaire général aux investissements, le directeur général de la banque publique d'investissement, le secrétaire général de la défense et de la sécurité nationale (SGDSN), le directeur général de la compétitivité, de l'industrie et des services (DGCIS), le délégué interministériel à l'intelligence économique (D2IE), le délégué interministériel à la sécurité privée (DISP), et les membres de trois collèges renouvelés tous les trois ans, le collège des opérateurs et utilisateurs non-étatiques, composé de dix membres, le collège des industriels, de quinze membres (dix représentants d'entreprises adhérentes au CICS, dont au moins quatre représentants de PME, et des représentants des pôles de compétitivité et de clusters régionaux d'industriels) et le collège des personnalités qualifiées, de dix membres. Il se réunit deux fois par an et établit les grandes orientations de la filière.

La préparation et le suivi des réunions du comité est assurée par un groupe de pilotage co-présidé par un représentant du SGDSN et un représentant de la DGCIS, composé, en outre, de deux vice-présidents choisis parmi le collège des industriels et le collège des personnalités qualifiées, de cinq représentants de cinq ministères (Intérieur, Écologie, développement durable et énergie, Défense, Enseignement supérieur et recherche, Commerce extérieur), des présidents et vice-présidents de sous-groupes de travail également institués, issus des trois collèges.

Les sous-groupes de travail, au nombre de cinq, sont :

- ***en format public - privé :***
- un sous-groupe « expression des besoins », présidé par un opérateur ou un utilisateur non étatique ;
- un sous-groupe « stratégie export, normes et intelligence économique », présidé par un membre du collège des industriels ;
- un sous-groupe « recherche et innovation », présidé par un représentant du monde de la recherche ;
- ***en format étatique :***
- un sous-groupe des prescripteurs de la sécurité, présidé par le SGDSN ;
- un sous-groupe « financeurs de la recherche et de l'innovation », présidé par la DGCIS.

Le SGDSN et la DGCIS animent le groupe de pilotage et les sous-groupes, sans qu'il soit nécessaire d'affecter un personnel permanent au comité.

Un démarrage rapide

Le CoFIS dispose d'une feuille de route selon sept axes :

1. identifier les forces et faiblesses du marché français de la sécurité ;
2. identifier les technologies critiques et stratégiques à préserver ou à développer ;
3. élaborer un premier recensement des besoins prioritaires de l'État et des opérateurs ;
4. soutenir le lancement de projets de démonstrateurs structurants pour la filière ;
5. soutenir les entreprises françaises à l'export, en favorisant l'émergence d'un club France ;
6. utiliser le levier européen, en proposant une stratégie nationale publique – privée ;
7. mettre en réseau les acteurs.

Les membres des collèges ont rapidement été nommés. Un mois après la signature de la charte, à Villepinte, à l'occasion du salon Milipol, fin novembre, le groupe de pilotage a dévoilé les priorités technologiques du CoFIS et un programme de démonstrateurs :

- les communications sécurisées à haut débit pour les forces de l'ordre ;
- la sécurité du transport aérien ;
- la vidéoprotection ;
- le bâtiment sécurisé ;
- les équipements de protection individuelle des forces de l'ordre ;
- la protection des approches portuaires et des lignes TGV ;
- ainsi que la sûreté des aéroports.

Par Olivier de Vulpillières, ICA, CGArm

Cyberprotection : enjeux et perspectives

Anticiper et détecter… avant d'agir avec discernement

Les meilleurs alliés réservent parfois des surprises. Pas pour les « initiés ». Des évènements importants impliquant la surveillance des flux d'informations et dont toutes les suites ne sont pas encore révélées, invitent à revisiter clairement le périmètre exact des « amers de confiance » dans le domaine de la cybersécurité. Dans un monde où une saine paranoïa mérite d'être plus largement partagée, de nouvelles solutions sont à développer, des coopérations doivent être renforcées, car l'anticipation et la maîtrise des effets des attaques ne sont pas les moindres des enjeux de demain.

L'histoire sans fin, mais de nouvelles cibles

D'un point de vue des objectifs de la menace « classique », matérialisée sous formes d'atteinte à la disponibilité, l'intégrité ou la confidentialité pesant sur les technologies de l'information, les intrusions sur des grands systèmes continuent, depuis celles visant les grands industriels qualifiés d'Opérateur d'Importance Vitale (OIV), jusqu'à ceux déployés au plus haut niveau de l'Etat. Mais cette menace se professionnalise, les attaques sophistiquées s'ajoutent aux menaces classiques et, surtout, de nouveaux périmètres techniques sont visés : les automates industriels, souvent dénommés SCADA[1]. Tout concourt donc à devoir pallier cette montée en puissance et surtout cette extension de la menace pour réinstaurer la confiance dans ce qu'il convient de qualifier de domaines critiques pour la souveraineté, aux plans militaire et économique.


Cybels_Intelligence-©Bernard ROUSSEAU

par **Philippe Leroy,**
Colonel (er) de l'Armée de l'air

Directeur en charge du développement des offres cybersécurité, chez Thales Communications & Security France qu'il a rejoint en 2006, Philippe Leroy ancien coordinateur SSI de l'Armée de l'air, a mis en place l'entité SSI lors de la création de la DIRISI, puis occupé le poste de Fonctionnaire SSI du ministère.

Mais ajoutée à cette menace symétrique entre grands alliés, la dépendance avec l'informatique donne un nouveau champ d'action à la menace asymétrique depuis 2010, puisque désormais les exploits ciblent les éditeurs d'automates industriels et autres chaînes communicantes, sans que ceux-ci aient pu anticiper pour des systèmes conçus pour fonctionner H24/7 et durer souvent une trentaine d'années. Or à ce jour, des milliers de systèmes de contrôle industriel (ICS) sont accessibles via Internet …

Anticiper et détecter : l'union et la capitalisation font la force

Le combat entre l'attaquant et le défenseur n'a pas changé d'âme, mais les nouveaux périmètres et surtout les nouveaux acteurs concernés n'y sont pas préparés. Beaucoup s'interrogent désormais sur la vulnérabilité de leur système, pourtant selon eux non connecté. Les air-gap n'ont pas évité Stuxnet, les actions de télémaintenance sont offertes en ligne par des opérateurs : est-ce encore le règne de la confiance aveugle ?

En effet, l'air-gap, c'est-à-dire la protection par l'isolement est un concept de défense illusoire, car aucun système de traitement de l'information ne peut prétendre être durablement isolé du monde extérieur. Survient toujours un moment où il faut actualiser des paramètres, mettre à jour un logiciel, échanger des informations, changer des mots de passe, admettre de nouveaux opérateurs ou encore répondre aux attentes d'une intégration toujours plus poussée entre les différents niveaux d'une structure et les ERP (*Enterprise Resource Planning*) aux fins d'améliorer la productivité et l'efficacité.

Les organisations ont remplacé les réseaux traditionnels par les réseaux d'échanges « en mode séquentiel » mais très peu contrôlés, via les CD Rom, les clés USB, les Smartphones. Pourtant on sait par expérience qu'un système fondé sur la seule confiance des personnes est tôt ou tard voué à être pris en défaut par la négligence ou par la corruption. Cependant des solutions fiables à la sécurité prouvée apparaissent, qui permettraient de revisiter les interconnexions maîtrisées entre les réseaux de niveaux de sensibilité différents. Les postes multiniveaux et les passerelles interdomaines, basés sur des systèmes d'exploitation contrôlés qui permettent respectivement de cloisonner les rôles et espaces sur une même machine de confiance (qualifiée EAL4+ au titre des critères communs) et l'échange de flux bidirectionnels maîtrisés entre domaines de sensibilité ou de confiance distincts méritent un développement de sujet à part entière.

Plus globalement, pour pallier le seul problème de l'air-gap et des échanges maîtrisés intersystèmes, la stratégie « cyber » doit satisfaire trois préoccupations : l'attente des différents métiers en tenant compte de leurs contraintes spécifiques, le complément des solutions actuelles, notamment pour les nouvelles technologies (*Cloud computing*, mobilité et BYOD), la nécessité d'associer de manière croisée les expériences des offreurs de solutions de cybersécurité avec les fournisseurs de solutions industrielles, notamment au profit des fonctions critiques des OIV.

La première vise à développer des solutions de confiance, tant en termes de produits que de services adaptés aux contextes des OIV, récemment ciblés par les intrusions et autre dénis de service, mais également pour durcir contre la cybermenace les systèmes d'armes de la défense, à laquelle contribue les PEA récents et en cours pour des milieux métiers.

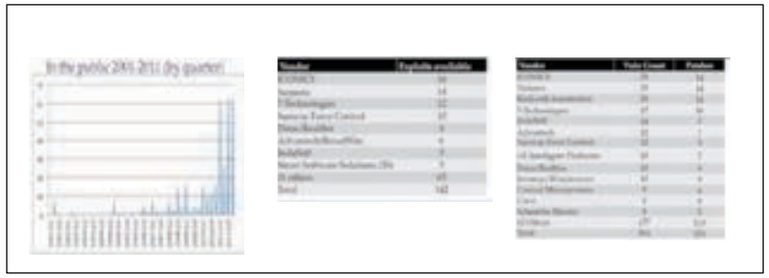
La deuxième permet de compléter les offres actuelles en poursuivant les efforts dans la sécurisation des grands écosystèmes, tels que les Cloud souverains (i.e. *Cloudwatt* et *Numergy*), car le phénomène du Cloud computing invite à resserrer les mailles de la surveillance et à formaliser les processus de confiance ; ou encore en complétant l'offre de cyberdéfense par l'adjonction de moyens de datamining, destinés à anticiper les attaques par recherche de mots clés sur les réseaux sociaux et ouverts, et d'autre part d'entraînement sur une plate-forme « *red/blue team* » qui complètent le socle de cyberdéfense CYBELS avec l'apport de la R&D du groupe et de PME innovantes.

La troisième vise à renforcer le niveau de résilience des automates et logiciels de supervision industriels face aux cybermenaces, en commençant par effectuer un constat des principales vulnérabilités selon leurs contextes de déploiement, et ainsi diminuer le niveau d'exposition au risque. L'accord de partenariat en cybersécurité récemment signé ente Thales et Schneider Electric France s'inscrit dans ce cadre.

Malgré tout, l'intrusion peut survenir à tout moment et depuis 2011, à l'instar du Groupe d'intervention rapide du ministère, Thales a mis en place une force d'intervention rapide, composée d'un panel d'experts hautement qualifiés en mesure de se porter au secours des grandes entreprises victimes d'intrusions, de proposer en mode « gestion de crise » aux côtés de la direction, un plan de remédiation préservant les priorités des métiers destiné à se réapproprier les ressources compromises du SI.

Conclusion

Fort du constat de besoin croissant de maîtrise des systèmes nationaux, le Livre blanc de 2013 insiste sur l'importance de la « cybermenace », qui constitue « une menace majeure, à forte probabilité et à fort impact potentiel », et annonce que la cyberdéfense « fera l'objet d'un effort marqué, en relation étroite avec le domaine du renseignement ». L'ANSSI va prochainement pouvoir inscrire son action nationale de cybersécurité grâce à une nouvelle loi qui va imposer le recours à des produits de confiance et surtout à de nouvelles solutions. Elle aura le mandat d'en vérifier la réalité via des campagnes d'audit, pour s'assurer de l'application effective des principes fondamentaux de la cyberdéfense, lorsque la cyberprotection est supposée acquise et que l'intrus est dans la place.



Gérer l'existant

- Cartographier et qualifier les infrastructures SCADA Métier et les priorités
- Détecter les vulnérabilités
- Réaliser des tests d'intrusion interne/externe
- Analyser les risques
- Corriger l'urgent
- Entraîner conjointement les acteurs « cyber » et métier

Préparer l'avenir :

- Optimiser la cyber-résilience des systèmes (normes et standards)
- Concevoir des infrastructures critiques résilientes par construction (technos distinctes) et y compris sous attaque
- Evaluer les composants COTS et qualifier la résistance aux intrusions et à la rétro-conception

Détecter Ralentir et Intervenir

La DGA contribue largement à cet effort national, par une montée en puissance sans précédent de ses effectifs, budgets et appui aux programmes.

Thales s'inscrit pleinement dans cette mouvance et adapte aux besoins ses capacités de développement et de production industrielle, d'intégration et de maintien en conditions de sécurité, d'opérateur de cybersécurité le tout dans un cadre totalement maîtrisé.

(1) Supervisory Control and Data Acquisition

La cyberdéfense des entreprises : comment faire face ?

Pour une approche systémique de la cybersécurité

La croissance exponentielle des attaques informatiques rend de nombreuses entreprises et services publics victimes de vols massifs d'informations, d'attaques sur leur image, de perturbations voire de sabotages. Une approche systémique de la cybersécurité les aide à conserver un coup d'avance.

Révolue l'époque des « gentils hackers » ! La cyberattaque est désormais une industrie très innovante et rentable, composée de dizaines de milliers de chercheurs, développeurs, fournisseurs, prestataires, courtiers et places de marché dans le monde qui collaborent afin de perturber, espionner, détourner, voire saboter. Les hackers s'attaquent à des cibles qui pouvaient s'estimer bien protégées (banques, sociétés de sécurité informatique, autorités de certification numérique, systèmes gouvernementaux ou classifiés …) et prennent le contrôle de systèmes d'information

De nombreuses entreprises ont vu leur dispositif de sécurité contourné

d'entreprises pendant des mois ou des années. Les médias s'en font souvent l'écho (Bercy, Sony, RSA, la Commission européenne, Aramco, de grands journaux américains…). Les écoutes et intrusions informatiques à grande échelle de la *National Security Agency* sont désormais dévoilées et la Chine n'est pas en reste avec de vastes opérations d'agression informatique révélées dans les medias ces dernières années.

Cependant, la plupart de ces attaques restent secrètes, non détectées même, et forment la partie immergée d'un immense iceberg qui fait des dégâts considérables, bien que silencieux. Ceux-ci portent atteinte aux informations sensibles placées au cœur des systèmes d'information ainsi qu'au bon fonctionnement des processus informatisés qui animent le fonctionnement de la société. Ce sont des téraoctets de savoir-faire français, des années d'investissement industriel ou scientifique, qui s'évaporent, sapant les avantages technologiques et concurrentiels de nos économies.

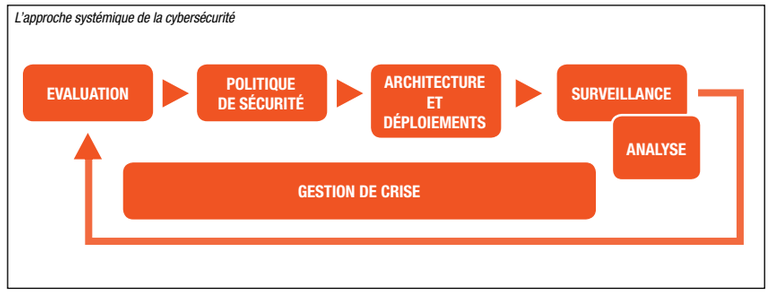
L'ère des cyberattaques ne fait que commencer

La situation tend à s'aggraver encore : les réseaux sociaux perçus comme de confiance, la connexion aux réseaux d'entreprises d'appareils mobiles en tous genres, le Cloud computing, l'interconnexion des systèmes industriels et les échanges de machine à machine créent chaque jour de nouvelles failles informatiques qui font le bonheur des pirates. 50 milliards d'objets, pour la plupart non protégés, pourraient disposer en 2020 d'une adresse IP ! Et de plus en plus d'organisations criminelles et d'Etats investissent ce domaine, porteur de puissance et de revenus faciles.

Les entreprises doivent faire face

Comment les entreprises peuvent-elles éviter de perdre le contrôle de leurs systèmes d'information, et par suite des informations et des processus qui leur sont essentiels ? La sécurité informatique la plus traditionnelle, organisée pour défendre un périmètre à l'intérieur duquel les systèmes d'information sont considérés comme de confiance, est dépassée par l'ouverture des réseaux et l'aggravation des attaques. Une démarche systémique[1] s'impose, intégrant de manière organisée et cohérente toutes les démarches qui contribuent à la cybersécurité.

L'approche systémique de la cybersécurité



La sécurité d'un système est celle de son maillon faible

Ainsi, bien avant de choisir telle ou telle solution technique, l'entreprise doit faire progresser sa sécurité sur les plans organisationnel, juridique et technique. S'appuyant souvent sur un prestataire spécialisé indépendant des fournisseurs de solution, elle doit piloter sa sécurité numérique, édicter des règles à l'attention de ses fournisseurs et salariés, sécuriser son informatique industrielle comme son informatique de gestion, ses produits, projets et applications comme ses infrastructures informatiques, et éventuellement s'assurer pour couvrir les risques résiduels, une fois que la démarche systémique les a placés sous contrôle. Et surtout, ces actions doivent être cohérentes entre elles car le pirate trouvera le maillon faible !

La démarche systémique de cybersécurité *(cf. figure)* s'inscrit dans une approche par les risques, qui permet d'accroître sur tous les fronts, de manière cohérente, la cybersécurité de l'entreprise. Elle résulte d'une approche de progrès bouclée comprenant, outre une bonne « hygiène informatique »[2] dans le comportement de chacun :

- une évaluation de la sécurité réelle de l'entreprise, menée à l'aide d'audits organisationnels et techniques et de tests d'intrusion, permettant d'identifier les faiblesses, d'évaluer le niveau de maturité de la sécurité de l'entreprise et de définir des plans d'amélioration ;
- une analyse de risques sérieuse, une politique de sécurité, une gouvernance appropriée, des contrats adaptés, une organisation solide et des collaborateurs sensibilisés ou formés ;
- une architecture informatique robuste et le déploiement d'outils de sécurité adaptés, correctement administrés et opérés ;
- une surveillance permanente du système d'information assurant le maintien en condition de sécurité et permettant de détecter au plus vite les incidents ;
- une analyse détaillée des événements intervenant dans le système afin de réagir rapidement en cas d'attaque ;
- une capacité de gestion de crise organisée et éprouvée permettant de réduire l'impact des agressions et de minimiser les dommages pour l'entreprise.

80 % des attaques informatiques sont bloquées par une hygiène informatique sérieuse et de bonnes mesures de sécurité préventives. 19 % des attaques sont parées à l'aide de dispositifs proactifs de surveillance et de détection des agressions. Quant au 1 % des attaques restantes, les plus sophistiquées, il est impossible de s'en prémunir à coup sûr, mais l'entreprise peut considérablement limiter leur impact si elle s'est dotée d'une sécurité en profondeur et s'est bien préparée à gérer la crise.

La conscience des acteurs économique mûrit

De plus en plus d'acteurs économiques prennent conscience de l'importance de sécuriser leur activité et leurs informations. Certains, les banques par exemple, en sont convaincus de longue date et s'adaptent à une menace dont la sophistication augmente chaque semaine. Beaucoup d'autres, dont de nombreuses PME, qui s'étaient jusqu'à présent contentés de mesures de sécurité élémentaires (anti-virus, firewall), améliorent résolument leur posture de cybersécurité. L'efficacité de ces actions se vérifie par des audits et des tests d'intrusion assurés par des tiers.

Ces évolutions entraînent la montée en puissance rapide d'une industrie du service en cybersécurité, dont le marché (hors solutions logicielles et matérielles) représente 3 Md€ en 2012 en France[3] et croît de 10 % par an au sein d'une économie pourtant atone. En effet, la plupart des entreprises et des services publics ne disposent pas de la ressource spécialisée leur permettant d'assurer pleinement leur cyber-protection, qui n'est pas leur cœur de métier, et sollicitent donc des prestataires spécialisés tels que Sogeti.

Nous n'en sommes qu'au début de l'histoire de l'industrie de la cybersécurité

Aujourd'hui souvent isolés, les prestataires collaboreront demain entre eux et avec la puissance publique pour mettre en commun les traces d'attaques opérationnelles et réagir au plus vite aux nouvelles méthodes d'agression. En effet, les agresseurs ont toujours l'avantage de la surprise et de l'imagination face aux défenseurs, et ceux-ci ne peuvent s'en sortir qu'en mettant en commun leurs capacités de détection, en leur opposant une communauté de la cybersécurité partageant son intelligence et ses renseignements.

Des entreprises payent le prix fort pour avoir ignoré les dangers du cyberespace dans lequel évoluent leurs opérations. Certaines n'y ont pas survécu : Diginotar, entreprise néerlandaise spécialisée dans les certificats de sécurité, a par exemple fait faillite après la découverte d'une intrusion informatique de grande ampleur. Face à l'ampleur prise par la menace informatique, les administrations et les entreprises ont intérêt à s'investir de manière très organisée dans la cybersécurité. Une approche systémique qui nécessite quelques efforts et ressources, mais permet de maîtriser les risques business d'aujourd'hui et de se prémunir d'événements bien plus graves et coûteux.

par **Yves Le Floch,**

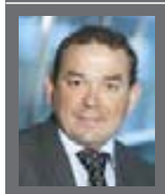
IGA
Directeur du développement de la cybersécurité du groupe Sogeti

Précédemment conseiller du secrétaire général de la défense et de la sécurité nationale chez le Premier ministre, il a contribué au renforcement des capacités nationales de cybersécurité et de cyberdéfense. Auparavant, il a exercé des fonctions managériales et techniques variées à la DGA et dans d'autres administrations d'Etat.

(1) Voir le Livre blanc de Sogeti sur l'approche systémique de la cybersécurité : www.fr.sogeti.com/sites/default/files/Documents/Publications/Une%20approche%20syst%C3%A9mique%20de%20la%20cybers%C3%A9curit%C3%A9.pdf
(2) Voir le guide d'hygiène informatique de l'ANSSI : www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
(3) Voir l'étude 2012 de l'observatoire de la confiance numérique : http://www.confiance-numerique.fr/download00010002.aspx?f=./iso_album/observatoire_confiance_numerique_acn_2012.pdf

Le « Centre de Cyber-défense » de Airbus Defence and Space

Ou comment traquer les signaux faibles pour débusquer et contenir les cyber-attaques avancées



par **Patrick Radja,**
Directeur du département «Cyber Defence & Engineering» à Airbus Defence and Space

Patrick Radja est en charge du développement des solutions de cyber défense et des services associés afin de lutter contre les cyber attaques. Il est également directeur de l'ingénierie et des opérations en France. Il est diplômé de l'Ecole Nationale d'Ingénieurs de Brest (ENIB) et titulaire d'un master en électronique.

par **Emmanuel Bresson,**
ICA

Emmanuel Bresson, Ingénieur en Chef de l'Armement, est en charge des offres à l'International à Airbus Defence and Space, après avoir été pendant 3 ans affecté à la région Moyen-Orient (2010-2013). Auparavant il a travaillé comme expert en cryptographie à l'ANSSI (Services du Premier Ministre) et au CELAR (aujourd'hui DGA/MI). Il est titulaire d'un Doctorat en Informatique et diplômé de l'École polytechnique (X95).

Le principal obstacle, aujourd'hui, à la défense contre les attaques informatiques, est la difficulé à détecter les premiers signes de présence des attaquants pour éviter qu'ils ne s'infiltrent jusqu'au cœur de vos systèmes d'information et pour réagir au plus vite. Pour cela, Airbus Defence and Space a développé les « Centres de Cyber-défense » (CDC) qui répondent à cette problématique en faisant communiquer en temps réel des services de veille, de surveillance des réseaux et des équipes de réaction et d'investigation. Cette approche répond à la préoccupation majeure des gouvernements, des infrastructures critiques et des industries stratégiques: éradiquer au plus tôt la menace. Ou : comment traquer les signaux faibles pour débusquer et contenir les cyber-attaques avancées ?

Êtes-vous sûrs d'être bien protégés ?

Une politique de sécurité traditionnelle intègre plusieurs briques technologiques telles que des anti-virus sur les postes de travail, des sondes de détection d'intrusion, des pare-feux, etc. Ces mesures sont nécessaires pour contrer la majeure partie des attaques, mais sont-elles suffisantes ? Alors que la sophistication des attaques augmente quotidiennement, êtes-vous sûrs de toutes les détecter ?

