ShortMag

Magazine des Ingénieurs de l'Armement - Hors série - Janvier 2014

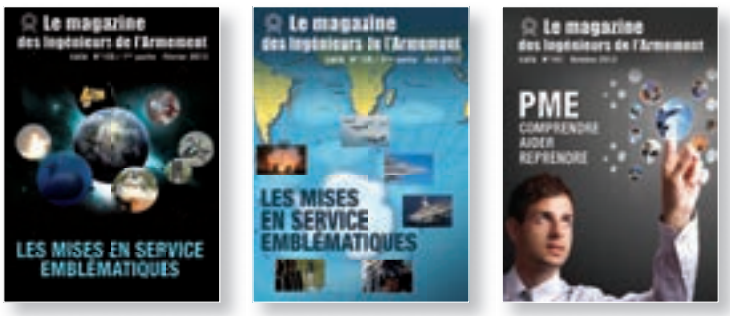
La cybersécurité

Dossier du magazine caia N°102 - Février 2014

Short sommaire

La CAIA, Confédération Amicale des Ingénieurs de l'Armement mène de nombreuses activités parmi lesquelles :

Les Magazines



L'Annuaire

Le Gala de l'Armement

Edito

Jérôme de Dinechin
Rédacteur en chef

Chers lecteurs,

la gazette que vous tenez en main vous présente quelques extraits du prochain magazine des Ingénieurs de l'Armement.

Comme pour bien d'autres domaines techniques, ces pages mettent en évidence les impacts majeurs de la cyber sur la défense et la sécurité de notre pays et de ses alliés.

C'est précisément le rôle des Ingénieurs de l'Armement d'évaluer ces impacts, et de construire avec et au profit des forces de la nation les grands systèmes qui permettront de la défendre. Ce rôle de l'ombre, a permis de doter la France d'une force nucléaire stratégique et de systèmes de défense du meilleur niveau mondial, que ce soit sur terre, sur mer, dans les airs ou l'espace. Il continue plus que jamais aujourd'hui, en s'ouvrant à d'autres domaines.

Cela ne peut se faire sans une intime compréhension de enjeux technologiques, de l'innovation et de sa dynamique. Cela ne peut se faire non plus sans une capacité à conduire des programmes complexes à forte dimension technique, au contact à la fois des opérationnels et des industriels. Enfin, cela implique de bien comprendre les enjeux géostratégiques et de travailler de plus en plus en environnement international.

Le magazine des IA, dont vous pouvez retrouver les derniers numéros en ligne sur le site de notre association www.caia.net, s'efforce d'apporter une réflexion approfondie ainsi qu'un regard de vérité sur des sujets cruciaux aujourd'hui. Et si on ne peut pas tout dire, on le dit aussi !

Vous souhaiteriez approfondir ce domaine ou un autre ? (mailto:caia@caia.net)

Bonne short-lecture

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

Sommaire

Magazine 102 - Février 2014

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

Edition et régie publicitaire :
SACOM 01 41 10 84 40,
lneyret@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

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 y 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 !

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, voir même 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, mais 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 mais le constat s'est considérablement durci puisque le nouveau livre blanc n'hésite plus à parler d'actes de guerre et de priorité nationale !

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'arme 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. Nous pensons en avoir, même si la modestie doit rester de mise dans ce domaine. 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 d'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

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.

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

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 application 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 prendre sur leur temps, que je sais compté, afin 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 appelé SSI) ;
- la « cyberdéfense » responsable de la détection et de la réaction face aux attaques informatiques (parfois également appelé lutte informatique défensive ou LID) ;
- la « cybercontinuité » qui veille au maintien des capacités essentielles lors des attaques et à la résilience des systèmes.

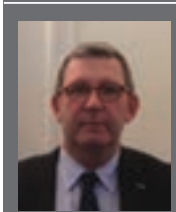
En termes d'organisation, au sein du ministère de la défense et sans entrer dans certaines subtilités, la DGA est en charge, dans les trois domaines, des travaux de recherche et de développement ainsi que des acquisitions. Du point de vue opérationnel, la protection est gérée par une chaîne SSI placée 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.

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.