Les produits de sécurité, par exemple, intègrent à leur installation des règles basiques de détection d'intrusion. Si elles ne sont pas mises à jour régulièrement, elles deviennent obsolètes et inopérantes face aux nouvelles attaques. Et cela constitue la première difficulté : qui sait vraiment mettre à jour ces équipements pour faire face aux dernières techniques des attaquants ?

La deuxième difficulté tient à la détection : les infrastructures habituelles de supervision de sécurité appelées SOC (pour Security Operations Centre) supervisent uniquement des équipements de sécurité et se limitent souvent à envoyer de simples alertes, sans analyse d'impact et sans plan de remédiation. De plus, l'obsolescence des règles de détection, citée plus haut, rend les alertes du SOC de moins en moins pertinentes. En conséquence, les nouvelles attaques ne sont tout simplement pas détectées et c'est souvent le début d'un cercle vicieux.

Enfin, la troisième difficulté pour se protéger est de coupler la détection à une analyse. Cette dernière est trop souvent absente de la stratégie de sécurité : alerter, c'est bien, mais l'objectif est, in fine, de prendre la bonne décision de réaction ! Pour cela, il faut connaître le contexte opérationnel, le métier du client, sa stratégie, etc. Ce n'est pas forcément en coupant l'accès à Internet que l'on résout les problèmes !

La réponse à la problématique : une cyber-défense active

371 jours est le délai moyen constaté par les experts de Airbus Defence and Space entre le début d'une cyber-attaque avancée et la détection de celle-ci. Dans la lutte quotidienne contre les attaques les plus pernicieuses, le temps est l'ennemi n°1.

Pour cela, le Centre de Cyber-défense – CDC fait communiquer en temps réel les différents services indispensables à la lutte contre les cyber-attaques :

- le service de veille qui analyse le flux continu des nouvelles menaces et des nouvelles vulnérabilités,
- la supervision qui reçoit du service de veille tous les outils nécessaires à la détection des nouvelles attaques dès qu'elles sont identifiées,
- les capacités d'investigation pour qualifier les alertes, analyser leur impact potentiel et proposer les réactions adéquates.

Le CDC répond à ces enjeux de cyber-défense grâce à des équipes d'experts, des outils développés spécifiquement pour traquer les cyber-menaces et à une organisation intégrée. Ce triptyque est la clef de voûte d'une cyber-défense efficace.

Les principes fondamentaux du CDC sont :

- la connaissance et l'anticipation
- la détection et l'investigation
- la compréhension et la décision.

Connaître et anticiper

La capacité à connaître et anticiper les cyber-menaces repose essentiellement sur des activités de veille, qu'il s'agisse des nouvelles attaques ou des nouvelles vulnérabilités, publiées soit par le monde académique, soit par des hackers sur des blogs ou des forums de discussion.

Le CDC intègre cette veille et possède également des moyens de simulation et de test, qui permettent de valider ces nouvelles attaques en environnement quasi réel. Deux éléments fondamentaux ressortent de ces tests :

- une « signature » de la nouvelle attaque qui permet de la reconnaître et de la rechercher dans les systèmes d'Information de nos clients, et
- des contre-mesures appelées «règles de détection» qui permettront la mise à jour de tous les équipements de sécurité afin qu'ils la bloquent au plus tôt.

Toutes les signatures recueillies sont capitalisées dans une base de connaissance, qui est enrichie en permanence et directement connectée au CDC.

Détecter et investiguer

Les moyens de protection et de détection actuels sont nécessaires mais ne suffisent plus. Le repérage précoce des signaux faibles permet d'enrayer au plus tôt le développement d'une intrusion informatique. L'entité CyberSecurity d'Airbus Defence and Space a développé cette nouvelle approche et a créé un outil alliant recherche de signatures et détection de comportements révélant la présence d'attaquants. ***Keelback***® est le nom donné à cet outil que les équipes du Centre de Cyber-défense utilisent quotidiennement.

Keelback® est déployé à deux niveaux du réseau : sur les postes de travail du parc informatique et à la sortie du réseau vers Internet. A chaque fois, il est composé de trois modules : détection de comportements « anormaux », protection contre ces comportements et investigation afin d'en comprendre l'origine. Chaque incident est remonté vers un centre de traitement central et confronté aux signatures de la base de connaissance évoquée plus haut ceci en vue de comprendre les enjeux et d'en tirer une décision.

Comprendre et décider

Le Centre de Cyber-défense présente une stratégie d'ensemble du traitement d'un incident tant au niveau technique qu'opérationnel, et l'outil ***Cymerius***® y joue le rôle-clef d'orchestrateur. Qu'il s'agisse de traitement d'incidents ou de réponse sur incident, quand les équipes sont déployées sur le terrain pour contenir un attaque, les opérateurs font appel à cet outil qui permet de suivre les actions en temps réel.

Cymerius® synchronise les tâches au sein du CDC. Certaines peuvent être lancées automatiquement, d'autres demandent la validation d'un opérateur avant de pouvoir être exécutées. L'orchestrateur permet d'affranchir l'opérateur de nombre d'activités fastidieuses comme la collecte de tous les logs nécessaires à l'investigation suite à détection d'un incident. Il peut ainsi se concentrer sur le travail d'analyse et de qualification. L'enjeu consiste à apporter une valeur métier et business à la sécurité. La connaissance des menaces, associée à la criticité des actifs du client permet de prendre les bonnes décisions pour visualiser et endiguer au plus vite les attaques en cours.

Les « Experts »

Airbus Defence and Space a établi ses Centres de Cyber-défense (CDC) en Europe. En France, actuellement, plus de 50 spécialistes en cyber-défense travaillent au CDC d'Élancourt. En Grande-Bretagne, plus d'une vingtaine d'experts œuvrent à Newport ; ils sont déjà une dizaine en Allemagne pour le nouveau CDC basé à Munich. Ces experts ont tous en commun un très haut degré d'expertise et affichent les habilitations de sécurité les plus élevées.

Profils des attaquants

La première caractéristique des attaquants est leur motivation, qui s'analyse à l'aune du schéma classique MICE – Money, Ideology, Compromise, Ego. Quel que soit leur objectif final, ils sont très bien renseignés sur leur cible (via l'exploitation des réseaux sociaux par exemple), extrêmement organisés, parfois même mandatés et financés par des Etats. Ils recherchent des informations très ciblées.

Les plus perfectionnés de ces groupes d'attaquants développent des outils spécifiques pour leurs besoins propres et les font évoluer au cours de l'attaque, comme l'utilisation de PlugX que nos experts ont vu émerger dès 2013. Cependant, dans bien des cas, la plupart des équipes d'attaquants utilise encore des outils malveillants ayant servi à des attaques déjà anciennes mais hélas encore opérationnelles.…

Ils connaissent donc parfaitement les méthodes pour contourner les équipements de sécurité standards et utilisent aussi les outils d'administration classiques d'un système d'information, ce qui les rend indétectables au premier abord. S'introduire dans votre réseau peut s'avérer long pour ces attaquants mais cela leur importe peu : un seul essai fructueux suffit pour arriver à leurs fins.

Conclusion

Le Centre de Cyber-défense existe aujourd'hui, c'est l'environnement autant que l'outil quotidien des experts. d'Airbus Defence and Space. Son développement a été favorisé par le niveau d'excellence de nos experts et des services intelligents qu'ils ont développés pour traquer les cyber-menaces. Ces centres opérationnels offrent en temps réel aux clients: une vision synthétique et globale de leurs réseaux et des événements de sécurité qui s'y produisent, le bénéfice d'une base de connaissance centralisée mise à jour en permanence et rassemblant tous les détails sur les signatures et modes opératoires des attaquants et enfin des équipes d'experts en cyber-sécurité, opérationnels en 24/7.

L'identité numérique, pierre angulaire de la sécurité dans le cyberespace

Acteurs privés et publics, France et étranger, où en sommes-nous ?

Les Etats, comme les acteurs privés, ont identifié que la croissance du secteur numérique nécessitait le développement de la confiance. Les moyens techniques existent, le mode et la rapidité du déploiement restent très variés.

Avec la fraude liée aux réseaux et protocoles, la fraude à l'identité constitue une menace majeure dans l'univers professionnel comme dans l'univers privé. Pour contrôler la pénétration d'un système au nom d'une personne, il faut agir sur toute une chaîne qui part de la création de l'identité, qui passe par l'authentification et qui peut aller jusqu'à l'analyse comportementale (mon banquier peut s'étonner d'un achat qui tranche avec mes habitudes de consommation).

Le monde compte 2 milliards d'abonnés internet, 6 milliards d'abonnés au téléphone mobile et plus de 50 milliards d'objets connectés. Chacun d'entre nous est confronté à la gestion de la sécurité d'une multitude de comptes par des moyens variés.

Euh, variés, vous avez dit variés ?

Qui n'a pas cédé à la tentation d'un mot de passe unique et trop simple pour gérer l'accès à de nombreux comptes ?

Au-delà de la sécurité, apparaissent de vastes enjeux de facilité d'usage, de respect de la vie privée et d'interopérabilité. Le développement rapide de la mobilité à travers les « smartphones » exige également de nouvelles solutions. Les enjeux sont rapidement contradictoires entre eux, et l'Etat joue un rôle fondamental dans la garantie de l'équilibre entre les exigences de sécurité et celles de protection de la vie privée. Un usage raisonné de la biométrie s'impose progressivement dans une chaîne complète de délivrance et d'usage : par exemple la reconnaissance faciale sur « smartphone » ne nécessite aucun investissement matériel.

Gérer l'accès à une multitude de comptes : le trousseau de clés ne rentre plus dans la poche…

L'Etat et la biométrie, deux acteurs au cœur de l'équilibre entre sécurité, facilité d'usage et respect de la vie privée.

Les Etats comme les acteurs privés s'intéressent de près au domaine de l'identité numérique. La stratégie des Etats-Unis est décrite dans la « National Strategy for Trusted Identities in Cyberspace (NSTIC) » : la priorité est d'inciter les acteurs privés à agir, avec un fort support de l'Etat américain auteur de normes, financeur de pilotes et « early adopter » pour ses administrations.

Pour de nombreux usages, on ne peut se contenter d'une identité « créée à la volée » (par exemple choix libre d'un couple login + mot de passe). On doit partir d'une identité régalienne (cas en Europe de l'Estonie ou de l'Albanie) ou d'une identité délivrée par des entités qui émettent pour elle-même ou pour des tiers moyennant rémunération (cas des banques en Scandinavie). On doit ensuite dériver des identités secondaires multiples, adaptées à différents usages.

Au quotidien, l'authentification forte repose sur un couple, par exemple carte + code PIN, auquel peuvent techniquement se substituer carte + biométrie ou biométrie + base centrale. L'acceptabilité de ces techniques fiables et éprouvées est variable. En France, le recours à une base centrale biométrique est actuellement exclu. Il n'existe pas de texte législatif autorisant une carte d'identité électronique pouvant embarquer des fonctionnalités d'identité numérique utilisables sur internet (puce e-services). Seules sont autorisées les fonctionnalités de voyage au standard international OACI du passeport électronique déjà déployé. A une échelle plus restreinte en revanche, les agents en mairie utilisent depuis plusieurs années une carte d'agent public avec des fonctions d'authentification et de signature électronique permettant de sécuriser le processus de délivrance des documents d'identité. Plus récemment, le concept de « policier 3.0 » mis en avant par le ministre de l'intérieur peut être interprété dans les deux sens suivants :

- un policier doté d'équipements mobiles connectés en toute sécurité et lui apportant une efficacité accrue, par exemple pour analyser une scène de crime en temps réel ;
- un policier capable de faire la police dans le monde numérique.

Le domaine des équipements et services de sécurité se distingue de celui de l'armement par une échelle de temps plus courte et par une moindre implication de l'Etat. Les acteurs privés, industriels, opérateurs, fournisseurs de service jouent un rôle essentiel et livrent souvent à l'exportation des systèmes ou services plus avancés que ceux qu'ils peuvent réaliser en France. Pour autant l'Etat peut et doit continuer à assurer, au-delà de son rôle de régulateur, un rôle de catalyseur et de précurseur.

Exemple d'application pour tout smartphone : protection de fichiers par biométrie avec accès par reconnaissance faciale ou vocale

par **François-Xavier Fraisse,**

ICA

François-Xavier Fraisse a été dix ans en poste à la DGA, dans les domaines du guidage - pilotage de missiles, puis du soutien aux exportations. Il a ensuite rejoint Morpho au sein du groupe Safran. Il dirige une business unit après avoir exercé différentes responsabilités sur des programmes d'identification policière, de gestion de l'identité, de contrôle aux frontières et de sécurité des transports.

Big Data, big risks

Nous bénéficions d'une évolution prodigieuse en matière d'accès et de consommation de l'information. Tout a changé depuis vingt ans avec l'avènement d'Internet, la multiplication des terminaux mobiles et le foisonnement de nouveaux usages. La cybersécurité a accompagné cet essor en tentant de préserver un équilibre entre gravité des risques, coût de la protection et acceptation des contraintes. Voyons comment elle répond aux nouveaux défis posés par les derniers avatars de cette évolution du cyberespace vers l'infosphère que sont le *Cloud computing* et le *Big Data*.

Le *Cloud computing* (le *Cloud*) représente une nouvelle façon d'utiliser et de fournir l'informatique (calcul, connexion, stockage) aux entreprises et aux particuliers. On peut le comprendre comme juxtaposition d'externalisation et de mutualisation. L'externalisation structure l'évolution de l'informatique *(voir figure n°1*). Avant, le réseau, les machines physiques et virtuelles, les applications et les données demeuraient sous contrôle de l'entreprise. Avec le recours à un hébergeur, le contrôle du réseau, du stockage et des machines physiques est partagé avec lui. Avec le *Cloud IaaS* (*infrastructure as a service*), l'entreprise ne contrôle plus rien du réseau, du stockage et des machines physiques. Enfin, avec *Cloud SaaS* (*sofware as a service*) l'entreprise ne gère plus que ses données d'entrée et de sortie.

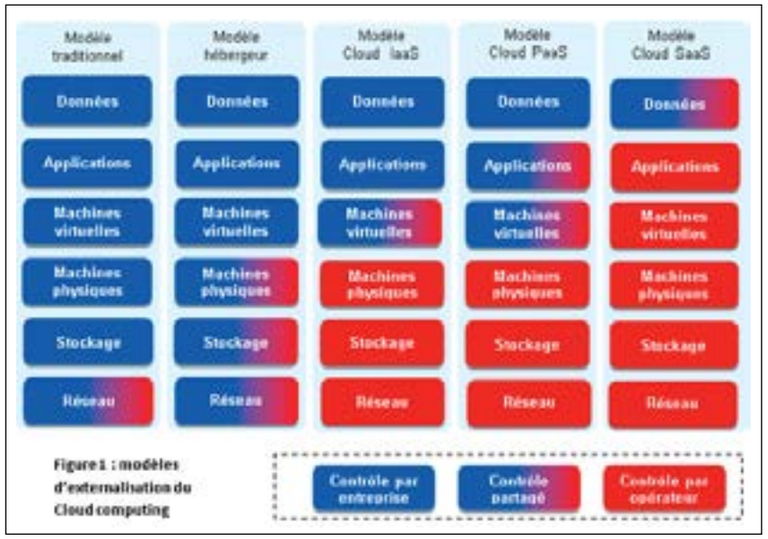


Figure 1 : modèles d'externalisation du Cloud computing

Cette externalisation porte en elle des risques de sécurité spécifiques comme ceux de confidentialité. Les lois s'appliquent territorialement : alors que certains s'imaginent le cyberespace comme un nouveau terrain de jeu hors d'atteinte, il faut savoir que les données sont toujours quelque part où des lois s'appliquent. Les données stockées aux Etats-Unis, par exemple, sont accessibles aux autorités américaines (interceptions légales, Patriot Act, etc.). On s'est bien rendu compte avec PRISM de la réalité de cette menace. L'analyse de risques est essentielle. Elle doit intégrer le risque étatique, évaluer sa probabilité (concurrence, géopolitique…) et son préjudice potentiel qui permettra de borner l'enveloppe financière à consacrer à la sécurité.
Un deuxième risque de sécurité attaché à l'externalisation est celui d'enfermement : retour en arrière non garanti, voire non prévu dans le contrat, coût prohibitif de migration ou de reprise des données…

La deuxième grande caractéristique du *Cloud* est la mutualisation à grande échelle. Cette concentration permet d'offrir aux directions informatiques des économies colossales. On entre dans l'ère industrielle de l'informatique avec ses usines géantes : Amazon disposerait dans ses data-centres d'environ un demi-million de serveurs informatiques. Numergy, l'opérateur français de *Cloud* souverain, a annoncé l'objectif d'un million de machines virtuelles en 2016. Ce n'est qu'à ce niveau que l'on obtient les économies d'échelle qui rendent le *Cloud* tellement incontournable. Cela ne peut se réaliser qu'en mutualisant des milliers de clients dans une seule infrastructure physique. Ce n'est pas sans conséquence sur la cybersécurité. La probabilité d'une cyberattaque contre ces infrastructures géantes est de ce fait considérablement accrue. Elles constituent une cible plus intéressante et plus motivante. Si on accueille plusieurs milliers de clients, la probabilité résultante que l'un d'entre eux soit ciblé est aussi plus élevée. Et si l'objectif du pirate est l'effacement de données, tant pis pour les utilisateurs d'à-côté.

par **Philippe Duluc,**
ICA

Directeur de l'offre cybersécurité de Bull, X82, ingénieur de l'Armement, a démarré sa carrière consacrée à la sécurité au ministère de la défense et au SGDN où il a été Conseiller auprès du Secrétaire général. Puis a rejoint le secteur privé d'abord chez Orange en tant que Directeur sécurité groupe, puis chez Bull. Il est également Vice-président de l'ACN en charge de la cyber-sécurité, et Secrétaire du groupe projet du Plan gouvernemental de relance industrielle cyber-sécurité.

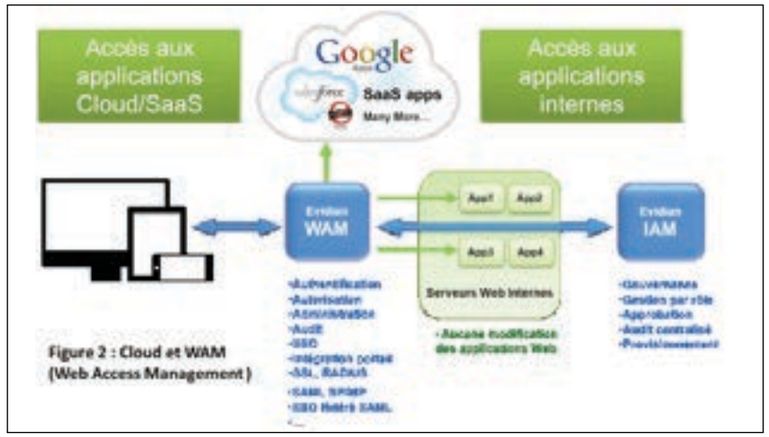


Figure 2 : Cloud et WAM (Web Access Management)

Il s'agit d'un risque collatéral. Comme il y a mutualisation, les données peuvent être affectées lorsque l'opérateur de *Cloud* est ciblé par une attaque ou par une procédure judiciaire. Deux exemples : saisie de baies de stockage par l'autorité judiciaire à cause d'un client pédophile qui y stocke des images, mais - manque de chance - qui contiennent aussi votre comptabilité ; utilisation frauduleuse de *Cloud* par un autre client pour porter des cyberattaques (*voir encadré*) avec un risque juridique ou de riposte. D'autant que le *Cloud* attire certains cybercriminels en leur procurant de la capacité d'attaque massive, anonyme et facilement mobilisable.
Tout devient plus compliqué avec le *Cloud*, comme la gestion des droits d'accès. Dans le cas typique d'une entreprise achetant un service SaaS à un opérateur qui loue l'infrastructure nécessaire à un revendeur IaaS (à l'instar de DropBox qui s'appuie sur EC2 d'Amazon), on a de nombreux rôles (utilisateur final, administrateur client, administrateur opérateur SaaS, administrateur revendeur IaaS, administrateur fournisseur IaaS) dont il faut gérer la sécurité des accès et garantir le principe de « moindre privilège » avec un niveau d'auditabilité élevé. Une technologie comme le WAM (*Web Access Management*) peut se révéler être un bon compromis (*voir figure n°2*) pour gérer l'accès aux applications internes ainsi qu'à celles qui sont hébergées dans le Cloud public, tout en fournissant les rapports indispensables aux auditeurs.
Compte tenu de l'évolution des menaces et du fait maintenant acquis qu'il est impossible d'empêcher une infection initiant une attaque, une stratégie de cyberdéfense est devenue indispensable. Seul un SOC (*security operations center*) moderne est à même de détecter les attaques réussies qui laissent toujours des traces parfois imperceptibles. Il faut rassembler des téraoctets de données : logs de firewalls, descriptions de vulnérabilités, matrices de droits d'accès et de rôles, comptes rendus d'audit, listings de connexions, etc. Il s'agit ensuite d'effectuer des croisements élaborés pour détecter ces signaux faibles révélateurs. C'est du reste un exemple de ce qu'est le *Big Data* : des volumes gigantesques de données non-structurées, parfois captées à des hauts débits, et sur lesquelles on effectue des calculs complexes comme de l'analyse décisionnelle ou de la corrélation basée sur des signatures.
Gros succès médiatique pour le *Big Data*. Tout le monde en parle sur le web, autant des craintes qu'il suscite quant à la protection des données personnelles que la création de valeur qu'il permettrait. L'évolution technologique (notamment du côté logiciels libres comme Hadoop) ouvre de nouveaux horizons avec l'émergence de nouveaux services inespérés jusqu'à maintenant (comme la publicité de masse ciblée), permettant à tous les gestionnaires ou « propriétaires » de données de monétiser ces dernières. Cela intéresse les opérateurs de communications électroniques, les fournisseurs d'accès à l'internet, les agences web, une grande partie du monde scientifique, ainsi que la défense et la cybersécurité. Les volumes de données à collecter et à consolider sont colossaux : 90 % des données existantes sur terre ont été créées ces seules deux dernières années ; Facebook exploite depuis 2010 le plus grand *cluster Hadoop* au monde, pour son infrastructure MySQL avec un volume de 35 à 40 pétaoctets.
Aux risques classiques déjà démultipliés par le *Big Data*, s'ajoutent des risques spécifiques comme par exemple :

- cas du calcul massif distribué quand une cyberattaque sur l'un des nombreux nœuds de calcul peut réduire à néant le travail de toute la grille ;
- cas du stockage de masse quand on priorise traditionnellement en fonction de la fréquence d'accès et pas en fonction de la criticité des données ;
- qualité des données collectées auprès des terminaux professionnels ou grand public comme des ordiphones ou des tablettes ;
- difficulté à assurer la sécurité de bout en bout au travers d'éléments distribués, hétérogènes et non de confiance ;
- complexité du contrôle d'accès à des catégories de données répondant à des référentiels de sécurité différents auxquels il faut se conformer …

On se situe au tout début des promesses du *Cloud* et du *Big Data*. Des questions de cybersécurité restent aujourd'hui ouvertes, et sur lesquelles de l'innovation est nécessaire et attendue. De nouveaux modèles de sécurité se présentent comme le *zero-trust model* dont la sécurité de bout-en-bout est l'une des premières réponses. Le chiffrement dans le *Cloud* pose aussi des problèmes : comment gérer les clés au plus près des utilisateurs finaux ; comment effectuer des calculs sur des données chiffrées par l'utilisateur et sans les déchiffrer (domaine de la cryptologie homomorphique) ? La sécurité de l'accès aux multiples données chiffrées du *Big Data* serait facilitée par l'emploi de chiffrement basé sur les identités, voire sur des attributs d'identité. La prise en compte des questions de cybersécurité dans l'infosphère constitue clairement une double opportunité pour les utilisateurs d'informatique au premier rang desquels figure l'Etat d'abord, et pour l'industrie française, voire européenne de la cybersécurité ensuite. C'est sans doute un challenge à relever en partenariat public - privé.

D'après Bloomberg, le service de *Cloud* EC2 d'Amazon a été utilisé en 2011 pour attaquer le réseau PlayStation de Sony et exposer les données personnelles de presque 10 millions d'utilisateurs, ce qui a constitué l'une des plus grosses cyberattaques aux Etats-Unis. L'attaquant a fourni une fausse identité à Amazon et a pu ainsi ouvrir un compte EC2.

Naissance d'une PME de cybersécurité

Pourquoi une PME lorientaise spécialisée dans les vedettes et patrouilleurs de surveillance maritime crée-t-elle une filiale pour distribuer des logiciels de chiffrement ?

par **Louis Le Pivain,**
IGA

Président de Navitec-Raidco Marine

Après 8 ans à DCN Lorient, Louis Le Pivain (X 72 ENSTA branche Mer) passe 10 ans à l'étranger (Arabie Saoudite, Canada, Belgique). Il a été directeur au SGDSN, coordonnant en interministériel l'intelligence économique et la promotion des exportations d'armement avant de présider la section Carrières au conseil général de l'armement puis de quitter l'administration en 2006 pour racheter la société Raidco Marine. Il est conseiller du commerce extérieur, vice-président du GICAN, membre des conseils d'administration de l'ANAINHESJ, de l'AACHEAr et de la CAIA.

Comme souvent, tout commence par une rencontre, celle d'un fabricant de logiciels de cryptage avec le propriétaire de la PME. Le fabricant est digne de confiance, il est soutenu par des services étatiques spécialisés. Sa société est une petite entreprise française discrète qui rassemble sous sa marque des compétences reconnues dans le domaine de la sécurité. Il a décidé d'être le catalyseur d'un « écosystème » rassemblant des concepteurs et des intégrateurs. Il ne connaît pas le volet commercial et ne souhaite pas s'y impliquer.

Le constructeur de bateaux dispose quant à lui d'une excellente image de marque commerciale, tout particulièrement auprès de dirigeants étrangers. Il n'a aucune compétence technique dans le domaine de la cryptologie ni dans celui des télécommunications et ne souhaite pas en acquérir, mais a de bonnes compétences commerciales pour vendre des bateaux simples, faciles à utiliser et parfaitement adaptés aux besoins de clients qui se défendent contre des pirates ; alors pourquoi ne pas vendre aussi du matériel de cryptologie selon le même principe ?

La complémentarité apparaît clairement entre le fabricant de matériel crypto et le constructeur de bateaux ; une bonne dose de patriotisme associée à un zeste d'inconscience font le reste et emportent la décision.

Les démarches administratives sont lancées : rédaction de l'objet social et des statuts de la filiale, ouverture d'un compte bloqué sur lequel est déposé le capital social. Un statut de SARL est retenu car c'est celui qui présente le plus de souplesse. Logiquement le siège social est établi à la même adresse que celui de la maison mère. La conclusion de ce parcours est l'obtention du fameux K Bis, véritable carte d'identité de toute société, et l'obtention d'un carnet de chèques. Raidco Sécurité est créé. Il s'agit ensuite de trouver des clients.

L'éclatement de l'affaire Snowden donne tout son intérêt à cette création. Les administrations et entreprises françaises sont en situation de sous-culture « sécurité » qui frise parfois l'angélisme. Il existe en leur sein une absence de prise de conscience des menaces et des vulnérabilités. La sécurité de l'information n'est pas réellement perçue comme un investissement immédiatement rentable.

Des systèmes actuels trop compliqués !

Quelle stratégie de positionnement adopter pour une PME qui se lance dans la fourniture d'équipements de cryptologie ? Il convient tout d'abord de bien différencier l'offre par rapport à celle de grands groupes hégémoniques tels que Bull, Thales, Cassidian ou Safran qui proposent des réponses aux besoins de la Défense et de l'interministériel sur financement étatique et sous maîtrise d'œuvre de la DGA dont la mécanique lente et complexe des programmes d'armement n'est plus en phase avec la vitesse d'obsolescence des technologies informatiques. Ils proposent des gros systèmes performants mais lourds. Ainsi en est-il de Teorem, le téléphone crypté mis au point par le groupe Thales, dont les utilisateurs se plaignent qu'il est trop compliqué: la grande majorité des 14 000 exemplaires commandés par l'administration française risque fort de dormir au fond de coffres sécurisés.

Le développement technologique des passeurs de drogue impose de crypter les communications y compris sur un semi-rigide

La PME va donc résolument se tourner vers le « *user friendly* » et privilégier la simplicité d'utilisation et la convivialité d'emploi pour que la mise en œuvre du chiffrement ne soit pas une course d'obstacles. Un haut responsable, qu'il soit dirigeant d'entreprise, haut fonctionnaire ou homme politique, n'est pas prêt à se soumettre à des contraintes de mise en œuvre de chiffrement que seuls les militaires ont pu accepter dans le passé. L'ergonomie d'utilisation devient prépondérante dans le choix de solutions sécuritaires. Aussi la solution consiste à développer un logiciel qui effectue le chiffrement à partir du téléphone usuellement utilisé par le dirigeant.

Face aux vulnérabilités des entreprises et au risque de pillage généralisé, trouver des solutions de protection de leur patrimoine informationnel est une question de survie pour les entreprises. Elles ne sont cependant pas prêtes à y consacrer des sommes importantes, dans une période de crise où le montant de chaque dépense est examiné à la loupe. Ainsi convient-il de proposer une solution « *low cost* », comme sait le faire une PME aux modestes moyens financiers et aux frais de structure et de fonctionnement très réduits.

Vedette de la gendarmerie maritime équipée de moyens de communication cryptés

Apporter une solution souple en communication cryptée pour les dirigeants de PME

Enfin, tout en ne reniant pas le parti pris de simplicité et de modicité évoqué ci-dessus, il est fondamental de pouvoir garantir que les solutions de chiffrement proposées n'ont pas été piégées par des puissances étrangères.

En effet, en dépit d'une réelle expertise dans le domaine de l'informatique et du logiciel, après avoir raté le tournant de la micro informatique à la fin des années 70, la France a raté celui de la protection de l'information au début des années 2000, période où fut décidée la dérégulation en matière de vente et d'usage des moyens de chiffrement.

Cette libéralisation ne fut malheureusement pas accompagnée de la moindre politique industrielle qui aurait permis l'émergence de sociétés françaises sur le marché de la sécurité.

La France qui était malheureusement déjà hors jeu en termes de fabrication de micro-ordinateurs et de systèmes d'exploitation avec l'arrivée de Microsoft ou d'Apple a laissé s'engouffrer des compétiteurs étrangers américains et israéliens puis russes et chinois sur le marché du cloud computing, des réseaux sociaux, mais aussi des systèmes de sécurisation des données.

Dans le domaine des télécommunications la situation n'est pas plus reluisante. Le dernier fleuron industriel français en la matière était Alcatel, spécialiste des commutateurs de réseaux mobiles. Son rapprochement avec l'américain Lucent a définitivement mis fin à la maîtrise des réseaux mobiles en France, contraignant les opérateurs à construire leurs architectures à base de produits américains ou chinois dont on connaît aujourd'hui la perméabilité.

La France et ses opérateurs n'ayant plus aucune maîtrise des architectures télécoms - c'est-à-dire de la « tuyauterie » - il devient urgent de privilégier la protection de l'information elle-même. C'est bien la piste sur laquelle s'engage résolument une PME qui a la volonté d'aller de l'avant contre vents et marées.

Cyberespace
Une nouvelle dimension des conflits géopolitiques

Les révélations d'Edward Snowden sur le vaste programme de surveillance de la NSA ont eu le mérite de démontrer, si certains en doutaient encore, que le développement exponentiel de l'Internet n'a rien ôté de sa pertinence à la géographie ni eu raison des rivalités de pouvoir qui animent le monde. Bien au contraire, l'Internet ajoute une couche de complexité aux conflits géopolitiques d'une intrication croissante.

Le concept même de cyberespace, issu de la littérature de science fiction, a d'abord émergé dans le discours des pionniers de l'Internet, fortement imprégnés de culture libertaire, comme la représentation d'un nouvel espace libre, indépendant, où les lois des gouvernements du monde physique ne s'appliqueraient pas. Il revient en force aujourd'hui dans le discours des Etats qui cherchent à défendre leur souveraineté et réaffirmer leur puissance dans, par et pour le cyberespace, qui est devenu l'objet, le vecteur et le théâtre des rivalités de pouvoir géopolitiques.

par **Frédérick Douzet,**

Professeur des universités

Frédérick Douzet est titulaire de la Chaire Castex de cyberstratégie (Cercle des partenaires IHEDN, fondation EADS) et directrice adjointe de l'Institut Français de Géopolitique de l'Université Paris 8. Ses recherches portent actuellement sur les enjeux géopolitiques du cyberespace, sujets auxquels elle s'intéresse depuis les années 1990 et sur lesquels elle dirige une équipe de doctorants et d'étudiants de Master de géopolitique.

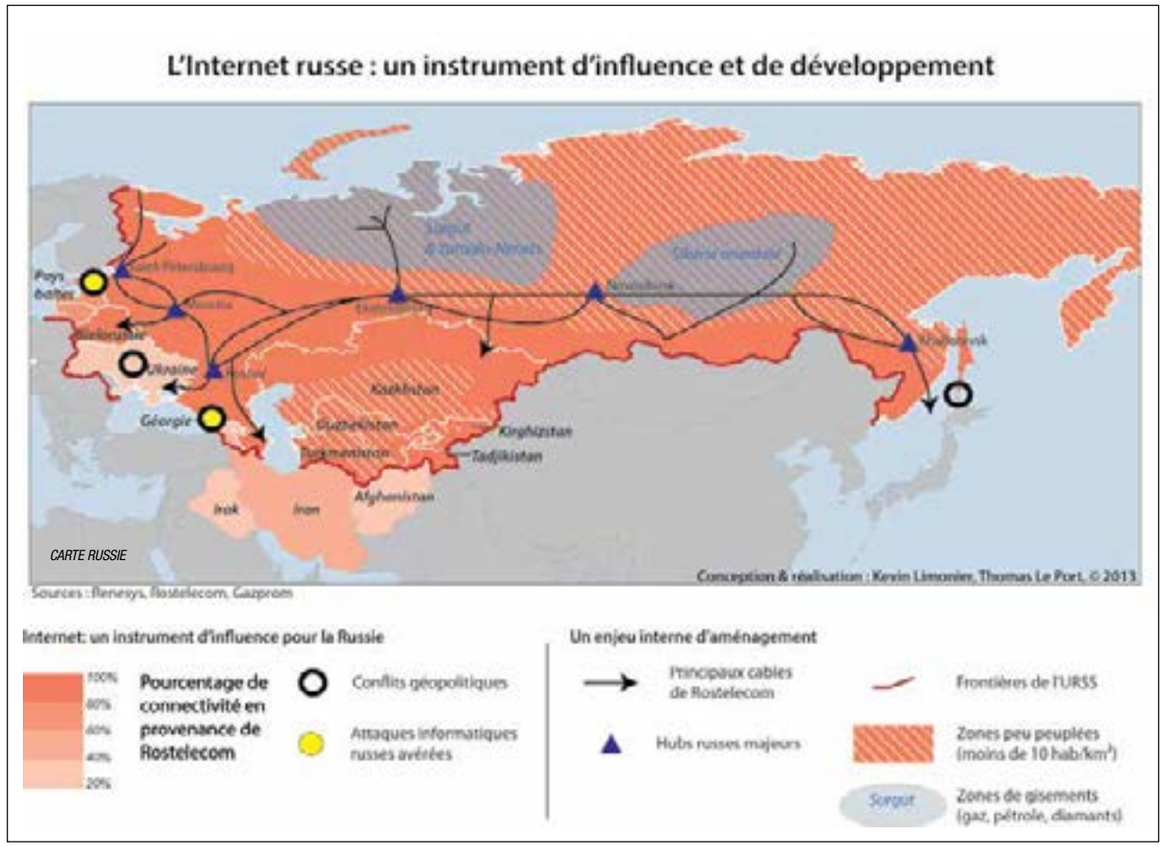
Risques et opportunités du cyberespace

L'internet a en effet suscité autant de défis que de promesses. Les enjeux sont particulièrement importants pour les Etats qui sont exposés à de nouvelles menaces et vulnérabilités, susceptibles d'affecter leurs pouvoirs régaliens. Leur capacité à assurer la sécurité de la nation et défense du territoire est mise au défi par la difficulté à stopper les cyberattaques qui, si elles touchaient les infrastructures vitales, pourraient mettre en danger les populations civiles. Le maintien de la sécurité intérieure et l'ordre public est confronté à la cybercriminalité qui traverse les frontières par les réseaux, rendant de plus en plus complexe l'appréhension, l'arrestation et la poursuite judiciaire des criminels. L'exercice de la souveraineté est problématique alors que les limites de juridiction s'entremêlent dans le monde des réseaux, où le principe de territorialité n'est pas si simple à établir lorsque l'utilisateur, l'entreprise et les données concernés par un même conflit sont situés dans trois pays différents. Enfin, la souveraineté économique et financière se heurte à l'extension des réseaux qui facilitent l'intelligence économique, l'espionnage industriel ou l'évasion fiscale, alors que des multinationales ont acquis une puissance financière et politique inédite. Mais les Etats peuvent aussi, par le biais des réseaux, accroître leur capacités militaires et de renseignement, la surveillance de leur propre population, leur puissance économique ou encore leur influence diplomatique et culturelle.

Les entreprises privées et les organismes publics font également face à de nouveaux risques liés aux possibilités de pénétration malveillante de leurs réseaux visant à corrompre l'information, voler des données ou des secrets industriels, saboter des installations, divulguer ou effacer accidentellement des données. Mais les entreprises peuvent aussi tirer une réactivité, une créativité et une compétitivité accrue de l'interconnexion des systèmes et tirer profit des marchés lucratifs du développement de l'architecture, des services et des contenus des réseaux ou de la cybersécurité.

Ces enjeux impliquent aussi une multitude d'autres acteurs, des forces politiques (terroristes, militants, fondamentalistes religieux …) comme des individus (criminels, « hacktivistes », acteurs non-étatiques, militants libertaires …) dont le pouvoir est renforcé par le faible coût et la forte accessibilité de la technologie. Ils touchent enfin les simples utilisateurs, dont les réseaux ont révolutionné les pratiques professionnelles et sociales, envahissent le quotidien, mais qui, pour la plupart, ne disposent ni des compétences techniques ni des moyens de protéger leurs propres données et leur vie privée de tous les acteurs évoqués plus haut.

Pendant longtemps, ces questions sont restées entre les mains d'une petite communauté d'experts. Aujourd'hui, les gouvernements, les entreprises, la société civile, les militaires ont besoin de mieux comprendre ces enjeux afin d'élaborer une stratégie pertinente, à savoir la capacité à coordonner leurs actions et positionner ses forces dans le but d'atteindre ses objectifs. Car avec le développement massif de l'Internet et son omniprésence dans nos vies quotidiennes, beaucoup de décisions techniques sont devenues politiques et stratégiques.



Chaire Castex de cyberstratégie

La Chaire Castex de cyberstratégie a pour mission de développer la recherche fondamentale et appliquée en géopolitique du cyberespace afin de nourrir cette réflexion stratégique. La géopolitique est l'étude des rivalités de pouvoir sur des territoires, à différents niveaux d'analyse (Lacoste, 1993). Elle permet d'analyser les dynamiques d'un conflit sur un territoire, les représentations contradictoires et les stratégies des acteurs pour son contrôle, son appropriation et la défense de leurs intérêts au sein de ce territoire.

Le cyberespace n'est certes pas un territoire comme un autre en géopolitique, à savoir « une étendue sur laquelle vit un groupe humain et qu'il considère sa propriété collective » (Lacoste 2003). Le cyberespace n'est pas non plus un milieu naturel, contrairement aux autres domaines militaires ; c'est un espace entièrement construit et tout ce qui s'y passe est le résultat de l'action de l'homme. C'est en revanche l'objet de représentations contradictoires d'un territoire — libre ou à conquérir, souverain ou bien de l'humanité à préserver, selon les acteurs — et qui jouent un rôle dans les conflits géopolitiques.

Le cyberespace, c'est à la fois l'Internet — un réseau physique fait de câbles, de serveurs, de routeurs, d'ordinateurs — et l'espace qu'il génère : un espace intangible dans lequel s'opèrent des échanges déterritorialisés entre des citoyens de toutes nations, à une vitesse instantanée qui abolit toute notion de distance. Les conflits du cyberespace n'existent pas en dehors de leur contexte géopolitique. Ils sont le produit des rivalités de pouvoir classiques sur lesquelles ils ont à leur tour un impact, alors que la plupart des conflits géopolitiques comportent désormais une dimension « cyber ». Mais les paradigmes classiques sont mal adaptés en raison des spécificités propres au cyberespace : difficulté d'attribution des attaques, vitesse d'évolution de la technologie, incertitude sur l'impact des armes, impossibilité de les tester en grandeur nature, possibilité de dissuasion par dénis d'accès accrue, multiplication et diversité des acteurs…

La réflexion stratégique est dès lors complexe et pluri-disciplinaire, puisqu'elle peut concerner aussi bien le développement de câbles sous-marins que la lutte d'influence dans l'espace informationnel des réseaux sociaux, en passant par la gestion stratégique des données, le développements de services, la coopération politique ou juridique ou encore l'élaboration de standards techniques.

Notre méthode s'appuie sur le raisonnement cartographique à plusieurs niveaux, qui vise à présenter les enjeux et stratégies du cyberespace dans leur contexte géopolitique. La carte présentée ici permet de comprendre la stratégie d'influence de la Russie sur son étranger proche, par le développement du réseau Rostelecom opérateur contrôlé par l'Etat. Il s'étend dans les zones peu peuplées mais stratégiques et alimente prioritairement la quasi-totalité de l'espace postsoviétique. Il se double d'une enclave linguistique et culturelle entretenue par la prédominance des réseaux sociaux nationaux et des contenus en russe, qui nourrissent la représentation d'un Internet souverain, le « RuNet ».

Plus que jamais, étant donné la complexité des enjeux, la réflexion stratégique a besoin que les mondes universitaires, militaires et techniques se rencontrent et associent leurs efforts.

Une thèse en mathématiques à l'étranger comme formation initiale : dépaysement garanti

Ces dernières années une proportion non - négligeable des IA qui ont intégré le corps de l'Armement ont choisi de suivre une formation par la recherche, et de plus en plus d'entre eux partent effectuer leur doctorat à l'étranger. Ce genre de formations « exotiques » présente-t-il un intérêt pour la DGA et les IA concernés ? Nous livrerons quelques pistes de réflexion à ce sujet à travers le retour d'expérience d'un IA en fin de thèse.

par **François-Renaud Escriva,**

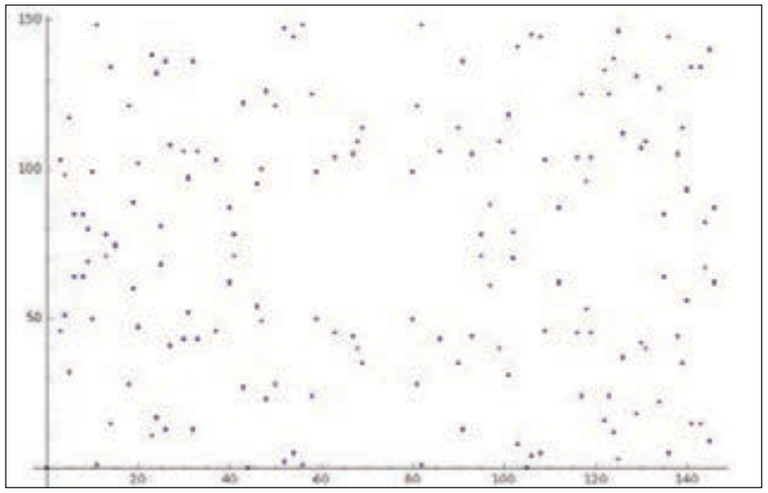
IA

L'IA François-Renaud Escriva (X2007 – IA 2010) a suivi une formation par la recherche. Il est actuellement en 3e année de thèse de mathématiques à la Vrije Universiteit Amsterdam (Pays-Bas).

Pourquoi partir étudier à l'étranger ?

Ayant toujours eu le goût des mathématiques, mon choix d'entrer dans le Corps, et de suivre une formation par la recherche, a été assez naturel à ma sortie de l'X. Quel meilleur moyen, en effet, de pouvoir assouvir mon intérêt pour cette discipline, et de me frotter au monde de la recherche ; tout en sachant que les compétences acquises seraient mises à profit, et ce dans un contexte de montée en puissance du domaine SSI à la DGA ?

Qui plus est, sachant que je travaillerais un certain nombre d'années en France après ma thèse, j'ai cherché à aller faire mon doctorat à l'étranger, afin de découvrir un autre type d'environnement de travail que ceux auxquels j'avais été habitué jusque là. J'ai eu la chance d'être contacté, juste après ma sortie de l'X, par un de mes anciens professeurs qui, connaissant mon profil et mon envie d'expatriation, me transmettait les coordonnées d'un de ses collègues qui cherchait un étudiant pour commencer un doctorat sous sa direction aux Pays-Bas. Après quelques contacts avec ce professeur, il ne m'a pas fallu longtemps pour accepter une proposition de thèse de sa part, proposition qui m'offrait, en plus d'un sujet intéressant à titre mathématique, et plus ou moins lié à certains problèmes cryptographiques (comme nous le verrons plus bas), la possibilité d'étudier à l'étranger tout en restant assez proche de la France (ce qui présente des avantages certains au moment du processus d'affectation pour le premier poste). Ainsi, j'étudie aux Pays-Bas depuis le début de mon stage de master en avril 2011, et ce jusqu'à la prise d'un premier poste à l'automne 2014.



Ensemble des points de la courbe elliptique y^2=x^3+x sur un corps à 179 éléments.
Fonction zêta : Z(C,t) = (1+14t+149t^2)/((1-t)(1-149t))*

Des différences dans le métier de doctorant

Quand on pense à une expérience étudiante dans un pays étranger, les deux différences qu'on évoque presque toujours en premier sont celles de la langue et de l'organisation du système scolaire. La première fut rapidement mise de côté car tout le monde, ou presque, parle anglais couramment en Hollande. En ce qui concerne la deuxième, le système néerlandais est beaucoup plus direct, et offre moins de passerelles que le nôtre (avec ce que ça comporte d'avantages et d'inconvénients). Ainsi, j'ai dû noircir une quantité certaine de tableaux blancs pour expliquer, pendant des pauses café, le système d'enseignement supérieur français, les grandes écoles, les grands corps de l'Etat, etc. Malheureusement, la tâche est considérable et je ne suis pas sûr d'y être arrivé avec succès.

Ces problèmes relativement superficiels mis de côté, j'ai remarqué, pendant ces deux ans et demi, deux différences plus profondes en ce qui concerne les doctorats. Tout d'abord, les interactions sociales, notamment en termes de rapports hiérarchiques, me paraissent beaucoup moins formelles qu'en France. Je ne prétends pas que ceci soit toujours une bonne chose ; néanmoins, le fait que les rapports entre les étudiants et les chercheurs (et pas seulement entre un directeur de thèse et ses thésards) soient beaucoup moins distants que ce que j'ai pu connaître en France me semble favoriser le travail de recherche, en rendant les interactions entre ces différents groupes plus fréquentes.

De plus, même si les charges de travail qui sont dues aux universités, notamment en termes d'heures de cours à effectuer, ne changent pas tellement entre les deux pays, les doctorants (sauf les exceptions comme les militaires français de passage) sont ici considérés, administrativement parlant, comme des chercheurs et des salariés de l'université, et non plus comme des étudiants. Dans un pays où la place du chercheur dans la société est, à ce qu'il me semble, mieux reconnue, ce statut facilite un grand nombre de choses dans la vie quotidienne des thésards (en terme d'accès à un prêt ou de facilités pour trouver un logement par exemple), ce qui leur permet de mieux se concentrer sur leurs recherches, et d'être potentiellement plus productifs.