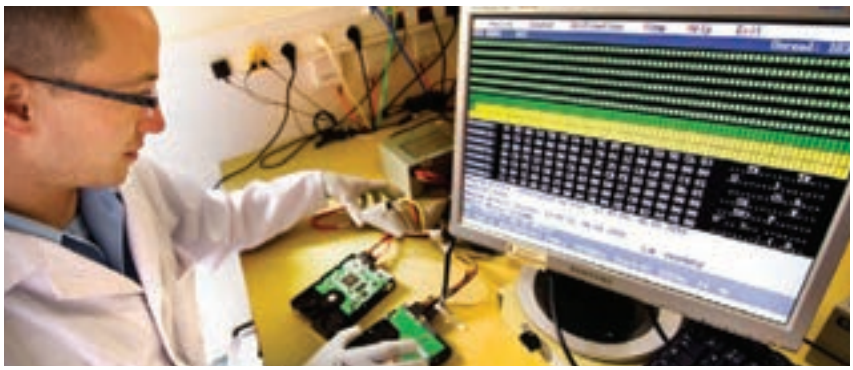
Dans les années soixante-dix, la crainte d'un développement non contrôlé et d'une utilisation frauduleuse des fichiers de données à caractère nominatif motivent les premières dispositions du code pénal régulant un cyberespace naissant. C'est la loi du 6 janvier 1978, relative à l'informatique, aux fichiers 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 leur 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 état 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



par
Marc Watin-Augouard,
Inspecteur général des Armées

«Ancien inspecteur général des armées-gendarmerie, le général d'armée (2S) Watin-Augouard dirige le centre de recherche de l'Ecole des Officiers de la Gendarmerie Nationale. Fondateur du Forum International de la Cybersecurité (FIC), il est membre du comité d'organisation. 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 et membre du comité de rédaction de la Revue de la Défense Nationale et de la Revue Administration.



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 indentité, 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.

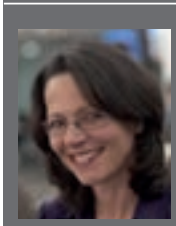
Mais les Etats devront encore longtemps compter sur eux-mêmes. Depuis le Livre Blanc sur la défense et la sécurité nationale de 2008, la France s'est engagée dans une stratégie volontariste que le dernier Livre Blanc vient conforter. La loi de programmation militaire, promulguée le 19 décembre, renforce les deux piliers de la cyberdéfense : l'Agence nationale de sécurité des systèmes d'information (ANSSI) et le pôle défense (EMA-défense 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.

Cyberespace
Une nouvelle dimension des conflits géopolitique

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.

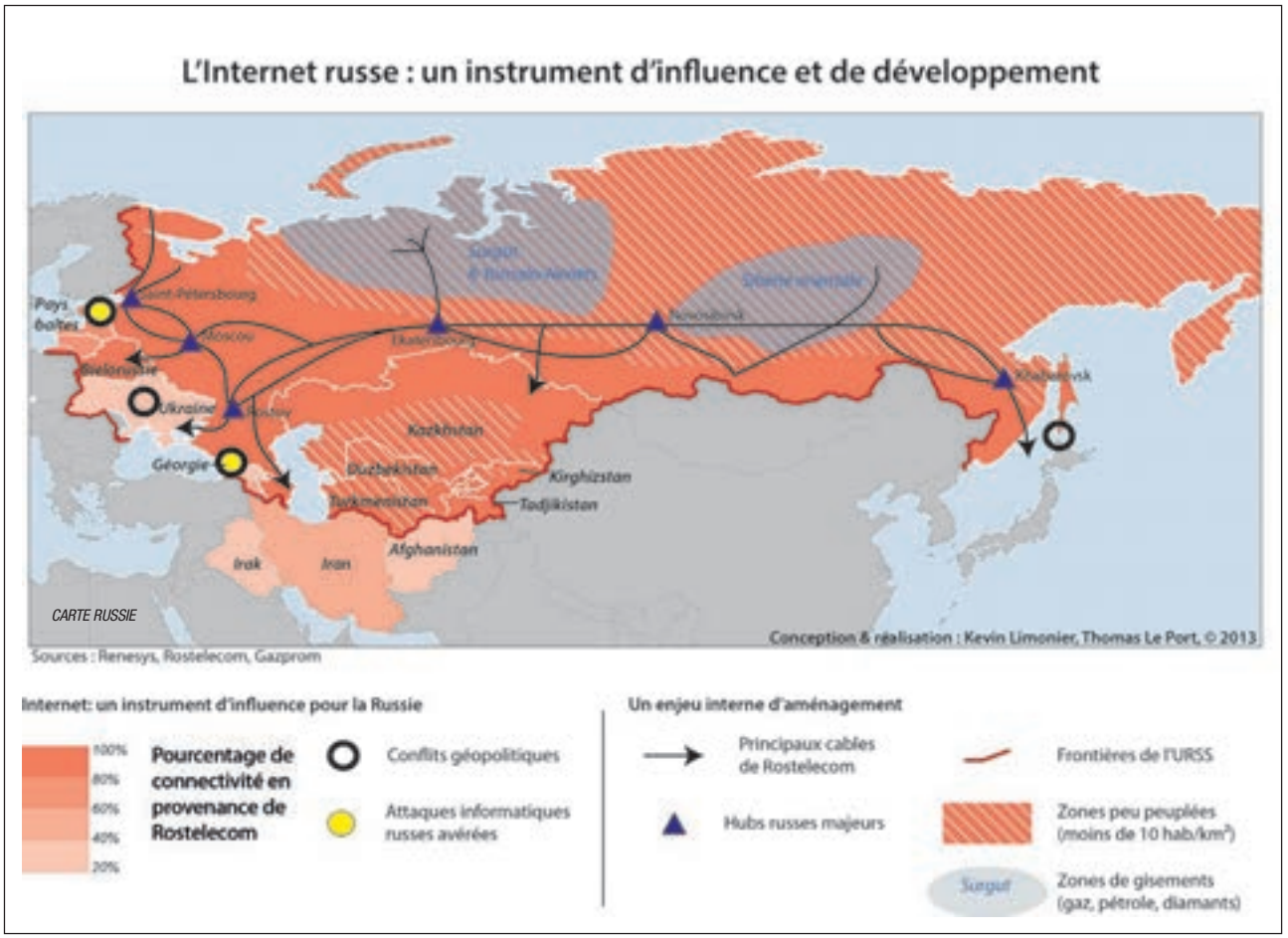
Risques et opportunités du cyberespace

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 prosécution 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 ses 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 multiscalaire, 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.

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 du Groupe EADS

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

COFIS (Comité de la filière industrielle de sécurité)

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.

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.

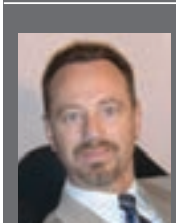
L'écoute est réelle, le besoin est là, c'est le bon moment…

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



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.

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

L'approche systémique de la cybersécurité


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

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.

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.


Le guerrier du futur

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.

(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

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[1] 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

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.

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 pour-

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 ?

ra 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[2].

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[3].

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[4], 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'E. 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.

(1) Consiste à engorger de trafic parasite la connexion Internet de la victime. Ce genre de trafic représente de l'ordre de 20 % des données qu'achemine un opérateur de télécommunications et, curieusement, une bonne part en vise non pas des entreprises mais des utilisateurs individuels : il s'agit probablement de joueurs en ligne que leurs adversaires sans scrupules paralysent opportunément pour leur faire perdre la partie.

(2) http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/

(3) http://people.umass.edu/gbecker/BeckerChes13.pdf

(4) http://intelligence.house.gov/sites/intelligence.house.gov/files/Huawei-

Regard sur… le corps des Ingénieurs de l'Armement

Le corps de l'armement est une communauté d'ingénieurs recrutés majoritairement en sortie de l'Ecole Polytechnique, pour conduire les grands programmes de défense et de sécurité dont l'Etat a besoin. Ils font partie de la haute administration, aux côtés des autres grands corps techniques de l'Etat, corps des Mines, corps des Ponts Eaux et Forets, corps de l'INSEE, et des corps administratifs.
Particularité, les Ingénieurs de l'Armement ont un statut militaire, d'abord issu de l'histoire des Corps qui l'ont précédé et constitué, et qui traduit aujourd'hui à la fois une proximité avec les forces armées dont ils développent les grands systèmes, et un sens de l'Etat et du service public particulier.

Les grands systèmes de défense et de sécurité

Les Ingénieurs de l'Armement ont développé des compétences pointues dans de nombreux domaines technologiques, puisque pratiquement toutes les évolutions techniques ont un impact sur les enjeux de défense et de sécurité.

Comme exemples de programmes dont la France peut s'enorgueillir : Les sous-marins nucléaires lanceurs d'engins qui comptent parmi les objets les plus complexes au monde, les radars, les missiles, les systèmes d'information opérationnels, les satellites militaires ou d'observation, les frégates, les systèmes de surveillance aérienne…
En examinant les caractéristiques de ces grands systèmes, nous pouvons en retenir quatre :

L'excellence technologique : les systèmes de défense et de sécurité ne peuvent pas se contenter des technologies actuelles. Dans la lutte séculaire entre la lance et le bouclier, il est nécessaire de se tenir à jour des innovations et de leur dynamique.
Ainsi aujourd'hui, les orientations couvrent la cyber ainsi qu'il est présenté dans ce magazine et les systèmes de systèmes, permettant de concevoir des systèmes capables de travailler ensemble de manière coordonnée, aujourd'hui et demain.