Et les maths dans tout ça ?

Quand on fait des mathématiques, il est toujours difficile d'expliquer son travail sans remplir des tableaux de formules ; je vais néanmoins tenter d'expliquer ici les grandes lignes de ce que je fais. Bien que faisant des recherches de maths pures, un des projets sur lesquels je travaille est, comme évoqué plus haut, connexe à certaines questions qui se posent en cryptographie : je pense ici au problème du comptage de points. La question naïve est la suivante : étant donné une courbe, avec de bonnes propriétés, définie sur un corps fini (penser ici à quelque chose qui ressemble à Z/pZ), combien de points possède-t-elle (*voir l'illustration*) ? La question est, bien évidemment, à relier à la cryptographie sur les courbes elliptiques, et, notamment, au choix des paramètres. Ce que cherchent à faire les mathématiciens en pratique est de calculer, en un temps polynômial en les données du problème, une certaine fonction génératrice (la fonction zêta) qui encode cette information, ainsi que le nombre de points de la courbe sur toutes les extensions finies du corps de départ. Dans le cas d'une courbe elliptique, les algorithmes pour faire ce calcul « rapidement » sont bien connus. Pour des classes plus larges de courbes, des algorithmes sont connus pour faire ce calcul moins rapidement, mais pour le faire en un temps « décent » malgré tout (je pense notamment aux courbes hyperelliptiques qui sont susceptibles d'intéresser le cryptographe). Notre approche, avec mon directeur de thèse, Rob de Jeu, et un de ses collègues, Amnon Besser, a été d'élargir ces derniers algorithmes, en introduisant de nouvelles méthodes pour faire certains calculs, afin de savoir résoudre ce problème pour une classe très générale de courbes, qui contient quasiment toutes les courbes « avec de bonnes propriétés ».

Le bilan de ma formation

À l'heure du bilan, autant commencer par évoquer les points négatifs car, ne nous leurrons pas, toute formation en possède. Il est parfois arrivé, pendant les deux premières années, que les contacts avec la DGA soient un peu rares, et qu'un léger manque d'information se soit fait ressentir. Cela dit, il faut reconnaître que nous avons été bien pris en charge en dernière année ; et le retour à la DGA ainsi que la recherche du premier poste seront sans doute moins délicats pour nous qu'ils ne l'ont été pour certains de nos proches prédécesseurs.

Je suis, cependant, très heureux rétrospectivement d'avoir choisi cette formation pour de nombreuses raisons. À titre personnel, j'ai tout d'abord eu la chance de pouvoir étudier puis travailler dans une discipline qui me passionnait pendant quatre ans, sans trop de contraintes. En outre, en plus des bénéfices traditionnels liés à une formation par la recherche (acquisition d'une autonomie certaine, apprentissage de la gestion du temps, du stress, rapport à l'échec, stimulation de l'esprit critique et des capacités d'analyse, etc.), je pense qu'une formation à l'étranger est très profitable, en ce qu'elle favorise l'ouverture d'esprit et oblige l'étudiant à faire preuve d'initiative pour s'intégrer dans une culture qui n'est pas la sienne.

Par conséquent, je pense que cette formation fut pour moi très enrichissante, et m'a doté d'un bagage technique et humain qui va me permettre d'aborder sereinement mon premier poste.

Le concept de cyber-dissuasion a-t-il un sens ?

Les menaces sont sournoises et diffuses, les représailles aussi…

Définir la cyber-dissuasion

Plus généralement, la dissuasion est un « mode particulier de l'interdiction » qui vise à « prévenir certains mouvements bien identifiés de l'adversaire ». Cette interdiction ne prend pas la forme d'une pression physique sur l'adversaire, mais de « menaces clairement formulées », afin d'amener ce dernier à « constater rationnellement que son propre intérêt est de ne pas s'engager dans la ou les directions interdites ».

Si la langue française ne connaît qu'un seul terme, la langue anglaise en distingue deux : « dissuasion » et « deterrence ». La « dissuasion » s'inscrit en amont de la « deterrence » ; elle est l'ensemble des actions qui visent à annihiler chez un adversaire (ou même un allié) toute tentation non pas d'agression, mais de développement de capacités agressives, en le convainquant des conséquences qui résulteraient de ce choix (coûts, absence de bénéfices. Si le coût surpasse les bénéfices espérés, un acteur rationnel devrait être dissuadé). Il convient de décourager à la base toute initiative qui s'avèrerait à plus long terme menaçante. La « deterrence » consiste quant à elle à empêcher que le tiers déjà doté de ces capacités n'ait la possibilité ou l'intention d'en faire usage, et à le « dissuader » de les accroître ou de les transférer. La « dissuasion » est ainsi un travail de conviction et d'interdiction de création de capacités ; la « deterrence » est la phase qui vise à imaginer les méthodes permettant de contrer l'utilisation de capacités existantes, à s'en protéger.

par **Daniel Ventre**

Daniel Ventre appartient au CNRS (CESDIP). Il est titulaire de la Chaire Cybersécurité & Cyberdéfense (Ecoles Militaires de Saint-Cyr Coëtquidan – Sogeti – Thales).

Aucune réflexion sur la cyber-dissuasion ne semble pouvoir aujourd'hui échapper à la recherche de similitudes avec la dissuasion nucléaire. Certains affirment que les principaux concepts de la dissuasion nucléaire s'appliquent au cyberespace ; d'autres, au contraire, qu'ils sont incompatibles avec le « cyber » ; d'autres encore que la dissuasion faisant partie du vocabulaire stratégique depuis des siècles, il n'y a aucune raison pour qu'elle ne puisse s'appliquer au cyberespace. Aucune approche ne fait consensus. Mais au-delà de différences ou convergences avec la dissuasion nucléaire, la cyber-dissuasion peut être définie comme la menace de riposte à une cyberattaque « majeure » (c'est-à-dire principalement contre des infrastructures critiques, vitales). La riposte pourrait être militaire conventionnelle (dissuasive asymétrique), ou cybernétique (dissuasion symétrique). La cyber-dissuasion peut également désigner l'utilisation du « cyber » comme moyen de dissuasion, c'est-à-dire comme capacité au service de la stratégie de dissuasion d'un Etat.

Les obstacles vers une cyber-dissuasion

De la définition proposée ci-dessus de la dissuasion, nous retenons qu'elle suppose :

1. l'existence d'acteurs rationnels, capables de prendre conscience de la supériorité des risques encourus par rapport aux gains espérés. Or au regard du large spectre d'acteurs susceptibles d'utiliser le cyberespace, nous pouvons faire l'hypothèse que les acteurs rationnels ne sont pas les seuls à devoir être pris en compte. La cyber-dissuasion ne peut prendre en compte toutes les situations, toutes les menaces ;
2. l'existence de capacités rendant le discours crédible et suffisamment menaçant : le discours américain posé dès 2010 menace les agresseurs potentiels de représailles soit cybernétiques (« cyber » contre « cyber ») soit conventionnelles (militaire armée). Afficher l'existence de capacités de réaction « cyber » remet en question une partie de la stratégie de communication des Etats qui devront dès lors reconnaître l'existence de ces capacités offensives jusqu'ici encore souvent niée. Une réponse symétrique suppose de disposer de moyens d'attribution fiables, avec des marges d'erreur infimes ; d'être capable de distinguer les attaques sous fausse bannière ; de gérer le risque d'erreur d'interprétation, toujours possible ; de maîtriser la complexité des systèmes qui accroissent les risques de dommages collatéraux et la difficulté de maîtrise des effets produits (notons ici que la complexité des réseaux, l'interdépendance des Etats en raison de leurs connexions à un même système global qu'est le cyberespace, peut constituer en soi un principe dissuasif pour des acteurs rationnels conscients de la difficulté qu'il y a à maîtriser les effets produits) ;
3. des adversaires identifiés : or nous savons que dans le cyberespace les adversaires peuvent masquer leur action, l'attribution être difficile, incertaine. L'une des conditions premières de la cyber-dissuasion résiderait donc dans l'existence de capacités d'attribution infaillibles. En l'état, les agresseurs sont au contraire incités, encouragés à agir, davantage qu'à la retenue ;
4. un répertoire d'actions précis qui fera l'objet des interdictions : en matière « cyber », cet ensemble d'interdits peut être exprimé de manière assez large. Il peut désigner des modes d'action, des cibles interdites (exemple : les infrastructures critiques), des seuils de violence inacceptables, ou au contraire les taire. Mais l'un des écueils là encore demeure l'attribution, car les menaces de représailles ne peuvent s'appliquer de pareille manière selon que les cibles de ces dernières sont étatiques ou non ;
5. l'existence de directions non interdites (une marge de manœuvre accordée à l'adversaire), la dissuasion ne pouvant prétendre tout interdire. Pour l'heure, le cyberespace fait encore précisément partie des espaces non couverts par une véritable stratégie de dissuasion. De sorte que les cyberattaques font encore partie de cette marge de manœuvre qui est accordée aux Etats.

La cyber-dissuasion consisterait à trouver l'équilibre entre une « intention clairement exprimée […], une capacité technique […] un mode d'expression clair pour se faire comprendre d'un adversaire dans un jeu aux règles imprécises ».

La Cybersécurité : Eurosae relève le défi pour la formation

Eurosae, filiale de l'ENSTA ParisTech et de l'ISAE, accompagne avec succès ses clients avec des formations dédiées aux domaines de l'aéronautique, du spatial, de la défense et des hautes technologies. Face aux nouveaux besoins du marché, Eurosae a mis en place des programmes de formation continue sur la cybersécurité.
Ces formations couvrent les solutions technologiques, la réglementation et les organisations, la mise en œuvre de techniques très pointues, et les formations de sensibilisation où sont abordés les aspects humains.

par **Frédéric Guir,**
ICA

Frédéric Guir (X80 – ENSTA 85), docteur en synthèse organique de l'université Paris XI Orsay, a commencé sa carrière au Centre d'Etudes du Bouchet dans le domaine de l'évaluation de la menace chimique, et a participé à partir de 1992 au désarmement chimique de l'Irak. Il a poursuivi sa carrière avec la supervision à la DRI des relations d'armement avec divers pays du Golfe, et sera ensuite attaché d'armement à Abu Dhabi de 2001 à 2004.
A son retour, il s'oriente vers les métiers de la formation d'ingénieur à la DRH pour faciliter leur internationalisation, et ensuite à l'ENSTA ParisTech pour faire évoluer les programmes de formation nationaux. Il est depuis 2011 directeur d'Eurosae, la filiale de formation continue de l'ISAE et de l'ENSTA ParisTech.

Panorama des formations en Cybersécurité

L'offre actuelle se structure autour des divers acteurs traditionnels du domaine informatique.
D'un côté, les PME innovantes, les sociétés de conseil informatique, les prestataires de confiance proposent, chacun dans leur domaine de compétence, des formations ou de l'accompagnement.
De l'autre, les écoles d'informatique et plus spécialement les écoles d'ingénieurs informatiques, proposent des offres de formation initiale, plus rarement de la formation professionnelle.
Pour sa part, l'ENSTA ParisTech propose le Mastère spécialisé « Architecture et sécurité des systèmes d'information » qui s'est vu renforcé en 2010 par un module complet dédié à la cybersécurité.
Forte de son lien avec l'ENSTA ParisTech, Eurosae propose pour mi-2014 une offre globale de formation continue reposant sur l'expertise de l'ENSTA ParisTech et des meilleurs experts du domaine avec l'ambition de devenir le véhicule de formation.
Cette offre d'Eurosae permettra aux industriels français de former leurs ingénieurs au meilleur niveau technique et de sensibiliser l'ensemble des catégories de personnel concernées par la cybersécurité, le tout selon les exigences de l'ANSSI et du ministère de la défense.
Mais avant il a fallu résoudre la quadrature du cercle de l'enseignement de la cybersécurité, qui tient à ce que le cyberespace est vaste et sa sécurisation multiforme.
En effet d'un côté, les systèmes d'information et leur interconnexion à travers internet se sont répandus dans presque tous les secteurs d'activité et de l'autre, les formes de la cybercriminalité sont multiples.
Si nous pouvons dire avec Jack Welch « *le marché est plus grand que nos rêves* », nous sommes bien aussi obligés de constater que « *la menace est plus grande que nos cauchemars* ».
Ces deux caractéristiques de taille représentent un défi d'ampleur pour un organisme de formation continue : enseigner l'expérience et les techniques d'aujourd'hui mais aussi donner les moyens d'anticiper les défis de demain.
Les évolutions technologiques perpétuelles de l'informatique et l'émergence de nouvelles menaces réclament en effet une approche globale et les RSSI de demain doivent développer une vision complète de tous les aspects de la cybersécurité, afin de contrer les attaques futures.
Eurosae a confié la tâche d'élaborer son offre de formations à la cybersécurité à notre camarade Thierry Leblond, IGA, qui a conduit avec succès des projets de grands systèmes d'information sécurisés, tant dans le secteur privé que dans l'administration.
Il fédère sur le projet d'Eurosae une équipe d'experts autour d'une approche globale de la cybersécurité. (voir encadré de Thierry Leblond).

Une initiative structurante : le pôle d'excellence

Dans sa démarche d'ingénierie, Eurosae est aidée par l'arrivée d'une bonne nouvelle : la création d'un pôle d'excellence de cyberdéfense en Bretagne avec la nomination par le ministre de la Défense en décembre 2013 d'un chef de projet, l'ICA Pincemin pour tirer avantage des investissements déjà consentis dans cette région.
En effet, outre la DGA/MI à Bruz, le ministère y dispose de sérieux atouts pour répondre à son besoin d'un mastère spécialisé en cyberdéfense : l'Ecole des transmissions de l'Armée de Terre à Rennes, l'Ecole Navale à Brest et l'Ecole de Saint-Cyr Quoetquidan.
A l'instar d'Aérocampus en région Aquitaine, il y a tout lieu de penser qu'un « Cybercampus » permettrait l'éclosion des meilleures formations à la cybersécurité sur place.
Pour cela, il convient non seulement de fédérer les compétences locales mais aussi d'attirer sur place la collaboration active des grands acteurs du secteur issus d'autres régions.
C'est ainsi qu'Eurosae et l'ENSTA ParisTech, chacune à son niveau, étudient déjà la localisation de certaines de leurs formations en cybersécurité sur place.
Cette initiative permettra d'enrichir le pôle d'excellence de leur propre compétence et fera bénéficier leurs stagiaires des ressources d'excellence du « Cybercampus » à venir dans une stratégie de fertilisation croisée, qui est au cœur du modèle économique d'Eurosae.

La cybersécurité change rapidement et ne peut être enseignée sans contact avec la vraie vie industrielle

Eurosae est une société d'économie mixte contrôlée à 80 % par deux établissements publics d'enseignement supérieur, l'ISAE et l'ENSTA ParisTech sous tutelle du ministère de la Défense. Son action prolonge et complète celle de ses actionnaires notamment dans le secteur concurrentiel du service à l'industrie dans le domaine de la formation professionnelle. Son chiffre d'affaires est en 2013 de 3,6 M€.
En fait Eurosae est un intégrateur de formation et ne possède pas de formateurs salariés en propre : elle fait appel à des formateurs en provenance de grandes entreprises, qui sont donc à la pointe des technologies et ont une connaissance pratique de l'évolution des besoins.
Les écoles de leur côté ont leur propre activité de formation continue en offrant des modules de mastères ou des formations certifiantes (Certificats d'Etudes Spécialisées) dont certaines sont co-développées avec Eurosae pour faciliter leur commercialisation sur mesure.
Eurosae complète l'action des écoles en développant des services mutualisés accessibles à l'ensemble des acteurs du secteur économique.
En effet les formations techniques très pointues ne sont viables que si elles sont proposées en même temps à l'ensemble de la profession et répondent aux besoins présents et futurs du marché existant. C'est un grand avantage que ne peuvent offrir les universités internes des entreprises limitées à leur clientèle interne.
De façon plus globale, Eurosae offre ses formations aux grands organismes technologiques du pays tant industriels qu'étatiques tout en ayant recours aux experts qui travaillent dans ces mêmes grands organismes.
Cette transmission mutualisée du savoir et du savoir-faire est au cœur de la stratégie de fertilisation croisée qu'Eurosae a établie avec ses clients et qui fait partie de son ADN.
C'est cette capacité de synergie entre public/privé qu'Eurosae veut mettre à la disposition du futur pôle d'excellence en cyberdéfense.

par **Thierry Leblond,** IGA

fondateur de Scille SAS, conseil en stratégie et sécurité des SIC auprès d'Eurosae

« Quand on parle de cybersécurité, de quoi parle-t-on ? » La cybersécurité est protéiforme. C'est pourquoi nous avons retenu une approche globale à la fois organisationnelle, humaine, technique, réglementaire et opérationnelle articulée en cinq thématiques :

- finalités de la cybersécurité et aspects stratégiques ;
- comprendre l'attaquant et se protéger ;
- architectures et développements informatiques sécurisés ;
- réglementation, méthodologies et homologation de sécurité des systèmes d'information ;
- gestion de crise « cyber ».

Ce découpage est cependant mouvant car l'arrivée de nouvelles technologies informatiques ultra-compétitives autour de la mobilité, du Cloud et de la virtualisation, qui s'imposent déjà dans notre quotidien, changent l'approche traditionnelle de la sécurité des systèmes d'information. Dans ce contexte de perpétuelle évolution de la menace informatique et de demande croissante de formation des personnels en cybersécurité tant en termes de sensibilisation que de perfectionnement et d'expertise, Eurosae a souhaité disposer d'une offre de formation cohérente et globale au profit de son catalogue de formation en s'appuyant sur des experts de ce domaine, partenaires de la démarche.

Cyber sécurité aux Etats-Unis : dérives d'une militarisation à l'américaine

Le traitement de la cyber sécurité aux Etats-Unis est confronté à une absence de véritable stratégie nationale. Il est totalement otage de la NSA, ce qui conduit à rendre la formidable position dominante américaine au minimum embarrassante, certainement dommageable pour la sécurité collective de part et d'autre de l'Atlantique et probablement intenable en l'état à terme.

Très largement versés en coopération étroite avec son allié britannique dans le domaine offensif depuis la deuxième guerre mondiale, les Etats-Unis (si on en croit l'histoire officiellement publiée sur les conflits cybernétiques) auraient été confrontés au problème de sécurité de leur réseau de manière manifeste pour la première fois en 1986 lorsque des hackers allemands auraient pillé des informations sur les programmes de défense anti-missile pour les vendre au KGB.

Depuis et jusqu'à aujourd'hui, force est de constater que les Etats-Unis ne se sont jamais vraiment départis d'une militarisation toujours renforcée de leur politique de cyber sécurité, transformant ainsi progressivement leur indiscutable supériorité sur le plan des capacités offensives en vulnérabilité sur le plan défensif, face aux évolutions rapides des nouveaux enjeux sociétaux et économiques façonnés par deux facteurs principaux : premièrement l'avènement de nouveaux acteurs sur la scène internationale dans le domaine offensif et deuxièmement la croissance exponentielle de l'utilisation des technologies de l'information dans l'économie du pays.

Le débat est pourtant bien lancé aux Etats-Unis depuis plus de 10 ans et les enjeux sont particulièrement bien énoncés. Les uns après les autres, les documents de politique fédérale clament haut et fort les méfaits des attaques contre l'économie digitale américaine et la nécessité urgente et impérieuse d'instaurer des règlementations ainsi qu'une organisation et des moyens qui préservent et réconcilient l'ensemble des enjeux : non seulement la sécurité nationale mais aussi la liberté et la sécurité d'accès à Internet, les libertés individuelles, la sécurité des infrastructures vitales, la promotion des activités économiques, le soutien et la protection de la base industrielle nationale, etc.

Ainsi les politiques et stratégies au niveau de la Maison Blanche se sont succédées, tout comme les nominations de coordinateurs nationaux (sorte de « tsars » du domaine sans véritable pouvoir). Le DHS (Department of Homeland Security) a été créé avec pour mission principale dans le domaine cyber de protéger le secteur civil privé et gouvernemental. Des centres de coordination tels que le NCCIC (National Cybersecurity and Communication Integration Center) ainsi qu'un plan national d'actions en cas d'incidents majeurs, le NCIPR (*National Cyber Incident Response Plan*), ont été mis en place. Enfin le NIST (*National Institute of Standards & Technology*), en tant que composante technique du dispositif, a développé des standards et protocoles pour renforcer la défense des réseaux civils.

Tout cela peut paraître attractif en théorie mais en pratique très peu de progrès ont été accomplis dans la défense du secteur civil qui demeure largement dans une impasse. Conséquence d'un manque chronique de moyens et d'un cadre éthique et juridique restrictif, le DHS se refuse à mettre en œuvre les technologies et pratiques nécessaires (jugées trop intrusives) pour véritablement analyser les vulnérabilités des infrastructures vitales civiles (privées et gouvernementales) et apporter les remèdes correspondants en terme de réglementation. Seule exception, le secteur bancaire qui s'est pris en main voyant un retour direct dans les investissements consentis dans la défense de leurs réseaux et qui bénéficie ainsi d'un soutien technique gouvernemental significatif, notamment en terme d'accès aux moyens de simulation d'attaques.

A l'opposé, la NSA agit avec profusion de moyens et dans un cadre éthique et juridique particulièrement permissif qui encourage la prise de risque systématique et la mentalité de « *cow boy* » enthousiaste de la gâchette. La quasi-totalité des financements, des technologies et de l'industrie (près de 800 entreprises implantées autour de Fort Meade) est contrôlée par la NSA. Les opérations de lutte active tant pour le DoD que pour la communauté du renseignement sont également contrôlées par la NSA dont les agents sont seuls habilités à agir. Enfin, le service juridique de la NSA est à la hauteur de son service action et depuis le « *Patriot Act* » l'agence a un mandat très large puisqu'elle est officiellement en charge de mettre en œuvre tous les moyens nécessaires (et en tout lieu) pour surveiller et intercepter les communications de tout acteur pouvant influer sur la sécurité nationale, sans autre véritable forme de contrainte.

En résumé, la NSA s'est trouvée dans une situation où elle a carte blanche pour agir et où le traditionnel système américain de « *check and balance* » a volé en éclat. Ainsi l'histoire récente depuis Stuxnet jusqu'aux révélations de Snowden a illustré la dérive d'une énorme structure américaine totalement optimisée pour la lutte informatique active sans contrôle politique civil à la hauteur des enjeux.

Les conséquences néfastes de cette situation sont multiples pour la cyber sécurité des Etats-Unis et de leurs alliés occidentaux. Sans parler de la perte de confiance qui est un problème sûrement gérable entre alliés, une fois passée la crise politique, d'autres revers sont davantage problématiques. D'une part les technologies et les concepts pour la protection des réseaux étant directement dérivés de ceux utilisés pour les actions offensives, ils sont le plus souvent tout simplement rendus indisponibles pour ne pas compromettre les capacités offensives. D'autre part, la politique internationale américaine basée sur une approche évangélique d'adhésion à des standards de conduite est désormais ouvertement décrédibilisée, ce qui renforce d'une certaine manière la position des pays décriés par ailleurs pour leur tendance au pillage industriel.

En conclusion, si, comme semblent le penser la plupart des spécialistes, l'enjeu principal de la cyber sécurité pour éviter une escalade incontrôlée d'un conflit cybernétique réside dans les capacités de défense des réseaux et non dans les capacités offensives, l'Oncle Sam (qui est coutumier du fait) se trouve dans une situation où il est surtout menacé par son ombre.

par **Marc Esteve,**

Chairman & CEO, U.S.-CREST Group

Impliqué dans les relations transatlantiques de défense et de sécurité depuis une vingtaine d'années, l'ICA (ER) Marc Esteve a été en poste au SAA de Washington de 93 à 96 et de 02 à 06. Il est chairman & CEO de U.S.-CREST Group et est diplômé de l'ICAF (Industrial College of the Armed Forces).

La troisième voie du monde « cyber »

« *Pour gagner le pari de la confiance, tout projet numérique d'envergure doit tracer clairement en amont le fil entre liberté et sécurité.* »

La problématique de la coexistence des acteurs de l'économie numérique est mouvante et renvoie à celle des enjeux sociétaux des systèmes. Pour brosser quelques traits de son évolution on distinguera (faisant abstraction des acteurs de la sécurité) trois « profils type » : utilisateur lambda, malfrat, personne recueillant des données personnelles.

par **Frédéric Tatout,**
ICA

Chercheur au CEA puis chef de projet à la DGA, Frédéric Tatout a été responsable de l'animation de thématiques du développement des usages numériques au ministère de l'industrie, parmi lesquelles la SSI et la confiance. Après une période comme responsable de secteur industriel à la DGA, il dirige des projets transverses et d'amélioration de performance du MCO aéronautique au sein de la SIMMAD.

Sous un angle historique, la loi informatique et libertés du 6 janvier 1978 place la France comme un précurseur dans la lutte contre les abus concernant les fichiers de données personnelles. Elle cible tout particulièrement les projets émanant de la personne publique, en raison notamment (mais pas seulement) de l'importance des moyens qu'elle est susceptible de déployer à cette fin, à l'époque, par rapport aux acteurs du secteur privé. Mais très vite certaines affaires (vols de disques durs, entre autres) démontrent que l'écart des niveaux de risque entre secteur privé et public


Target Announces $5 Million Investment in New Cybersecurity Coalition

s'estompe. Enrichie par la directive 95/46/CE, cette loi est refondue en 2004, en intégrant cette évolution : allègement relatif du régime d'autorisation pour les projets du secteur public, renforcement de l'obligation de sécuriser les données, sanctions pécuniaires à l'encontre d'acteurs privés fraudeurs ou négligents.

Qu'en est-il alors de la SSI ? Avant le 11/09/2001 il s'agit d'un enjeu clé de la confiance dans les premiers services en ligne. En Europe continentale, on prône le déploiement d'outils de sécurité (carte à puce, signature électronique forte, etc.) ; aux USA, la liberté d'entreprendre et les « schémas de confiance » autorégulés. Le débat sur la fraude à la carte bancaire en 2000 illustre cet écart outre Atlantique : on a deux systèmes aussi proches en apparence (du moins dans le regard des utilisateurs) qu'éloignés en termes de processus, organisation et technologies. Dans ce contexte, les fraudeurs se régalent, entre autres, de l'éclosion du commerce sur Internet : les tickets de paiement (ramassés ou achetés dans une cour d'école ?) contiennent encore à l'époque le nécessaire pour payer sur Internet !

Septembre 2001 : volte-face de la Maison Blanche qui prône désormais une approche renforcée et globale de la sécurité. Passent en urgence le *Patriot Act*, qui concerne, soit dit en passant, « toute organisation ayant des intérêts aux US », le *Transport Security Act* (TSA) visant à contrôler les entrées sur le territoire US. Dans la foulée suit le passeport à puce. Les compagnies aériennes sont sommées de récupérer des données sur les voyageurs, les autorités européennes dénoncent un acte unilatéral. Naît alors outre Atlantique un débat intense sur les transferts de données personnelles au-delà des frontières. L'accord Safe Harbour n'étant pas jugé suffisamment convaincant, la loi informatiques et libertés se dote en 2006 d'un premier niveau de contrôle (faible) sur les transferts de données personnelles hors d'Europe.

Pendant ce temps les media relèvent des lacunes des nouveaux systèmes de contrôle aux frontières (toners d'imprimante piégés retrouvés en soute, 10/2010), leurs inéluctables exceptions de fonctionnement (fausses alarmes, non détections, etc.) illustrées entre autres par l'affaire Umar Farouk Abdulmutallab, l'homme qui cachait des explosifs dans ses sous-vêtements : signe que les exceptions, même les plus anodines en apparence (voyageur bloqué dans le sas de reconnaissance d'empreinte par exemple) doivent absolument être anticipées sous peine, cette fois, de générer des accidents. L'absence de conséquence dramatique semble montrer (jusque-là) qu'elles l'ont été. Il semblerait aussi que l'Etat régulateur et le tenant des libertés individuelles aient appris à surmonter leur défiance réciproque des années 80.

Avec Internet 2.0, la dualité essentielle entre sécurité et liberté connaît une nouvelle évolution. A quoi ressemble-t-elle à présent ? On notera que parallèlement au renforcement légal des capacités de lutte contre la menace « cyber », le débat sur l'identité numérique se développe. La création de Google + en réaction (apparemment) à des polémiques n'est qu'une partie de l'iceberg. D'une part, le déploiement de moyens fiables d'identification (identifiant et signature électronique forte) semble plus que jamais nécessaire pour renforcer de manière significative la sécurité. D'autre part, on observe la faible puissance des techniques d'anonymisation des données personnelles face au développement du « *Big Data* ». Et parmi les 3 profils type évoqués ci-dessus, l'acteur recueillant des données personnelles du secteur privé pèse désormais bien plus lourd qu'avant (tout comme le malfrat), qu'il soit « personne clé » d'un leader d'Internet très au fait des subtilités réglementaires ou responsable marketing de groupes plus traditionnels (souvent pas très au fait en la matière…).

Faut-il parler d'une ligne de crête entre les deux scenari extrêmes, « *anarchie cyber* » et « 1984 », que l'on pourrait perdre ? Inutile de faire du catastrophisme. Mais pour déminer leur champ stratégique les porteurs de projet devront s'habituer à clarifier toujours plus leur posture, affiner leur discours sur les problématiques indissociables de sécurité et liberté, et anticiper, du concept à la mise en œuvre du projet.

Ils devront aussi plus que jamais, de même que les institutions concernées, surveiller le terrain réglementaire au plan international. On notera par exemple qu'il faut dépenser une énergie folle pour amener un géant de l'Internet à payer une amende dérisoire par rapport aux bénéfices tirés de l'usage fait des données personnelles ! Certes, la bataille des instances de régulation pour maîtriser les dérives des moyens de CRM (*Customer Relationship Management*) n'est pas perdue. Face au lobby intense déployé par le GAFA (Google, Apple, Facebook, Amazon), le Parlement Européen vient d'adopter un projet de règlement apparemment très musclé :

- pouvoir de sanction accru (jusqu'à 100 M€ ou 5 % du chiffre d'affaires mondial) ;
- droit à l'oubli permettant à tout citoyen d'exiger l'effacement de ses données personnelles ;
- durcissement du contrôle préalable en cas de transfert de données personnelles hors de l'UE ;
- dispositions contre la tentation de diluer les responsabilités des « *privacy data officers* ».


response & resources related to Target's data breach

Visit this page for regular updates and reliable information about our recent data breach, including all official company communications.

Target offers free credit monitoring & identity theft protection

to learn more and register for the one-year offer, click here

Ainsi, les usages des outils et services de CRM, très appréciés des vendeurs pour mieux cibler les clients, seront mieux encadrés. L'intrusion publicitaire en ligne aura des limites. On ne persuadera jamais facilement un responsable marketing de se discipliner en la matière, mais les juristes des entreprises responsables joueront au moins un peu mieux le rôle de garde-fou.

Mais une bataille gagnée (en apparence…) en cache d'autres. Prenons le VRM, par exemple (*Vendor Relationship Management*) : il vise, à l'inverse des CRM, à aider les clients à mieux cibler les vendeurs. Seront-ils payants ? Sinon, quel sera leur *business model* ? Débats animés sur la notion de consentement libre et éclairé de leurs abonnés en perspective …

Les données de 110 millions de clients de Target sont potentiellement piratées ? Qu'à cela ne tienne (*cf. illustration*), un an d'assurance contre le vol d'identité leur est offert ! Et que proposera le leader mondial du VRM lorsqu'il se sera fait prendre ses dossiers personnels sur deux tiers des Européens ?

A l'heure où l'Internet 3.0 et le « *Big Data* » explosent, une chose est sûre : un cheminement serein le long d'une « troisième voie » médiane porteuse de confiance exigera un effort accru des contributeurs de bonne volonté : travail, cohérence et vigilance, nous l'avons noté. Et aussi beaucoup d'écoute, tant interne aux organisations que vis-à-vis de l'extérieur !

Pour aller plus loin :

- www.oecd.org/sti/security-privacy : site de l'OCDE, qui anime le débat entre Etats membres sur les enjeux économiques et sociétaux de l'économie numérique. Quelques publications récentes : analyse des stratégies nationales de cybersécurité, décrivant leur tournant vers l'intégration croissante des questions de souveraineté en plus des aspects économique et sociaux (2012) ; enjeux socioéconomiques du « *Big Data* » (2013).
- VRM, du concept au marché (rapport de 2010 en ligne sur le site d'Altran)
- www.wishbox.fr (service de VRM).

Cyber… Cerbères ? Tout change… rien ne change

L'informatique est, partout, connectée. La cyberdéfense, ou lutte informatique, n'est finalement que la forme que doit prendre la défense, sans pour autant changer fondamentalement les approches stratégiques. Ce qui est nouveau, c'est qu'il s'agit d'informatique et de réseaux (mais pas seulement), mais la réflexion et les modes d'action devraient rester assez invariants pour la défense.

Cet article n'évoque rien qui ne soit déjà connu et ne vient rien cautionner.

Stuxnet, qui a attaqué les centrifugeuses utilisées par l'Iran dans son programme d'enrichissement d'uranium, relève d'une attaque « cyber-physique », une cyberattaque venant corrompre un processus de contrôle - commande portant lui-même sur une infrastructure physique, en l'occurrence des centrifugeuses.

Il y a eu deux attaques distinctes : l'une pour obtenir une surpression des centrifugeuses, l'autre pour obtenir une vitesse de rotation trop importante, aboutissant à une résonance. Les deux ont eu pour objectif de compromettre le processus de centrifugation et/ou d'endommager fatalement les centrifugeuses, mais ne visaient pas les mêmes modules de contrôle commande. C'est la deuxième qui a été publiquement plus largement révélée, peu après sa détection. Les attaquants n'ont semble-t-il pas spécialement cherché à la rendre indétectable.

Nous ne reproduirons pas ici la description technique des tactiques : pour passionnantes qu'elles soient, celles-ci sont finalement « spécifiques » d'une situation donnée et ont été largement publiées. Arrêtons-nous à quelques points génériques, de portée plus stratégique, eux-mêmes aussi largement commentés.

Les attaques n'ont pas immédiatement détruit les centrifugeuses, mais les ont empêchées de fonctionner normalement. Au vu de la complexité de l'attaque, il est raisonnable de penser que l'attaquant aurait pu les détruire. Il ne l'a donc pas voulu. Une cyber - offensive peut avoir des objectifs modulés.

La deuxième attaque a été détectée ; sa restitution montre qu'elle était effectivement assez aisément détectable. Etait-ce voulu (montrer sa force et dissuader), ce que laisse penser l'ensemble de cette opération, ou non voulu, ou indifférent ? Les jeux stratégiques sont à rebonds multiples, y compris et notamment à l'ère de la lutte informatique.

Le virus est « sorti de sa boîte », comme si c'était celle de Pandore, et s'est répandu au-delà de l'Iran … confortant la pertinence du terme « virus ». C'est un retour d'expérience un peu inattendu et donc riche, s'agissant d'un logiciel a priori circonscrit à des modules de contrôle - commande industriel, non connectés au monde ouvert de l'internet. Cela montre aussi, incidemment, que sauf à prendre des mesures particulières pour anniHiler sa propre création, l'attaquant n'est pas certain de pouvoir circonscrire et limiter son attaque.

Nous ne retournerons pas ici le couteau dans la plaie que constituent de ce point de vue tous les systèmes de type SCADA non sécurisés, construits sur des systèmes d'exploitation commerciaux dont on ne maîtrise pas le contenu.

L'attaque, sophistiquée, a été possible grâce à une compréhension, et donc une connaissance approfondie, quasi exhaustive, de la configuration technique du système attaqué, ce qui renvoie aux méthodes de renseignement de toutes sources, y compris et en premier lieu de sources ouvertes. L'attaque a certainement été testée avant l'opération, avec tous les paramètres des centrifugeuses, de leur contenu, etc. Il a donc fallu un environnement d'essais, avec des éléments réels ou simulés ; mais pour que des éléments simulés soient valides, il faut par ailleurs d'autres essais … La lutte informatique est loin d'être virtuelle et de se jouer dans le seul cyberespace.

Finalement, et cela renvoie à d'autres contributions sur la cyberdissuasion, une question essentielle est de savoir s'il y a des seuils dans les capacités d'attaques, si certaines sont réservées aux Etats, compte tenu des moyens à mettre en œuvre, ou si au contraire des « organisations », voire des « individus » peuvent y accéder. Est-on dans un paradigme symétrique ou asymétrique ? Dans une logique symétrique, on peut se dissuader, en préparant la guerre pour avoir la paix. Dans une logique asymétrique, on est attaqué sans pouvoir dissuader les fous ou les joueurs (à supposer qu'ils soient distincts), et on n'a pas d'autre issue que de faire la guerre, se défendre, et lutter. La leçon fondamentale de la stratégie moderne reste valide : on ne choisit pas son ennemi ; c'est lui qui nous désigne et on ne peut échapper à devoir se défendre.

C'est techniquement compliqué, complexe, car un moyen de surveillance et contrôle peut souvent être une voie de pénétration pour un attaquant.

On dit, expérience historique à l'appui, que les guerres font plus de victimes parmi les populations civiles que parmi les militaires. Mutatis mutandis, il ne faut pas rêver : la lutte informatique fera bien plus de ravages dans les infrastructures critiques civiles que dans celles des armées. Mais tout comme le mandat des armées est de protéger le pays, et donc les « civils », avec des moyens et actions militaires, il pourrait revenir à la défense de protéger activement, ou à tout le moins de contribuer à protéger, les infrastructures critiques civiles.

On a de longue date su, dans les différents centres techniques, étudier sur pièces les systèmes ou équipements étrangers pour en restituer l'architecture et les performances : de façon à s'en protéger ou les neutraliser… selon la situation opérationnelle. Des efforts considérables ont été consentis, dans la durée, dans les domaines les plus cruciaux (armements classiques comme nucléaires, détection et guerre électronique, etc.).

La lutte informatique n'échappe pas à cette logique, et n'est pas virtuelle : il faut disposer d'équipes multidisciplinaires, d'outils et de moyens d'essais eux-mêmes sophistiqués, etc. Ce n'est pas un choix, mais une nécessité.

Et pour conclure sur une pointe ironique, citons un fameux proverbe du far-west américain : si tu dégaines le second (ou, ce qui revient à peu près au même, si tu laisses l'autre dégainer avant toi), tu es mort. D'aucuns paraissent s'en être fait un principe d'action pour la lutte informatique.

par **Arnaud Salomon,**
ICA

Arnaud Salomon (X78, Sup Aéro), a successivement occupé des postes au Laboratoire de Vernon, à la direction des missiles et de l'espace à la DGA, aux ministères de l'éducation nationale, et de la recherche et de la technologie, puis, depuis le début des années 2000 dans l'industrie : CS Communication et Systèmes, Altis. Ses activités ont été consacrées, sous différentes formes, au management et à la technologie. Il est membre du conseil d'administration de la CAIA et Animateur du club sectoriel « Systèmes d'Information » auprès du Conseil général de l'Armement.

Audit de la sécurité des systèmes d'information (SI)

En principe le but d'un audit de SSI est d'apprécier si les risques dus au SI sont acceptables ; bien évidemment une « analyse de risques » préalable aura déterminé les risques acceptables et inacceptables et les mesures à prendre, techniques et non techniques, pour éliminer les risques inacceptables. L'auditeur appréciera donc si ces mesures couvrent correctement les risques et également si elles sont correctement mises en œuvre, avant de proposer quelques recommandations.

par
Jean-François Pacault,
IGA

Jean-François Pacault (X 65) a travaillé aussi bien au sein de la DGA – dans les constructions navales et dans l'électronique principalement – qu'à l'extérieur, collectivités locales, Délégation à l'aménagement du territoire, Service central de la sécurité des systèmes d'information. Son dernier poste, de 1999 à 2010, était au service du Haut fonctionnaire de défense et de sécurité du Ministère des Finances, en charge des secteurs de l'informatique et des télécommunications.

De la théorie à la pratique

En pratique, l'audit peut consister à vérifier si un corpus de règles est correctement appliqué ; ces règles sont bien sûr définies avec grand soin pour constituer une bonne approximation de l'état de l'art en matière de SSI ; les audits nécessaires à l'obtention d'un certificat fonctionnent évidemment sur ce modèle mais, comme le respect des règles - que les Anglo-Saxons dénomment joliment « *compliance* » - n'a jamais dissuadé un attaquant, le bon auditeur s'efforcera de ne pas rester prisonnier de ce catalogue. Avec cette précaution de bon sens, l'audit permettra non seulement d'obtenir le certificat convoité, mais atteindra son but premier, qui est d'être utile.

Sécurité et sûreté

La sécurité, c'est être à l'abri des attaques ; mais à quoi bon se protéger contre des attaques si une vulgaire panne ou erreur peut causer des dommages au moins aussi graves ? Les puristes expliqueront qu'il ne s'agit là que de sûreté et non de sécurité, mais en pratique bien des mesures à prendre sont efficaces à la fois pour la sécurité et pour la sûreté et il est souvent difficile, sans une analyse approfondie, de déterminer si un incident est dû à une malveillance ou à une panne. Par conséquent un audit « de sécurité » doit également prendre en compte la sûreté.

Et maintenant, « *De quoi s'agit-il ?* » (Foch)

Quels systèmes ou sous-systèmes va-t-on auditer ? Quelles en sont les limites physiques et logiques ? Quelle contribution apportent-ils à la sécurité et aux risques de l'ensemble du Système d'Information ? Et, à l'intérieur du périmètre à auditer, à quoi, organisation, personnel, locaux, quels matériels et logiciels, demande-t-on à l'auditeur de s'intéresser ? Remarquons au passage le pronom indéfini « on », car il faudra également être clair sur la personne qui fait exécuter l'audit : ce peut être le propriétaire du système à auditer, ou son utilisateur lequel peut être distinct du propriétaire par exemple pour des prestations externalisées ; ce peut être aussi une autorité extérieure, administrative ou professionnelle, qui impose l'audit à ses ressortissants. Enfin il faut être clair sur la profondeur des investigations que devra mener l'auditeur, souhaite-t-on par exemple des audits de code ou des tests d'intrusion ? Des obligations réglementaires peuvent dans certains cas fixer la profondeur des investigations, comme aussi les constituants qu'il faut auditer ; sinon c'est au commanditaire de les définir.

Après le quoi, le comment

Même quand il n'est pas demandé de vérifier la bonne application d'un ensemble de règles précis, l'auditeur comme l'audité ont intérêt à suivre un fil conducteur, et fort heureusement il n'en manque pas.

Parmi les systèmes de règles simples – simples à énoncer, du moins – on trouve notamment les 40 mesures d'hygiène de l'ANSSI et les « *20 controls* » du SANS Institute. L'auditeur examinera lesquelles de ces mesures sont prescrites, la pertinence et l'efficacité des règles et moyens utilisés pour les appliquer et ce qui en est réellement de leur application. Pas de référence, dans ce cas, à un quelconque niveau de risque : il s'agit de mesures de base qui assurent une sécurité minimale.

La série des normes ISO 2700x est mieux adaptable à différents niveaux de sensibilité et s'impose progressivement comme la référence pour le management de la SSI ; le COBIT comme l'IT-Grundschutz et l'appréciation des risques informatiques dans la profession bancaire s'en inspirent maintenant largement. À noter que la norme 27001 peut déboucher sur la certification ; 70 organismes français ont été certifiés en 2012, soit un peu moins qu' en Thaïlande.

Pour les administrations américaines, le système FISMA (*Federal Information Systems Management Act*) est d'application obligatoire ; il renvoie aux documents techniques FIPS édités par le NIST (*National Institute for Standards and Technology*), dont le SP 800-115 pour les aspects techniques.

Autre référentiel d'application obligatoire, pour les téléprocédures et échanges de données des administrations françaises (ordonnance du 31/12/2005), le Référentiel Général de Sécurité ; les systèmes visés par cette ordonnance doivent être qualifiés par l'ANSSI ; les excellentes règles du RGS peuvent fort bien servir de fil conducteur pour auditer des systèmes qui ne sont pas dans le champ de l'ordonnance de 2005.

Certaines professions aussi imposent l'application de règles qui leur sont propres, notamment :

- la *North American Electric Reliability Corporation* (NERC) qui a promulgué une centaine de règles ; l'application en est obligatoire aux Etats-Unis dans la profession sous peine d'amende et des programmes d'audit détaillés existent pour « garantir la compliance » ;
- l'industrie des cartes de paiement (*Payment Card Industry Data Security Standard, PCI-DSS*) classe dans une douzaine de catégories les mesures à prendre pour « protéger les données du porteur de carte (nom, numéro de compte…) et les données d'authentification (code secret…) » ; il est décliné par chaque marque de cartes (Visa, Master Card, etc.) qui se charge de faire appliquer la compliance par les commerçants et fournisseurs de services avec qui elle travaille.

Comment cela se passe-t-il ?

Quelques points majeurs doivent être précisés à l'avance :

- la confidentialité des informations recueillies et créées au cours de l'audit ;
- les responsabilités en cas de dommage au système audité, par exemple au cours des tests d'intrusion ;
- les actions que l'auditeur ne pourra pas entreprendre sans autorisation expresse de l'audité, notamment au cours des tests d'intrusion ;
- la conduite à tenir en cas de découverte de délits.

Statue de Cassandre aux Tuileries (J.-F. Pacault)

Passons, parce qu'elles sont bien spécifiées dans nombre de documents, sur les étapes de l'audit et sur les procédures qui règlent les rapports entre auditeurs et audités ; ces procédures sont bien sûr rigoureuses, aussi bien pour fixer les responsabilités des deux parties que pour préserver un minimum de sérénité dans une aventure qui peut devenir un peu tendue.

Et remarquons – ce qui est, tout compte fait, rassurant – que le meilleur corpus de règles ne dispensera pas l'auditeur de faire preuve de compétence, certes, mais aussi d'imagination, de bon sens et certainement de tact, pour ne pas froisser les audités et conserver leur coopération.

Quis auditoret auditores ipsos ?

Excellente question, même si elle est posée en latin de cuisine, car les auditeurs doivent être compétents, cela va encore mieux en le disant, et ils doivent être de confiance.

La première qualité n'est déjà pas toujours facile à mesurer, mais on y arrive : un bon millier d'auditeurs ISO 27001 ont ainsi été accrédités en France et l'ANSSI vient de publier (14/2/2013) le référentiel d'exigences applicables aux prestataires d'audit de SSI ; ceux qui y satisferont seront « qualifiés » et les audits qu'ils réaliseront sur les systèmes soumis à l'ordonnance de 2005 précitée seront pris en compte pour la qualification de ces systèmes.

La confiance est encore beaucoup plus difficile à apprécier objectivement. Un point abordable et fondamental, cependant, est la qualité de l'organisation de la sécurité de l'auditeur, dont il faudra convaincre le client. Arrêtons nous avant d'enclencher la « récursion » qui exigerait qu'elle soit elle-même auditée.

À l'attaque !

Bien conduites, les attaques sur les systèmes d'information pourraient certainement être ravageuses. D'où l'évocation d'un « Pearl Harbor numérique », rebaptisé « 11 septembre numérique » après 2001 et devenu depuis « Cyber 11 septembre ». Tout récemment le Financial Times nous apprenait, que « la [cyber]menace et celle que posent les armes nucléaires sont similaires » et que « la cyber-délinquance menace le système financier mondial ». « *Be afraid, be very afraid* » comme on dit Outre-Manche.
Mais au fait, qu'en est-il de ces attaques ? Distinguons celles que l'on connaît, parce qu'elles se sont produites, ont été découvertes et expertisées, de celles que l'on juge possibles ; au-delà, les rêves les plus fous peuvent se donner libre cours.

Les attaques connues

C'est un fait que les vraiment bonnes attaques ne sont connues que si leurs auteurs les dévoilent, par gloriole, par maladresse, ou, par exemple, pour appuyer une revendication ou une politique. Avec cette précaution à l'esprit, on constate d'abord que les virus très contagieux de jadis se font rares, ceux qui, à grand tapage, infectaient la planète en quelques jours et remplissaient de fierté leurs auteurs. Les motivations qui demeurent, éternelles comme la nature humaine, sont l'appât de l'argent mal acquis, l'idéologie (les « hactivistes »), la politique, l'espionnage étatique et industriel ; le cyber-terrorisme, aux effets peu discrets par nature, n'apparaît toujours pas. En tout cas les attaques sont devenues ciblées, qu'elles soient bruyantes comme le déni de service ou silencieuses comme les APT (*Advanced Persistent Threats*), apparues récemment et bien adaptées à l'espionnage et au sabotage discrets. Une évolution notable a eu lieu, enfin, parmi les gens qui réalisent ces attaques : on repère maintenant, outre des mercenaires qui travaillent pour autrui, des services étatiques qui se dévoilent, maladroitement ou volontairement – toutes choses inouïes il y a une dizaine d'années.

par
Jean-François Pacault,
IGA

Un aperçu de ces attaques

- l'incontournable ver Stuxnet, découvert à l'été 2010 et qui envoyait des commandes aberrantes aux centrifugeuses iraniennes et des mesures normales aux postes de contrôle ;
- le ver Flame, découvert en 2012 mais actif semble-t-il depuis 2007, qui visait également l'Iran, à des fins suppose-t-on de recueil d'informations en préparation de Stuxnet ;
- l'espionnage d'un grand industriel américain, bien décrit dans un rapport de Northrop-Grumman de 2009 ;
- au début des années 2000, l'écoute téléphonique de hauts responsables politiques grecs, par piégeage d'un central téléphonique de Vodaphone ; dans leur zèle à faire cesser ce scandale, les employés de Vodaphone ont malheureusement effacé toutes les traces et, pire encore, le principal témoin s'est suicidé peu après.

Quelques attaques qui pourraient être

Il faut bien sûr citer toutes les révélations d'Edward Snowden sur les activités de la NSA : il s'agit en effet d'attaques vraisemblables, bien qu'aucune preuve ne les étaye à ce jour – ce qui est peut-être simplement un signe de la grande habileté de ces attaquants. Les modus operandi ainsi dévoilés donneront certainement des idées à des gens malintentionnés.
La faisabilité d'attaques sur les processus de contrôle industriel a été amplement démontrée en laboratoire, sans qu'elles aient besoin pour réussir d'être aussi sophistiquées que Stuxnet ; fort heureusement à ce jour, les attaques réelles sont restées très rares, au point qu'on en est réduit à citer le sabotage d'une usine de traitement des eaux usées de Sydney il y a une quinzaine d'années. Le lecteur intéressé pourra avantageusement se reporter aux actes du congrès C&ÉSAR 2013 organisé par DGA-MI.
Plus exotique, on parle d'un nouveau virus incurable à ce jour, Badbios, qui s'attaque au BIOS, ce composant programmé – et reprogrammable – qui assure entre autres le démarrage des ordinateurs ; qui plus est, Badbios organiserait des transmissions par ultra-sons entre ordinateurs non connectés.
Enfin, des universitaires ont démontré qu'il est possible de piéger des circuits intégrés lors de leur fabrication ; leur démonstration porte sur un générateur de nombres aléatoires, ingrédient indispensable de toutes les fonctions cryptographiques qui en seraient donc affaiblies.

Les menaces

Les grandes catégories de menaces, c'est-à-dire les moyens par lesquels sont perpétrées les attaques, restent assez stables, mais les évolutions des techniques et des usages – comme la mobilité – offrent de nouvelles possibilités de les décliner. Parmi ces menaces on trouve notamment :
- les codes malicieux, qui depuis longtemps ne se limitent plus aux virus proprement dits ;
- les réseaux d'ordinateurs compromis (botnets), téléguidés pour effectuer par exemple les dénis de service ;
- les vulnérabilités et pièges des sites Internet ;
- les courriels piégés et « l'ingénierie sociale », qui sont souvent le meilleur moyen de s'introduire dans un système ;
- l'exploitation des erreurs de conception et de réalisation des logiciels, toujours pleines de possibilités ;
- l'écoute passive des communications, méthode traditionnelle toujours fructueuse, notamment avec le développement des réseaux sans fil ;
- la menace interne, largement médiatisée par les affaires américaines de Bradley Manning/Wikileaks et d'Edward Snowden/NSA/programme PRISM.

L'attaquant compétent sait bien sûr combiner harmonieusement ces menaces, mais ne donne pas de confiture aux cochons et adapte le niveau de ses attaques à celui des cibles : à quoi bon risquer de divulguer une attaque sophistiquée quand de vieilles recettes ont toutes chances d'être efficaces ?

P comme perspicacité, prophétie ou paranoïa ?

Un mot imprudent du président Reagan, à propos d'une implication libyenne dans un attentat, a amené la Libye à s'inquiéter de la qualité des machines de chiffrement suisses Crypto AG qu'elle utilisait. En 1991 et pour des raisons analogues, trafic chiffré apparemment connu d'autres pays, l'Iran, qui utilisait les mêmes machines, s'est également inquiété, au point d'incarcérer pendant un an le représentant local de Crypto AG et de ne le libérer que contre une rançon d'un million de dollars.
Il y a quelques années, une dispute a éclaté entre la société canadienne RIM et le gouvernement indien, à propos de l'assistant informatique Blackberry. Pourquoi diable Madame Clinton, ministre américain des affaires étrangères, est-elle intervenue dans cette affaire qui ne semblait pourtant pas concerner son pays ? Depuis les révélations d'Edward Snowden, ceux là même qui refusaient d'appliquer des mesures de sécurité élémentaire clament volontiers que tous les produits et services américains sont piégés ; le même soupçon plane d'ailleurs sur les produits chinois, comme l'explique le Congrès américain, et le gouvernement indien entame une enquête sur les produits de Huaweï et de ZTE.
La liste serait longue de ces attaques que l'on pourrait imaginer puisque, quand une attaque est possible, elle a déjà été faite, et quand elle est impossible, il suffit d'attendre assez longtemps pour qu'elle se réalise ; en attendant, elle peut fournir matière à un scénario d'exercice de crise informatique. La place manque, par conséquent, pour en aborder l'énumération, mais citons quand même, car il nous concerne peut-être, cet article d'un quotidien américain, vers 1992, affirmant que des virus avaient pénétré les systèmes irakiens « via des imprimantes piégées » ; il s'agissait probablement d'imprimantes Sagem.

Le rapport de Northrop Grumman : une attaque bien coordonnée

Après l'intrusion initiale, probablement via des courriels piégés, une première équipe a réalisé une cartographie exhaustive du réseau de la victime – appelons la N*** - et un recensement des fichiers intéressants.
Une copie de ces fichiers préalablement sélectionnés a été transportée par une seconde équipe, sans qu'il soit besoin de les ouvrir, vers sept serveurs d'exportation, choisis parmi ceux de N*** pour leur capacité et la qualité de leurs connexions vers l'extérieur. L'exportation proprement dite s'est déroulée sur quelques nuits, vers des serveurs extérieurs intermédiaires préalablement compromis chez des correspondants habituels de la victime, par exemple des universités. Le ballet des déménageurs était orchestré par quelques serveurs de contrôle - commande, réquisitionnés eux-aussi dans les systèmes de N*** et télécommandés de l'extérieur.
Quoique les préparations aient été discrètes, N*** avait néanmoins détecté des activités anormales et pensait, à tort, les avoir neutralisées ; ses ingénieurs n'ont pu réagir que grâce à une fausse manœuvre des attaquants au cours des opérations d'exportation.
Cette attaque illustre bien ce qu'en 1991 déjà on appelait la menace de haut niveau, « patiente et motivée, avec des équipes à plein temps et bien organisées, recherchant surtout le succès à long terme et la plus grande discrétion » (*National Academy Press, 1991 : Computers at risk, annexe E*). L'auteur de ces lignes était-il un prophète ou un praticien de la chose ?

VU SUR INTERNET : UNE MÉCANIQUE DÉLICATE

Le système TOR, développé sur crédits militaires américains, est un ensemble de serveurs sur Internet qui « anonymisent » et chiffrent les transactions de ceux qui l'utilisent, au grand dam de ceux qui ont mission d'intercepter le trafic Internet. Les esprits paranoïaques supposaient donc que TOR était piégé, par exemple par la NSA. Les révélations d'Edward Snowden indiquent que, sans piéger TOR, la NSA peut néanmoins accéder au trafic. Jugeons-en.
Par son monitoring général d'Internet, la NSA repère les utilisateurs de TOR, sans arriver à ce stade à percer leur anonymat, ainsi que les connexions de et vers les serveurs TOR. Elle redirige les utilisateurs TOR vers certains de ses propres serveurs, dénommés FoxAcid, qui y mettent en place des portes dérobées grâce à une bibliothèque d'attaques du nom de « EgotisticalGiraffe », en évitant soigneusement la détection par les anti-virus de la cible grâce une autre bibliothèque baptisée « DireScallop ». Cette redirection se fait grâce à un premier ensemble de serveurs, dénommés Quantum, judicieusement placé dans les réseaux des opérateurs de télécommunications (américains seulement ?) de façon à ce qu'ils répondent avant ceux à qui s'adressent réellement les internautes ; quand ils reçoivent une requête de la part d'un utilisateur TOR, ils le redirigent vers un serveur FoxAcid tout en se comportant vis à vis de l'internaute comme le site qu'il a réellement appelé. Ainsi infectés, les ordinateurs cibles n'ont bien sûr plus de secrets pour la NSA.
Une telle attaque n'est pas à la portée de n'importe qui, évidemment, puisqu'il faut :
- avoir des accords avec les opérateurs pour assurer une surveillance générale d'Internet – un travail considérable en soi – et pour mettre en place les serveurs Quantum ;
- développer et maintenir, avec une qualité industrielle, les bibliothèques EgotisticalGiraffe et DireScallop ;
- coordonner le fonctionnement de tous ces rouages subtils.

Ce que ce cybernuméro n'a pas dit :

Attention en traversant les articles, un numéro peut en cacher un autre

L'actualité c'est la LPM qui donne la priorité à une capacité permanente de commandement et de contrôle, qui sous-entend un accès certain et sans entrave à un cyberespace ; c'est la même LPM qui assimile curieusement les cyberattaques à des attaques contre le territoire national et qui contient des éléments de sécurité intérieure, signe que la frontière entre militaire et civil perd de sa netteté ; c'est la lente évolution du droit qui se prépare à rendre légales certaines attaques informatiques destinées à maintenir notre souveraineté ; c'est la découverte feinte de la large utilisation des informations qui circulent sur les réseaux ; c'est l'inscription dans les textes de la cybersécurité de la centaine d'opérateurs d'importance vitale, qui élargit le domaine de la défense.

Les enjeux se mesurent par le fait que dans les départs des IA vers l'industrie, la cyberdéfense est depuis 5 ans la deuxième spécialité après le nucléaire ; par le nombre de rapports et de colloques ; par les conséquences des faiblesses, qu'il s'agisse d'enrichissement d'uranium, de la continuité des services de l'Etat ou d'incidents notables chez de grands industriels ; par la mise en service récente et progressive du « *Utah data center* » de la NSA capable d'enregistrer des exaoctets mais dont semble-t-il les installations électriques, elles-mêmes tributaires des réseaux – ou plus probablement d'une complexe mise en système – , ne sont pas encore fiabilisées.

Les raisons de ce qui manque dans ce numéro sont simples ; laissons au lecteur le soin de compléter lui-même son propre exemplaire, en lui donnant quelques pistes.

Réflexions à la carte

Les cas concrets d'exercices opérationnels où l'intervention de « rouges » (c'est-à-dire de l'équipe qui joue le rôle d'adversaire) provoque des dégâts sur la maîtrise des échanges entre commandements, et surtout les contre-mesures prises, n'ont bien sûr pas à être divulgués.

Les missions et plus encore les moyens des grandes entités qui, chacune dans son rôle, assurent une partie de la cyberdéfense, part primordiale de leur mission, resteront évidemment tues : DRM, DGSE, DCRI qui devient DCSI. Et un organisme comme la DGSE est encore moins enclin à évoquer sa coopération avec ses homologues étrangers, théoriquement inexistante mais dévoilée par un célèbre « *whistle blower* » américain. De même, les OIV, Opérateurs d'Importance Vitale, sont peu prolixes sur leurs précautions internes qui seront soumises à audit et à contrôle.

Les stratégies et programmes d'adaptations des SIC à l'évolution de la cybermenace, qui découlent du Livre blanc et de la LPM, posent des questions de nature nouvelle, à la fois techniques (DGA/MI – maîtrise de l'information –, ex-CELAR, est pilote mais n'est pas le seul), contractuelles (une adaptation vivante demande un marché vivant et peu ou prou des marchés liés, ce qui est interdit par le code des marchés publics) et d'organisation (sans confiance réciproque, il y aura des doublons incompatibles).

Les actions internationales de prévention, de protection et d'échange, parfois mises en avant, sont en fait très limitées : un exercice multinational piloté par l'Estonie, un engagement sans suite dans les accords franco-britanniques de Lancaster House, une tentative d'harmonisation des besoins d'en connaître dans les échanges de situation tactique maritime méditerranéenne du projet *BlueMassMed*, et peu d'autres.

Le rôle des sociétés, en complément de l'Etat, dans la connaissance, l'accès aux données et la protection des données a souvent été démenti, alors qu'il est évident aux Etats-Unis que la Défense ne peut pas se passer des services et des avis de Microsoft, et réciproquement.

La tentation est grande, dans les opérations extérieures, de choisir soi-même au niveau des petites unités sur le terrain le compromis entre la réactivité et la sécurité informatique, en n'imaginant même pas que les entreprises puissent légitimement faire de même.

On se souvient du système de téléphonie mobile Bi-Bop du début des années 1990, dont les zones de couverture réparties dans Paris étaient (et sont encore) repérées sur les réverbères par des adhésifs bleu et vert, et qui a été abandonné, certes pour des raisons techniques, mais aussi parce qu'il ne permettait pas de localiser les utilisateurs…

Les comparaisons internationales, en termes d'effectifs, de moyens techniques et juridiques sont peu disponibles. Ce qui est encore plus incertain, c'est une éventuelle coopération européenne visant à rechercher une sorte de souveraineté, opérationnelle ou industrielle, à 28 – ce qui est totalement irréaliste – ou à moins, ce qui reviendrait à échapper à la mondialisation d'un système qui justement a été fait pour cela, et donc à poursuivre une étanchéité chimérique. Le cadre d'une politique européenne de cyberdéfense, promis pour 2014, et la feuille de route, annoncés lors du conseil européen du 20 décembre, risquent fort de se limiter à de bonnes intentions.

Le cybermonde s'étend, pour atteindre maintenant la machine à café alors que les militaires cherchent à le circonscrire, et sa vulnérabilité est à la mesure de son omniprésence … et il ne s'agit même pas de la surveillance des données, qui pourrait à elle seule être le thème central d'un numéro de notre magazine.

« Il y a en chacun de nous un enfant de chœur qui sommeille, laissons-le dormir »

En bref, la cyberdéfense comme toute défense exige une protection du secret, mise en évidence par ce qu'on n'a pas dit. Les acteurs développent des matériels de guerre qui ne disent pas leur nom, et il est normal qu'ils ne soient pas décrits et que les limitations à leur usage et à leur développement ne soient pas précisées a priori.

Curieusement, l'étymologie indirecte du cyberespace contient une notion de pilotage, alors qu'on ne pilote rien du tout : par le jeu des réseaux et de la complexité, seuls les outils de pilotage sont là, mais le contrôle a disparu. Nous rêvons que le cyberespace mérite de nouveau son nom. Pour cela, la solution est un peu technique et surtout largement humaine. Sans aller jusqu'aux temps prochains où le cyberespace fera partie de nous-mêmes, chacun doit se comporter en fonction des règles, des risques et des possibilités. Le monde devient là aussi de plus en plus complexe. C'est bien pour ça qu'il y a des IA, non ?

par
Denis Plane,
IGA

« Arrivé au terme de ce numéro, le lecteur sera peut-être déçu : les enjeux sont considérables et d'actualité mais les cas concrets sont absents ».

Mot du président

par
Philippe Roger,
IGA
Président de la CAIA

Chers Camarades,
Mes meilleurs vœux, maintenant chinois, aux 1787 d'entre vous qui ne les ont (hélas !) pas reçus avec l'annuaire diffusé fin décembre (bravo !) à nos 1071 (ce n'est qu'un début !) cotisants 2013.
Que l'année du Cheval les encourage à miser sans attendre 50 euros sur les chances de la CAIA !
Nous sommes en effet au travail, j'allais dire au turf, sur quelques sujets qui méritent votre solidarité :
- le sort de l'X, de l'ENSTA, et du lien X-écoles d'application, sujet sur lequel vous avez été nombreux à répondre à mon appel mi-décembre, et qui reste en évolution, pas forcément favorable, du fait de l'Administration mais aussi du fait du Parlement ;
- la compétence des IA et leur employabilité hors DGA, sujet actuellement traité par le groupe de Jean-François Pacault, et qui risque d'évoluer défavorablement avec les nouvelles baisses d'effectifs de la DGA, qui menacent les centres d'essais ;
- l'évolution du haut encadrement de l'Etat, qui vient de faire l'objet d'une demande de rapport, demande prenant place dans la théorie interminable des occasions de proposer fusions et réductions aux Corps Techniques sans toucher jamais aux autres Corps de l'Etat.

Sur ces trois sujets, nous ne sommes pas à l'abri d'un coup de chance, mais encore faut-il être au départ et cravacher, et, pour ceux qui n'en ont pas le temps, faire quand même nombre avec nous en cotisant.
Nous ferons le point lors de l'AG du 3 avril plus particulièrement sur le deuxième sujet, sous forme d'une table ronde, et sur les deux autres dans mon laïus, où je vous demanderai aussi de bien vouloir reconduire notre équipe CAIA, non pas à l'écurie, mais pour un an.
D'ici là, ceux qui s'intéressent au premier sujet sont vivement invités à envoyer leurs commentaires sur l'évolution depuis décembre à Patrick Gerlier, sur un mail ad hoc qui porte courageusement le nom de page74010-xta@yahoo.fr ; Patrick exploite les mails reçus en décembre, puis formera un groupe de travail pour fonder au mieux notre position.
A bientôt sur les autres thèmes récurrents, Gala, Site, Annuaire, Magazine, Convention, dans le rapport moral à venir, mais, en attendant, intéressez-vous de près à la cyberdéfense, comme mes collègues Captains, Archibald et …, mais au fait, quel est le prénom du Captain Cap ?

Amicalement.
Philippe Roger

Le Captain Cap' :
- Garçon ! Un ShortMag CAIA bien tassé s'il vous plaît !

Le Garçon :
- Je n'ai plus de vodka, Monsieur Allais.

Le Captain, légèrement irrité :
- Garçon, vous êtes un ignorant, je ne vous demande pas un cocktail russe, mais cette revue distribuée au 5ème Forum International de la Cybersécurité, dont j'attendais merveilles, mais qui s'est arrachée avant mon arrivée. Mon collègue le capitaine H. ici présent doit la consulter aussi.

Le Garçon :
- Ah ! J'en ai une ! Je vous la prête mais elle s'appelle « reviens ! ». On vient de me phisher mon mot de passe pour mes recettes de cocktails américains; je ne sais plus concocter de « Stars and Stripes » et mon business va à vau-l'eau. Il faut que je travaille ma défense.

Le Captain :
- On voit d'où vient le coup…
Je dois, quant à moi, cadenasser le texte de mon discours électoral : si mon adversaire l'infâme Colonel O. voit à temps que j'ai remplacé l'arasement de la butte Montmartre au niveau de Paris par l'exhaussement de Paris au niveau de Montmartre, programme bien plus créateur d'emplois et séducteur d'électeurs, je peux dire adieu à la mairie. Quant au capitaine H, si son adresse est publiée, la cantatrice C., qui le poursuit de ses assiduités, va arriver chez lui et alors… et alors… n'en disons pas plus !

Le Captain, après lecture :
- Bon, j'y vois plus clair !
- *La CAIA n'est pas une désinence russe, mais l'association des Ingénieurs de l'Armement, honorable corporation militaire dont sept cent membres gèrent les plus gros investissements de l'Etat, et qui couvre maintenant le domaine de la cyberdéfense, en plus des canons (les courts et les longs).*
- *J'écrirai mon discours dans la paume de ma main en montant sur l'estrade, c'est plus sûr, et ne sera affiché sur aucun mur.*
- *Je lirai dès février la version complète du magazine, après ce très utile apéritif…*
  Et à ce propos :

- (d'une voix maintenant parcheminée) : Garçon ! Ces « Corpse Reviver », ça vient ?

Le Garçon, échevelé, livide, etc. :
- C'était aussi dans mes recettes !
Tout mon savoir-faire est perdu !

Le Captain, apoplectique :
- Vos clients aussi !
- Archibald, mon ami, Moulinsart est un peu loin, mais le « Sirius » est toujours amarré Quai Suffren, n'est-ce-pas ?

Philippe Roger, PCC Alphonse Allais

Du nouveau pour les IA : la renaissance des clubs

Après quelques années de basses eaux, quelques clubs ont décidé de se relancer, à l'image des clubs « sectoriels » d'autrefois. Ainsi, depuis l'automne dernier, trois clubs sectoriels réunissent des ingénieurs et officiers des corps de l'Armement à la Pépinière sous la houlette du CGARM. Ils ont pour thèmes la reprise de PME, le conseil-expertise et les métiers de DSI – SSI, trois sujets qui peuvent permettre un rayonnement de nos activités.
Pour vous les présenter, passons la parole à leurs coordinateurs… ci-dessous.
Bien sûr, cette liste n'est pas limitative, et si vous vous sentez l'envie de faire quelque chose dans votre domaine de prédilection (banque – assurance, aéronautique, management de transition, Bercy, …) contactez la Section Carrières.

JDD

Le club DSI ou «Direction des Systèmes d'Information» est un lieu d'échanges sur ce thème, dont l'importance et l'intérêt ne sont plus à démontrer.
Au rythme d'une rencontre par trimestre, « et plus si affinités », nous évoquons, pour mieux les comprendre, les grands déterminants technologiques ou méthodologiques du domaine des systèmes d'information...et donc de facto désormais des systèmes de toute sorte puisque le traitement de l'information devient de plus en plus universel.
Nous avons naturellement en tête de traiter les cinq grandes tendances de la décennie que sont les mises en réseaux (networking), le « machine à machine » (internet des objets), la mobilité, le cloud computing, et les données massives (big data).
Et nous découvrons aussi des profils de compétences particulièrement intéressants parmi nos membres.

Arnaud Salomon,
Coordinateur du club DSI - SSI

Et si au lieu de général directeur vous envisagez de devenir directeur général ? Et pourquoi pas même président directeur général ... de votre propre société en devenant entrepreneur, et ainsi découvrir un vrai management naturel avec de vrais morceaux de commerce et de finances à l'intérieur ? Certains ont sauté le pas de la reprise d'entreprise et nous font régulièrement partager leur expérience lors des petits déjeuners du club PME du CGArm. Les principaux thèmes de la reprise y sont abordés. Lors de la dernière réunion, Louis le Pivain et Claude Chabrol, deux anciens ingénieurs de l'armement ont présenté à une assistance de 25 personnes leur entreprise sous l'angle de l'équation financière personnelle. Que vous ayez déjà un projet ou que vous souhaitiez simplement vous informer, le club PME est une bonne occasion de rencontrer d'autres camarades ayant ce même intérêt. Prochain événement en mai…

Philippe Girard,
Coordinateur du club PME

A l'heure de la reconversion, le conseil en tente plus d'un. Il offre l'opportunité de valoriser ses compétences et son expérience avec une grande liberté, en multipliant les cadres d'intervention. L'autre côté de la pièce est moins séduisant : difficile criblage de son offre, démarche commerciale permanente, solitude de l'exercice,... Le club conseil expertise permet de partager et discuter l'expérience entre praticiens candidats et confirmés du conseil, de relativiser les difficultés et de communiquer l'enthousiasme. La formule des petits déjeuners thématiques répond bien à ce besoin. Deux petits déjeuners rassemblant une vingtaine d'IA ont déjà eu lieu, le premier avec trois témoignages (D. Reydellet, D. Kechemair et OP Jacquotte) et une approche méthodique de la définition de son offre de consulting basée sur son expertise, présentée avec brio par Didier Cohen. Un prochain rendez-vous sera programmé très bientôt.

Jacques Roujansky,
Coordinateur du club Conseil - Expertise



par **Flavien Dupuis,** IA

Statut du corps, le débat continue

Comme l'a rappelé Alain Crémieux dans un précédent numéro, le corps de l'armement souffre d'un déficit de rayonnement évident. Pour autant, cela est-il dû uniquement au statut militaire et aux limitations de droits civils qu'il entraîne ? La réponse n'est pas aussi limpide qu'il y paraît…

Flavien Dupuis (X 2006, Supaéro 2011), travaille actuellement au Centre d'Analyse Technico-Opérationnel de Défense (CATOD) à Arcueil, dans le domaine des systèmes de renseignement.

La perspective d'une réforme des statuts des officiers de l'armement suscite actuellement de nombreuses réactions, parmi lesquelles celle d'Alain Crémieux, qui a dressé dans le précédent numéro la liste des avantages et des inconvénients liés à un éventuel passage sous statut civil. Dans un esprit de discussion constructive, et sans la moindre arrière-pensée polémique, je souhaiterais, en tant que « jeune » qui a choisi la voie de l'armement, réagir à certaines idées évoquées dans cet article.

Je ne m'étendrai pas sur les avantages matériels liés au statut militaire, qui ont été rappelés avec justesse et exhaustivité par Alain Crémieux, sauf pour dire qu'ils procurent aux officiers de l'armement une souplesse et une liberté qui sont indissociables d'une certaine sérénité dans l'orientation de carrière. Ils ne sont pas contestables, et jouent souvent pour une part non négligeable dans la décision de rejoindre le corps.

Mais le statut militaire est bien plus qu'un agrégat de dispositions matérielles ou honorifiques. Il symbolise l'adhésion à une certaine idée du service de l'Etat, qui subsiste encore aujourd'hui dans l'esprit de ceux qui choisissent la voie de la défense. Il impose à celui qui le porte, qu'il soit ou non combattant, des impératifs déontologiques, ainsi que des exigences de tenue et de comportement qui n'existent dans aucune autre profession. Enfin, il relie entre eux tous ceux qui ont décidé de se mettre, directement et entièrement, au service de l'effort de défense national. Les ingénieurs de l'armement en activité à la DGA, parce qu'ils assurent l'équipement matériel des forces, participent pleinement à cet effort au même titre que d'autres corps non combattants comme les commissaires aux armées ou les médecins militaires.

Comme l'a rappelé Alain Crémieux, le statut militaire créé une symbiose entre officiers de l'armement et officiers des armées. Loin d'être mineure ou vouée à disparaître, cette symbiose me semble au contraire fondamentale. Bien plus que la manifestation d'une communauté de langage ou de tradition, elle rend possible l'immersion des jeunes officiers dans l'environnement militaire dès leurs premières années de formation (stage de formation militaire initiale ou FAMIA, entre autres). Ces différents stages donnent aux futurs ingénieurs de l'armement une connaissance technique et humaine des armées qui est exceptionnelle parce que vécue de l'intérieur, et que n'égaleront jamais toutes les visites officielles et autres « journées portes ouvertes ». Ce passé opérationnel constitue en outre un référentiel dans lequel l'ingénieur de l'armement puisera tout au long de sa carrière. Au-delà de ses vertus pédagogiques, cette symbiose instaure également une relation de confiance très sécurisante entre les représentants des forces et les hommes chargés de leur fournir les moyens de leurs missions. Dans ce jeu à trois que constitue la passation d'un marché d'équipement de défense, l'officier de programme sait de quel côté se trouve la DGA. Enfin, aussi loin que ma courte expérience professionnelle m'en donne le droit, je puis témoigner que cette symbiose est accentuée dans une mesure d'autant plus large que les officiers des armées n'ignorent pas que les ingénieurs de l'armement sont pour la plupart d'anciens élèves de grandes écoles ayant renoncé à des carrières potentiellement plus lucratives pour se mettre, comme eux, au service de la France et de sa défense.

Macaron_officier_armement

DGA-CNE

DGA-CEN

DGA-LCL

L'argument selon lequel la restriction des droits civiques aurait empêché les ingénieurs de l'armement d'accéder à la « classe dirigeante » me surprend, mais après tout ma faible expérience du domaine ne m'autorise guère à avancer plus loin sur ce terrain. Je me bornerai à dire que ni l'interdiction d'adhérer à un parti politique ou de se constituer en syndicat, ni le respect du devoir de réserve ne me semblent avoir jamais empêché quiconque de se constituer un réseau, de cultiver des appuis, de fréquenter des clubs, bref, d'emprunter les voies classiques qui rapprochent des sphères de décision. D'autre part je ne crois pas qu'un haut fonctionnaire ait eu spécifiquement besoin de prendre sa carte d'un parti ou d'adhérer à un syndicat particulier pour être nommé à la tête d'une entreprise publique.

L'idée que ce sont ces mêmes restrictions qui auraient empêché les ingénieurs de l'armement de participer à la vie politique locale me laisse également perplexe. L'argument s'applique plutôt bien aux responsabilités politiques nationales, pour l'exercice desquelles l'interdiction d'adhérer à un parti constitue effectivement un handicap quasi impossible à surmonter, mais pour le reste ? Le nombre considérable de maires ou de conseillers généraux « sans étiquette » (20 % des maires de France, soit plus de 7 000 élus, ne sont pas affiliés à un parti politique) prouve bien que l'implantation locale est souvent tout aussi importante que la couleur politique. Quant à la perte de revenu engendrée par la mise en détachement, elle peut être compensée par les diverses indemnités de fonction ou de représentation versées aux élus locaux, voire par la retraite que les ingénieurs de l'armement peuvent prendre passés seulement 15 ans de service. Qui sait d'ailleurs combien de temps encore le droit au cumul d'un traitement de fonctionnaire civil avec une indemnité de mandat électoral perdurera ? Ajoutons à cela le fait que la plupart des ingénieurs de l'armement travaillant dans les centres de province le font par réelle appétence technique, et que cette appétence s'accommode a priori assez mal du virus de la politique.

Pour autant, le constat de départ sur lequel se fonde Alain Crémieux est juste : le corps de l'armement ne rayonne pas assez. Mais plus que les restrictions de droits, c'est bien plutôt la nature de l'activité qu'exercent les ingénieurs de l'armement ainsi que la façon dont cette activité est perçue par l'extérieur que je placerais en tête des raisons de leur éloignement des grands cercles de décision. Il est normal qu'un ingénieur des ponts travaillant à l'équipement départemental soit amené, dans le cadre de son activité, à côtoyer le préfet puisque celui-ci est le chef des services déconcentrés de l'Etat dans son département. Tel n'est pas le cas pour un ingénieur en poste à la DGA, dont l'univers professionnel immédiat offre très peu d'occasions de contact avec le monde politique, et ce quel que soit le stade de carrière. Cette faible visibilité entraîne un manque de reconnaissance effectivement dommageable à l'image du corps de l'armement. A nous désormais de montrer que les ingénieurs de l'armement peuvent surmonter ce handicap tout en restant fidèles à l'esprit du corps. Ils peuvent pour cela s'appuyer sur deux éléments de circonstance nouveaux.

Le premier élément est la vocation résolument technique du corps de l'armement, dernier grand réservoir de compétence de l'Etat à avoir conservé ses aptitudes de gestion de projet de systèmes complexes à forte valeur ajoutée technologique. Cette compétence rare est éminemment transverse, et peut largement être transposée du monde de la défense où elle s'applique encore majoritairement aujourd'hui, à une industrie civile dont l'histoire montre que le développement s'est largement appuyé sur les progrès des sciences et techniques militaires. Il y a fort à parier qu'en cette période où les pouvoirs publics font de la réindustrialisation du pays un objectif majeur, cette compétence discrète finira par attirer sur elle l'attention des hauts décideurs, pour peu que le corps sache communiquer sur ses atouts.

Le second élément est l'évolution des choix de spécialisation formulés par les élèves de l'X partant dans les corps de l'Etat. Une correspondance de plus en plus forte se dessine actuellement entre les secteurs d'avenir de la défense et les desideratas académiques des polytechniciens, qui se détournent de certains domaines classiques comme les télécommunications ou l'équipement civils pour partir se former à la cyberdéfense ou à la conception des systèmes de drones par exemple. Cette attractivité nouvelle laisse augurer un recrutement de qualité ainsi qu'un rééquilibrage des positionnements relatifs du corps de l'armement par rapport aux deux autres grands corps techniques que sont le corps des Mines et celui des IPEF (ingénieurs des ponts et chaussées, des eaux et forêts). Il y a là une opportunité formidable pour démontrer que les ingénieurs de l'armement peuvent rayonner au-delà de leur cœur de métier et développer leur vocation interministérielle.

Enfin, il ne me paraît pas inutile de méditer le fait suivant : quand bien même le statut militaire aurait privé le corps des ingénieurs de l'armement du rayonnement que la qualité de son recrutement et la valeur de ses compétences aurait pu légitimement lui réserver, il faut alors admettre qu'il l'a également préservé du soupçon moral qui pèse aujourd'hui sur le reste de la haute fonction publique, accusée fréquemment de dérives oligarchiques et de collusions coupables. Pour si abusif que l'on tienne ce type de jugement, on ne peut pas méconnaître ni sous-estimer son impact sur l'idée que le pays se fait des serviteurs de l'Etat. Les ingénieurs de l'armement sont-ils prêts à courir le risque de s'exposer aux tentations qui ne manquent pas de se présenter à ceux qui s'approchent des charmes du pouvoir ? En vérité, pourrait-on trouver meilleur garde-fou déontologique que l'exigence de probité et d'intégrité qui s'attache à la condition d'officier ?

DGA-COL

DGA-BRI

DGA-GDI

DGA-GCA

DGA-GAR

par **Jérôme de Dinechin**, ICA

Jérôme de Dinechin est coach, et responsable de la Section Carrières du CGARM

Pour quoi suis-je donc fait ?

Les personnes que nous rencontrons à la Section Carrières, principalement des ingénieurs, sont nombreuses à se poser la question de leur « vocation professionnelle ». La question, lancinante, ressemble souvent à un « mais pour quoi suis-je donc fait ? » et s'accompagne d'une sorte de découragement : « tout le monde doit se poser la même question, non ? »
Et si elle était plus que cela ? C'est ce que je vous propose d'explorer ci-dessous.

Il est facile d'identifier autour de nous des personnes qui « sont bien » dans leur métier, et d'autres non. Ceux qui « sont bien » regorgent de vie, mènent plusieurs activités de front, éprouvent une saine fatigue mais récupèrent vite, et rayonnent autour d'eux. Les autres sont comme éteints, brûlés de l'intérieur, se découragent dans leurs travaux, sont souvent dans le questionnement du sens : « à quoi bon ? ». Vers le milieu de la vie, ils vivent un besoin urgent de changement et voudraient tout recommencer à zéro.

Avons-nous des « meilleurs talents » ? Nous possédons en général de nombreux talents, et si nous avons fait de hautes études, on pourrait presque dire que nous en avons plus qu'il nous en faut. Un ingénieur sait par exemple mettre en œuvre des calculs complexes, estimer les apports et difficultés de nouvelles technologies, diriger un projet en assumant des risques multiples, manager des équipes, assumer des risques, se confronter à des intérêts différents des siens y compris en milieu international, etc…

Pourtant, va-t-il ressentir le même goût pour chacune de ces activités ? Il est probable que non. Une fois passé l'intérêt de la nouveauté, elles auront une influence différente sur lui : certaines le nourriront, d'autres le dessècheront. Pour ma part, et comme vous peut-être, j'ai cru qu'apprendre justifiait de faire des choses que je n'aime pas. Ou qu'il était important de se contraindre pour mériter. Ou que pour réussir, il fallait être ambitieux. N'est-il pas plus simple de mettre en œuvre en priorité les talents qui nous nourrissent ?

Mais nos meilleurs talents ne sont pas là par hasard. Ils cherchent à s'exprimer dans un « service ». Sans revenir sur les neuf niveaux du sens que je vous invite à creuser dans l'excellent ouvrage « les responsables porteurs de sens » de Vincent Leenhardt, nous trouvons en général le maximum de satisfaction personnelle lorsque nous participons à une œuvre. Cette œuvre peut être le service de son pays, de son entreprise, de sa communauté, etc…

Comme aimait à le rappeler Victor Frankl en citant Nietzsche, « Celui qui a un pourquoi qui lui tient lieu de but, de finalité, peut vivre avec n'importe quel comment »

Comment trouver notre service ou dit autrement, notre « vocation professionnelle » ? Je vous propose de le chercher du côté de notre intuition profonde. Au cœur de notre personne en effet, se trouve notre inconscient, qui a fait l'objet de bien des découvertes et des théories. Le principe de cet inconscient, c'est qu'il ne se laisse pas attraper facilement par notre conscient ! A titre d'exemple, demandons-nous à quel âge remontent nos premiers souvenirs.

Wilder Penfield, neuropsychiatre canadien, s'est rendu célèbre dans les années 50 en implantant des électrodes dans le rhinencéphale de ses patients, souvent à leur insu. Leur stimulation déclenchait des crises émotionnelles attachées à des souvenirs de la prime enfance, et totalement oubliés, voire refoulés : un jouet cassé, la peur d'avoir été abandonné, une injustice... Réservoir de nos « refoulements » et autres expériences oubliées, notre inconscient contient également notre identité profonde avec sa dimension de gratuité, de soif d'absolu, de mission, …, ce que Jung appelle le « Soi » ou l' « imago dei ».

Sans aller jusqu'à l'électrostimulation, je vous propose trois méthodes pour essayer de mobiliser votre inconscient pour qu'il vous aide à déterminer à la fois vos meilleurs talents et le service auquel vous êtes appelé.

Les rêves qui nous ont enchanté

Tous les petits garçons veulent être pompiers, et les petites filles dresseuses de poneys.

Mais au delà de ces stéréotypes, nous portons des rêves d'enfant ou d'adolescent qui nous sont bien personnels. Tel voulait être explorateur, tel autre médecin, un autre encore ami universel, un autre peintre…

Ces rêves disent quelque chose de nos aspirations profondes.

Pourrions-nous essayer de nous replonger dans le temps, jusqu'à ressentir ce que nous avons souhaité ? Puis sur une feuille, décrire en quelques phrases les points importants de chaque rêve.

Une fois la description terminée, revenons aujourd'hui. Comment relisons-nous ces phrases ? Que signifient-elles en profondeur, de nous et pour nous ? Leur avons-nous donné une réalité dans tout ou partie de nos activités ? Pourquoi ? Aurions-nous envie de leur donner la liberté de le faire ?

Les expériences-sommets

On appelle « expérience-sommet » un moment où tout dans notre vie semble se mettre en cohérence. Comme un point d'orgue en musique, nous avons alors le sentiment que le temps s'arrête (1er critère), et que tout est comme cela doit être.

Dans cet instant, nous recevons aussi de la joie (2ème critère), et une envie de dire merci à quelque chose ou tout simplement à la vie.

On recherche particulièrement les expériences-sommets où l'on n'est pas tout seul. Bien sûr, un soleil levant est magnifique, mais il le sera d'autant plus que nous nous serons levé tôt et que nous aurons marché en cordée dans la nuit pour arriver au bon endroit au bon moment… Souvent, les personnes qui nous entourent à cet instant ressentent la même chose et nous témoignent de la gratitude (3ème critère). Ces expériences sont assez rares, typiquement une fois tous les cinq à dix ans. Pourtant, elles sont un puissant révélateur de nos meilleurs talents, ceux dont la mise en œuvre nous comblera.

Et pour nous, quelles expériences-sommets avons-nous vécues ? Je vous conseille de les décrire en quelques lignes, jusqu'à ce que la description soit suffisamment évocatrice, c'est-à-dire qu'elle rappelle une émotion. Puis dans un deuxième temps, de rechercher les talents mis en œuvre pour que cela advienne. Ensuite, de reformuler ces talents pour qu'ils puissent s'appliquer dans notre vie d'aujourd'hui.

Ce qui nous nourrit, ce qui nous pèse

Dans nos activités, nous savons bien ce que nous préférons, là où nous avons de la valeur ajoutée personnelle. J'ai l'exemple d'une personne qui se sent la vocation de meneur d'équipe en situation difficile. Ses meilleurs souvenirs sont ceux de challenges réputés impossibles et qu'elle a transformés en succès. Une autre dont le mot clef est « soigner », une autre « éclairer, expliquer ». Cela concerne les activités professionnelles bien sûr, mais aussi tous les domaines de notre vie. *Je vous invite à en faire la liste.*

Au contraire, d'autres activités me fatiguent au-delà de la normale. Les expressions populaires en parlent : « j'en ai plein le dos, c'est lourd à porter, ça me donne des boutons, … » *Et nous, aujourd'hui, qu'est-ce que notre corps veut nous dire de notre équilibre de vie ?*

Nous parlons ici de compétences acquises, celles que détectent les tests de bilans de compétences. Mais il se peut que dans notre histoire, certains de nos talents n'aient pas eu l'occasion de se développer : c'est l'exemple d'un enfant mélomane dans une famille sans culture musicale, d'un manuel dans un environnement intellectuel. Pourtant, ces talents sont présents en nous et ne demandent qu'à grandir. Ils nous apporteront beaucoup de joies si nous leur donnons la liberté d'éclore. *Y a-t-il des envies que nous portons depuis longtemps mais que nous n'avons pas eu l'occasion de développer ?*

Rendre son sens à ce que l'on fait

Au terme de ce questionnement, en reprenant les différentes listes évoquées ci-dessus, quel sens cela prend-il pour moi aujourd'hui ? Comment pourrais-je les vivre mieux dans mes activités actuelles ? Il se peut également que ma vie actuelle ne me permette pas d'exprimer ce que je sens pouvoir changer dans le monde… Alors quel(s) changement(s) effectuer dans ma vie ?

Bien d'autres approches convergentes avec celles-ci peuvent nous aider à déterminer notre service ou à lui rendre son sens. Progressivement, sa formulation va s'affiner : on reconnaît ce pour quoi l'on est fait ; on identifie quelle forme cela pourrait prendre idéalement ; on projette comment cela va se mettre en place dans un futur proche.

Connaître ses meilleurs talents et sa vocation professionnelle procure habituellement un sentiment de libération, comme si l'on se dégageait d'un destin pesant. Pour un ingénieur habitué à se conformer à une règle du jeu sans la remettre en cause, comme celle des études, des concours, ou des premiers jobs, c'est comme si le plafond s'ouvrait.

Bien sûr, le chemin n'est pas achevé pour autant. Pour celui qui est à l'arrêt, se mettre en mouvement revient à se confronter à une « inertie infinie ».

Il nous faut donc d'abord accepter cette vocation professionnelle, la (re)choisir.

Ensuite, agir en conséquence dans tous les compartiments de notre vie, que ce soit progressivement ou avec des ruptures pour nous en rapprocher.

Il est certain que ce choix entrainera des pertes et des renoncements, des critiques aussi.

En contrepartie, beaucoup d'aides se manifesteront le long du parcours, ainsi que l'a remarqué Goethe, « Il existe pourtant une vérité première dont l'ignorance a déjà détruit d'innombrables idées et de superbes projets : au moment où l'on s'engage totalement, la providence éclaire notre chemin. Une quantité d'éléments sur lesquels l'on ne pourrait jamais compter par ailleurs contribue à aider l'individu. »

Si vous m'avez lu jusqu'ici, y a-t-il quelque chose qui a bougé ? Quel que soit votre âge, il est possible de vous rapprocher de ce que vous êtes. Alors, pour quoi êtes vous faits ? Parlons-en.

par
Daniel Jouan,
IGA

Les pigeons voyageurs : une protection contre l'interception ?

L'utilisation de pigeons voyageurs pour transporter discrètement de l'information avec peu de risques d'interception remonte à la plus haute antiquité. La France y a recouru pendant les dernières guerres. Mais l'ère de l'électronique verra peut-être la fin de ce moyen sympathique de correspondance guerrière.

Dans une question écrite posée au Ministre de la défense en 2012, un parlementaire français s'est ému de ne plus voir qu'un seul colombier militaire dans les Armées françaises, situé au Mont Valérien. Il soulignait, à cette occasion, l'intérêt de l'emploi des pigeons voyageurs en cas de conflit armé, pour relayer nos moyens de transmission si une panne généralisée nous privait de tout moyen de communication radioélectrique. Il rappelait à cette occasion l'exemple de l'armée chinoise qui a décidé en 2011 de « recruter » et d'entraîner 10 000 pigeons voyageurs, en plus des 200 existants déjà. Le ministre de la Défense a souligné que l'effort de la France dans ce domaine porte sur les mesures prises pour assurer la fiabilité, la rapidité et la protection de nos communications militaires, mais que le pigeon voyageur a effectivement rendu de grands services dans le passé, en assurant des missions de transmission militaire sûres et endurantes, franchissant des lignes de communication terrestres non sécurisées. Les armées françaises disposent donc effectivement aujourd'hui du dernier colombier militaire d'Europe. Et la France recense près de 20 000 colombophiles amateurs susceptibles d'apporter un précieux concours en cas de forte fragilisation des réseaux de télécommunications.

L'utilisation du pigeon voyageur comme vecteur de correspondance est ancienne. Les Turcs et les Arabes maîtrisaient déjà l'élevage des pigeons pour obtenir un avantage sur les occidentaux pendant les croisades. L'emploi de pigeons a été considéré comme très fiable jusqu'à une époque récente, lorsque les techniques de communications électroniques et numériques ont permis de répondre à des besoins toujours plus grands de quantité et de rapidité de transmission de l'information.

L'armée française et la guerre de 1870

Pendant la guerre franco-prussienne de 1870, Paris assiégé, les républicains proclament le 4 septembre la République et la fin du Second Empire. Un gouvernement de défense nationale est créé, et un ministère, dit du « 4 septembre », part pour Tours.

Le 6 septembre, le préfet du département du Nord décide d'envoyer à Paris, par chemin de fer, des pigeons qui pourront rapporter des nouvelles de la capitale. 1 500 pigeons sont réunis à Tourcoing et à Roubaix accompagnés de deux colombophiles. Trois jours plus tard, les pigeons sont à Paris, nourris et soignés pour partie au Bois de Boulogne, les autres au Jardin d'acclimatation. Ils apporteront des nouvelles de la capitale à Roubaix et Tourcoing.

De même, des pigeons seront envoyés de Paris à Tours dans 64 ballons pour qu'ils reviennent ensuite avec des nouvelles du Gouvernement. Gambetta lui-même rejoindra en ballon le Gouvernement le 7 octobre, accompagné de nombreux pigeons.

On estime à environ 381 le nombre de pigeons ainsi transportés par ballon. Au retour, certains seront capturés par l'occupant, d'autres reviendront sans message, beaucoup se perdront (les pigeons sont désorientés par la neige et le brouillard), seront victimes de faucons amenés par les Prussiens ou tués par les chasseurs. Seuls une cinquantaine parviendront à rapporter du courrier. Ce sera néanmoins la seule voie de transport d'informations de la province vers Paris durant le siège.

C'est à cette époque que le photographe René Dragon inventa l'ancêtre du microfilm, grâce à un procédé de miniaturisation de texte, de plans ou photos sur une pellicule de quelques millimètres carrés. Un seul pigeon pouvait transporter 2 000 à 3 000 messages. Grâce à ce procédé, 115 000 dépêches officielles et plus d'un million de messages privés auraient ainsi été aéroportés de Paris ou vers Paris.

Comme ce sera le cas pendant la Première guerre mondiale, les prussiens interdirent la détention de pigeons, sous peine de mort. Les lanciers uhlans se livreront à la chasse au pigeon. Il en sera de même de nombre de paysans et d'habitants des villes, ne voulant pas être pris pour des espions ou des résistants à l'occupation. Leur attitude sera confortée par la menace de pénurie engendrée par la grande quantité de grains consommés par les pigeons pouvant conduire à une disette autant pour la nourriture humaine que pour celle des chevaux. Coté français, Gambetta, au contraire, décidera d'appliquer la peine de mort à toute personne faisant la chasse aux volatiles afin de protéger les oiseaux porteurs de messages.

Après la guerre, Edgar Quinet suggérera qu'un pigeon voyageur soit symbolisé sur les armoiries de Paris.

La Première guerre mondiale

Pendant la guerre de 1914 – 1918, les pigeons voyageurs ont été utilisés pour communiquer sur le front. Dès l'enlisement des armées à partir de 1915, l'information et la désinformation sont devenues vitales. La téléphonie, encore en développement, ne pouvait assurer dans tous les cas la liaison avec des unités isolées, ou sur de grandes distances avec la rapidité satisfaisante. Les deux camps utilisèrent assez largement les pigeons voyageurs, élevés et transportés dans des unités mobiles de campagne, camions spéciaux se déplaçant au gré des besoins sur les différents fronts. Un bus à impériale Berliet (dit Araba) fut transformé en pigeonnier roulant. Le bas de caisse contenait une réserve de grain et d'eau, ainsi qu'un logement pour le soigneur, et le haut du véhicule constituait le pigeonnier. En 1916, seize pigeonniers sur remorque ont été fabriqués en France.

Comme en 1870, l'occupant allemand veilla à interdire le lâcher de pigeons dans les zones occupées, notamment dans le nord de la France, région fortement imprégnée de culture colombophile. Les personnes trouvant un pigeon étaient tenues de le remettre à l'autorité militaire sous peine de s'exposer à des poursuites sous le motif d'espionnage.

Ces pigeons, comme les soldats, ont eu droit aussi à la reconnaissance de la Patrie. Un monument leur a été dédié à l'entrée de la citadelle fortifiée de Lille, près du champ de Mars. Certains monuments aux morts évoquent parfois aussi le pigeon voyageur. Exposés aux mêmes dangers et risques que les hommes, certains ont même été décorés. Le plus célèbre d'entre eux s'appelait Vaillant, dernier pigeon du Fort de Vaux, cité à l'ordre de la Nation. Lâché le 4 juin 1916 à 11 h 30, il apportait à Verdun l'ultime message :

« Nous tenons toujours, mais nous subissons une attaque par les gaz et les fumées très dangereuses. Il y a urgence à nous dégager. Faites-nous donner de suite toute communication optique par Souville, qui ne répond pas à nos appels. C'est mon dernier pigeon. Signé : Raynal ».

Gravement intoxiqué par les gaz de combat, le pigeon est arrivé mourant au colombier, mais sera sauvé et vivra encore quelques années.

Autre combattant de la Grande guerre, le capitaine René nous livre dans ses mémoires un témoignage pathétique du secours apporté par les pigeons en 1915 :

« Une unité de chasseurs à pied, engagée à fond, s'est trouvée en pointe et coupée des autres unités. Tous les moyens pour aviser le commandement de cette situation étaient fauchés par les bombardements ou le tir des mitrailleuses. Le téléphone était coupé et la liaison optique impossible en raison de la fumée des éclatements. C'est alors que les chasseurs qui avaient emporté quelques pigeons voyageurs obtinrent de les lâcher avec le message suivant : « Sommes sous le Souchez. Subissons lourdes pertes, mais le moral est très élevé. Vive la France ! » Du colombier, le message fut transmis à l'artillerie qui allongea le tir, protégeant ainsi nos chasseurs d'une contre-attaque allemande. Ainsi Souchez fut libéré. »

Revers de la médaille, on peut se demander si le pigeon voyageur n'a pas aussi été le vecteur de la propagation de la grippe espagnole dans les tranchées et les armées, notamment en 1917 dans le Pas-de-Calais dans le camp d'entraînement anglais d'Etaples.

Et comment les pigeons vivent-ils leur mission ?

Le pigeon voyageur est une race d'oiseau de l'espèce biset (*Columba livia*) spécialement sélectionnée pour effectuer des voyages avec des messages. Il est utilisé par les colombophiles en respectant quelques principes simples de « routage » :

- un pigeon ne sait faire que retourner vers son pigeonnier ;
- il faut donc garder dans chaque pigeonnier, des pigeons d'autres pigeonniers pour pouvoir envoyer les réponses ou les accusés de réception ;
- tout en ne gardant les pigeons que pendant une durée limitée pour que celui-ci ne s'habitue pas à son nouveau lieu de résidence et ne retourne plus à son pigeonnier de départ.

Une certaine maîtrise de la gestion des pigeons est donc nécessaire.

Les troupes trouvèrent néanmoins de nombreux avantages à leur utilisation pour faire remonter à l'état-major la connaissance de la situation sur le terrain :

- la liaison est sans grand risque d'interception (un pigeon est plus difficile à viser qu'un ballon) ;
- elle ne nécessite par de grands moyens (un pigeon est léger à transporter et facile à nourrir) ;
- la mission s'effectue avec beaucoup de discrétion (moins de bruit qu'un avion) et de façon presque invisible, car il est difficile de distinguer un pigeon « militaire » d'un pigeon « civil » ne transportant pas de message.

L'armée belge semble avoir été la seule armée à utiliser des pigeons voyageurs au cours de la Seconde guerre mondiale. Une statue représentant un pigeon prêt à aller porter un message a été édifiée à Bruxelles et inaugurée en 1931. Elle porte la mention « au pigeon soldat ».

L'US Navy utilise des pigeons pour le sauvetage en mer, en les conditionnant par entraînement à réagir à certaines couleurs, et notamment celles des gilets de sauvetage. Grâce à leur excellente vue, emportés dans une bulle sous hélicoptère, ils repèrent très facilement les naufragés, en tout cas mieux que ne le ferait l'œil humain.

La colombophilie reste aujourd'hui encore activement pratiquée en France et à l'étranger comme activité de loisir.

Théorie du drone

de Grégoire Chamayou, aux éditions La fabrique

Dans le développement des systèmes d'armes, le récent drone offensif joue un rôle à part. Il rompt la symétrie séculaire entre les combattants où chacun est légitime de tuer puisqu'en retour il peut lui aussi être blessé voire tué.
A travers cet essai volontairement polémique, Grégoire Chamayou, chercheur en philosophie au CNRS, souhaite « fournir à ceux qui voudront s'opposer à la politique dont le drone est l'instrument, des outils discursifs pour le faire ». Le cadre est posé. Pourtant, même si les exemples choisis sont presque exclusivement américains, soit parce qu'ils sont les plus avancés au monde, soit parce que les actions des autres bords sont moins connues, l'auteur aborde de manière exhaustive tous les aspects de l'utilisation du drone offensif : tactique, stratégie du moins celle qui résulte de l'usage, éthique, droit de tuer, redéfinition des frontières, psychologie du pilote de drone, fin de la guerre ou guerre universelle …
On ressort glacé en lisant un dialogue entre opérateurs de la CIA qui hésitent entre une silhouette d'enfant ou celle d'un chien avant de tirer. Et l'on se rapproche d'une description à la Georges Orwell en découvrant un monde hautement informatisé où l'autorité s'organise pour tout voir et tout savoir, puis détecte de manière automatisée des comportements potentiellement dangereux et petit à petit fait glisser le nom d'une personne dans une kill list.
Après les récentes polémiques sur les drones, cet ouvrage nous fait en tous cas réfléchir sur cette arme bien particulière lorsqu'elle devient un outil de « chasse à l'homme » et la philosophie des armements en l'absence de doctrine d'emploi.

LU AU JO

PAR DÉCRETS D'OCTOBRE 2013

Est promue au grade d'ingénieur général de 1ère classe :

Pour prendre rang du 1er décembre 2013
- L'IGA2 Levêque (Françoise).

Sont nommés :
- L'IGA2 Luzeaux (Dominique, Jean, Pierre), directeur adjoint « plans » de la direction interarmées des réseaux d'infrastructure et des systèmes d'information de la défense (1er décembre 2013).
- L'IGA2 Videau (Jean-Christophe, Philippe), chef du service du maintien en condition opérationnelle de la direction des opérations (1er novembre 2013).
- L'IGA2 Bouchet (François, Henri, Robert), directeur de l'unité de management Opérations d'armement terrestre de la direction des opérations (1er décembre 2013).
- L'IGA Pérard (Thierry), membre du conseil d'administration de la société Défense Conseil international.

PAR DÉCRETS DE DÉCEMBRE 2013

Sont promus au grade d'ingénieur général de 1ère classe :

Pour prendre rang du 1er janvier 2014
- L'IGA2 Mestre (François, Marie, Marcel)

Pour prendre rang du 1er février 2014
- L'IGA2 Luzeaux (Dominique, Jean, Pierre)

Sont nommés au grade d'ingénieur général de 2e classe :
Pour prendre rang du 1er janvier 2014
- L'ICA Noureau (Jean-Christophe)
- L'ICA Sellier (Cécile, Renée, Marie)
- L'ICA Thomas (Alain, Pierre, Marie)
- L'ICA Chenuil (Claude)

Pour prendre rang du 1er février 2014
- L'ICA Carlier (Thierry, Jean-Marc).
- L'ICA Carlier (Mireille, Gisèle).
- L'ICA Plessix (Florence, Marie-Thérèse)
- L'ICA Le Meur (Bertrand, Pierre, Roger)

Est nommé :
- L'IGA2 Baud (Thierry, Marcel), directeur de l'unité de management Missiles et drones de la direction des opérations de la DGA (1er janvier 2014).

PAR DÉCRET ET ARRÊTÉ DE JANVIER 2014

Sont promus au grade d'ingénieur général de 1ère classe :

Pour prendre rang du 1er février 2014
- L'IGA2 Gervais (Caroline, Marie-Noëlle)

Pour prendre rang du 1er mars 2014
- L'IGA2 Tinland (Jean-Luc, Serge)
- L'IGA2 Lesbre (Olivier, Jean-Philippe, Marie)

Est renouvelé dans ses fonctions :
Jean-Paul Herteman, vice-président du Conseil général de l'armement pour une durée de trois ans à compter du 1er mars 2013.

NOMINATIONS DGA

DÉCORATIONS

Ordre national du Mérite
Décret du 4 novembre 2013

Au grade de commandeur
FRACHON Bruno IG1A
LE GOFF Jean-René. IG1A
HOUTTEMANE Jean-Paul IG1A
LUSSEYRAN Pierre. IG1A

Au grade d'officier
BRUNI Eric IG2A
LEBLOND Thierry IG2A
NOUREAU Jean-Christophe IG2A
LE YAOUANC Yannick . . . . . ICA
DALLOT Pierre . . . . . ICA
NOUREAU Jean-Christophe . . . . . ICA
LEICHLE Jacques. . . . . ICA

Au grade de chevalier
ADENOT Pierre-Edouard. . . . . ICA
GUYON Jérôme . . . . . ICA
BENSO Eric . . . . . ICA
BOUYER Frédéric . . . . . ICA
KOFFI Philippe
CHIRON François . . . . . ICA
COLLIQUET David . . . . . ICA
PEDO Eric . . . . . ICA
DEBAERT Christophe . . . . . ICA
RATIEVILLE Matthieu . . . . . ICA
DIAZ DE TUESTA Gaël . . . . . ICA
SIGAUD Philippe. . . . . ICA
DUFOURD-MORETTI Delphine . . . . . ICA
FOSSAT Matthieu . . . . . ICA
VALETTE Frédéric. . . . . ICA
FULLER William . . . . . ICA
VAN HEMELRYCK Jorge . . . . . ICA
GOY Alexandre . . . . . ICA
GRANDEMANGE Christophe . . . . . ICA
WATTEAU François. . . . . ICA
GUILLOU Pascal . . . . . ICA

Au grade de chevalier,
par décret du 14 novembre 2013
COURBE Thomas . . . . . ICA

Mérite maritime

Au grade de chevalier,
par décret du 16 août 201
LE CORRE François

Médaille de la Défense nationale
Année 2013

Echelon or
VIVIER Thérèse. . . . . ICA

Echelon argent
JOSIEN Michaël . . . . . IPA

Echelon bronze
GRELOT Frédéric . . . . . IA
BANCET Alexis . . . . . IA
BEGUE Jean . . . . . IPA
DELONCLE Axel . . . . . IPA
PAING Jean-Baptiste . . . . . IPA
SAUDEMONT Claire . . . . . IA
PELLETIER Johana. . . . . ICA
THOME Emmanuel. . . . . IPA
ROMANO Géraldine . . . . . IPA
WININGER Emeric . . . . . ICA

NOMINATIONS DGA

MOBILITÉS ET DÉPARTS

Mouvements de juillet

ICA BERTHOMIEU Sébastien. . . . . DP SCGC
ICA BESSIS Jean-Pierre . . . . . HDSE CGARM
IA BOUDOT Thomas . . . . . DS CATOD
ICA CARCENAC Claude. . . . . DS S2IE
ICA CORNOLLE Didier. . . . . HDSE CGARM
ICA COUVERT Claude . . . . . DS S2IE
ICA DECOURT François. . . . . DO SCA
ICA FINTZ Pascal . . . . . SGA DAF
IPA GRANGIER Nicolas . . . . . DP SDM
IPA GUILLERMIN Nicolas . . . . . HDSE DIRISI
ICA LECOINTE Olivier . . . . . DS ICAF
IGA LEGRAND
LARROCHE Monique . . . . . DO DA
ICA PEDO Eric . . . . . DO UM TER
IPA PELLETIER Johanna . . . . . DS SASF
ICA REDAUD Christophe. . . . . DO SMCO
ICA ROVES Jean-Paul. . . . . DS SDCDE

Mouvements d'août

IPA CASTEL Emmanuel . . . . . DS PPE
IA DE MARESCHAL Marc
. . . . . DT DGA Ingénierie des projets
ICA DELANNOY Bruno . . . . . DRH CPP
ICA DROGI Nicolas . . . . . DS PPE
IA GUILLOTEAU Emmanuelle
. . . . . DT DGA Essais en vol
ICA LE GALLIC Richard. . . . . DS PPE
IA LONGUET Baptiste . . . . . DO SCA
ICA MERCIER Laurent. . . . . DS PPE Washington
ICA RABILLOUD Jean-Baptiste
. . . . . DT DGA Essais en vol
IPA ROGERE François . . . . . DO UM HELI
IPA TRAN Patrice
. . . . . Congé pour convenances personnelles
ICA TROTIN Eric . . . . . DI SED/SDAP
ICA VAN HEMELRYCK Jorge . . . . . DO UM ESIO

Mouvements de septembre

ICA ADENOT Pierre-Edouard. . . . . DI SED/SDAP
IA ADNET Guervan
. . . . . DT DGA Ingénierie des projets
ICA BAROUX Marie-Hélène. . . . . DO UM ESIO
ICA BELLOEIL Thierry . . . . . DS SDCDE
IA BENAC-LESTRILLE Gaétan
. . . . . DT DGA Maîtrise NRBC
ICA BERDER Eric
. . . . . DT DGA Ingénierie des projets
IGA BERVILLE Marc . . . . . DS CATOD
IGA BOMMELAER Guy . . . . . SMQ CND
ICA BORNERT Vincent . . . . . SIAé AIA
ICA BOUCHARDY Eric . . . . . DS SRTS
ICA CATHERINE Olivier . . . . . SIAé AIA
IA COHEN Lionel . . . . . DP SDM
IGA COLIN Yves . . . . . DO SDCOA
ICA CONAN Erwan . . DT DGA Essais de missiles
ICA COURNIL Michel . . . . . DO UM COE
ICA CROZES Cyril . . . . . DS SDCDE
ICA DAL François-Olivier . . . . . DP SDM
IPA DE SEZE Laëtitia . . . . . DO UM ESIO
ICA DESIT Franck. . . . . DS CATOD
ICA DIDIER Frédéric . . . . . DP SDM
ICA DOCK Jean-François
. . . . . DT DGA Techniques navales
ICA DUFOURD-MORETTI Delphine . DO UM TER
IGA FARGERE Norbert. . . . . DS Adjoint
IA FARLOTTI Martin . . . . . SMQ SQ
IA FOESSEL André
. . . . . DT DGA Techniques navales
ICA FORICHER David . . . . . DO UM TER
IPA GARCIA Jérôme . . . . . DO UM MID
ICA HERVE Guillaume. . . . . DP SDP
ICA HUGON Philippe. . . . . SIAé AIA
ICA IAGOLNITZER Michel . . . . . SGDSN
ICA JAGU Steeve
. . . . . DT DGA Ingénierie des projets
IGA JOUANJEAN Francis. . . . . HDSE CGARM
ICA LAHAYE Gilles . . . . . DI SGPM
ICA LAHOUSSE Alexandre. . . . . DO SMCO
ICA L'ANTHOEN Bernard. . . . . DO UM ACE
IA LE GALL Christophe
. . . . . DT DGA Techniques hydrodynamiques
IPA LE GOFF Xavier
. . . . . DT DGA Ingénierie des projets
ICA LE VEN Gaël. . . . . DP SDP
ICA LE YAOUANC Yannick . . . . . DO SMCO
ICA LENFANT Jean-Christophe. . . . SGA MSIAG
ICA LESTIENNE Tanguy. . . . . DO UM AMS
ICA LETELLIER Olivier. . . . . DS CATOD
IGA LEVET Jacques . . . . . SMQ CM
IPA LLORCA Yohann
. . . . . DT DGA Ingénierie des projets
IPA LONCHAMPT Corinne
. . . . . DT DGA Ingénierie des projets
ICA LORNE Thomas
. . . . . DT DGA Essais de missiles
IGA MALET Didier. . . . . DI DOE
ICA MANIERE Hervé . . . . . DS S2IE
ICA MARTY Jean Youri . . . . . Dét. AED
IA MASSARDIER François
. . . . . DT DGA Ingénierie des projets
IPA MERLIN Xavier . . . . . DS SASF
IGA MESTRE François . . . . . DS SASF
IA MINVIELLE Thomas . . . . . DS CATOD
IA MONVILLE Pierick . . . . . DS CATOD
IA MORVANT Julie
. . . . . DT DGA Ingénierie des projets
IPA PAING Jean-Baptiste . . . . . DP SDP
ICA PENNANECH Pierre . . . . . DO UM NAV
ICA PERRIN Jérôme . . . . . DO SMCO
ICA PICHON Stéphane
. . . . . DT DGA Techniques terrestres
ICA PRADELLE Anne. . . . . DT DGA Essais en vol
IGA PUYHABILIER Patrick
. . . . . HDSE ENSTA Bretagne
ICA RATIEVILLE Matthieu . . . . . Dét. OTAN
IA RIGAUT Thomas
. . . . . DT DGA Ingénierie des projets
IA SAINT-MAURICE Romain . . . . . DS CAB
IA SAINT-PIERRE Jean-Benoît
. . . . . DT DGA Essais en vol
IPA SALAHUN Caroline . . . DRH Ecole de guerre
IGA SERIS Pierre . . . . . HDSE CPPEBF
ICA SIMON Olivier
. . . . . DT DGA Maîtrise de l'information
ICA SIMON Christophe . . . . . DO UM AMS
IGA SPINA Eveline . . . . . DP SDP
ICA TESSAUD Nicolas. . . . . DS SDCDE
IPA TRABOULSI Nadim . . . . . DO CAB
IGA VINSON-ROUCHON Blandine . . . . . DT ST
ICA VIVIER Thérèse. . . . . DO UM AMS

Mouvements d'octobre

IGA CALECA Yves. . . . . EMAT SIMMT
ICA CARLIER Thierry. . . . . DS SDCDE
IGA CHABBERT Christian . . . . . HDSE IGA-Ar
ICA CHENUIL Claude . . . . DT DGA Essais en vol
ICA FABIANI Patrick . . . . . HDSE ISAE
ICA MARTINEZ Marie-José. . . . . DO UM HELI
IGA ROUJANSKY Jacques. . . . . HDSE CGARM
IGA SCHANNE Pierre . . . . . DT MIP

Mouvements de novembre

ICA BEAURENAUT Olivier . . . . . DS SASF
IPA CASAGRANDE Gaëlle . . . . . DO SCA
IA DUCAROUGE Mathieu
. . . . . DT DGA Ingénierie des projets
IPA GRELOT Geoffroy
. . . . . DT DGA Ingénierie des projets
ICA LE SAINT Laurent. . . . . DO UM COE
ICA PHAN Nathanaël . . . . . DO SIMMT
ICA PINCEMIN Paul-André
. . . . . DT DGA Maîtrise de l'information
ICA PINOT Pascal . . . . . DRH Adj. Ecoles
ICA TRIVAUDEY Franck. . . . . HDSE CGARM

Mouvements de décembre

IA BERGOTTI-DAOUDI David
. . . . . DT DGA Techniques aéronautiques
ICA BONIORT Laurent. . . . . Aff. Temp. SGDSN
ICA BONNAUD Hervé . . . . . DO SIMMAD
ICA BRUXELLE Jean-Yves . . . . . DS SASF
ICA ELOY Matthieu. . . . . Détaché OTAN
ICA GAUDEMET Thomas. . . . . DO UM NBC
ICA GIRARD Philippe . . . . . HDSE CGARM
IA GREUSARD Léo
. . . . . DT DGA Techniques aéronautiques
ICA LODEON Patrick. . . . . HDSE IGA-Ar
IA RIOU Morgane . . . . . DT DGA Maîtrise NRBC

DEPARTS RETRAITE

Mouvements de juillet/août/septembre

ICA CHAFFAUT François-Xavier
ICA DELANNOY Bruno
ICA DEPARDIEU Gilles
IPA LUTUN Bernard

CARNET PRO

Nathanaël Phan (1967) a été nommé Chef de bureau de SIMMT (01/11/2013)

Cécile Marly (1976) passe de la Préfecture à la CCI de la Région Centre pour occuper les fonctions de Directeur de l'action régionale (01/11/2013)

Laurent Giovachini (1961) est désormais conseiller de Pierre Pasquier, président de la société SOPRA (01/11/2013)

Eric Berder (1960) a été nommé Rapporteur à la Cour des Comptes (01/11/2013)

Michel Bouvet (1958) a fondé et dirige ESR Conseil, dédiée à l'accompagnement des acteurs publics et privés du monde de la recherche et de l'innovation (01/11/2013)

Arnaud Morigault (1979) a été nommé Directeur associé pour la branche secteur public de Cap Gemini Ernst & Young (CGEY) (12/11/2013)

Nicolas Chamussy (1967) a été nommé Chief of staff EADS CEO dans le groupe Airbus (29/11/2013)

Frédéric Garnier (1971) a été nommé Cyber Threat Intelligence à la Commission Européenne/CERT UE (01/12/2013)

Matthieu Eloy (1969) a été nommé Executive Coordination officer au sein de l'OTAN bureau du Dur Scientifique à Evere (02/12/2013)

Blaise Jaeger (1963) a rejoint CAP GEMINI comme Directeur de la division Aérospatiale & Défense d'Application Service France (10/12/2013)

Jacques Levet (1958) a rejoint la Fédération des Industries Electriques, Electroniques et de Communication (FIEEC) comme Directeur Technique (01/01/2014)

Guilhem de Robillard (1977) a été nommé Sous-Directeur Ingénierie du Service Parisien de Soutien à l'Administration Centrale du SGA, Ministère de la Défense (01/01/2014)

Hervé Turlier (1986) après son doctorat, effectue un post-doc comme chercheur fondamental à l'European Molecular Biology Laboratory (EMBL) (01/02/2014)

Amans Defossez (1980) a été nommé Customer Program Manager dans le groupe SAFRAN à Villaroche (01/02/2014)

Advanced Cyber Security.

Be fully prepared for the future.

TRUST THE FUTURE / CONFIANT EN L'AVENIR

WWW.CASSIDIANCYBERSECURITY.COM

AIRBUS
DEFENCE & SPACE