La dimension temporelle : les systèmes d'armes sont conçus pour durer plusieurs décennies. Ils devront évoluer et s'adapter plusieurs fois au cours de leur vie. Au moment de faire les choix d'architecture de systèmes, un certain nombre de paris doivent être pris sur les évolutions probables des techniques et des menaces. Comment intégrer un bon niveau de flexibilité dans les équipements pour qu'ils restent au meilleur niveau mondial suffisamment longtemps.

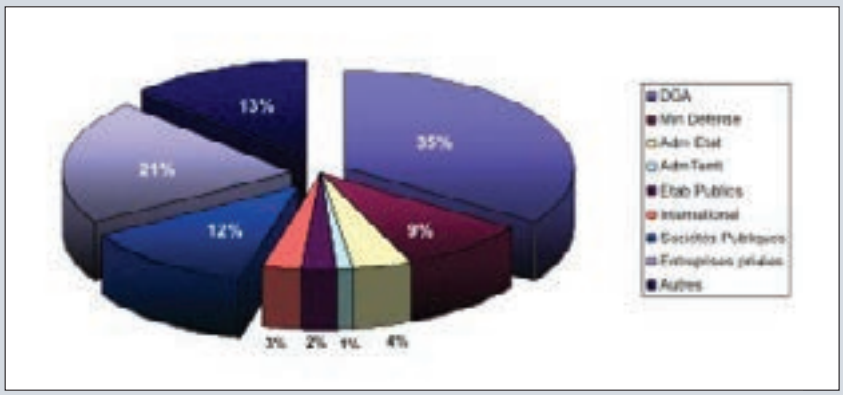
Une vision technologique et industrielle : pas de systèmes performants s'il n'y a pas de compétence industrielle en face. La France dispose d'une industrie de défense et de sécurité forte, dont les Ingénieurs de l'Armement ont contribué à asseoir les fondements : DCNS, Nexter, Airbus, Thales, Safran, mais aussi tout le tissu de la Base Industrielle Technologique de Défense (BITD) dont environ 4000 PME.
A travers le plus important budget d'investissement de l'Etat, géré par la DGA, ils assurent

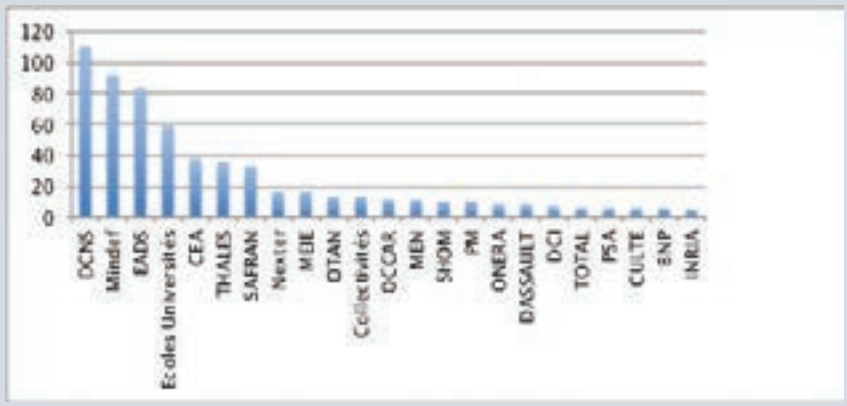
la satisfaction des besoins d'armement de la France, et maintiennent sur le long terme des capacités de conception et de production suffisamment indépendantes.

Une coopération internationale : de plus en plus de programmes sont conduits entre différents Etats : 7 pays sont ainsi associés dans le développement de l'avion transporteur militaire A400 M, chaque pays ayant bien sûr des spécifications particulières.

Qui sont les Ingénieurs de l'Armement

Le corps représente 1800 personnes dans la vie active, et il est difficile de définir une carrière type.





Une répartition public / privé équilibrée

Côté public, une répartition se fait au fil des années soit en restant à la DGA (qui emploie aujourd'hui 630 IA), soit en évoluant au Ministère de la Défense ou dans les ministères comme l'Intérieur, l'Ecologie, les Finances ou en se tournant vers les administrations territoriales, dans des organismes liés à la recherche, les grandes écoles, les établissements publics ou organismes internationaux.

Côté privé, après quelques années au service de l'Etat, les Ingénieurs de l'Armement peuvent, dans un cadre déontologique strict, se tourner vers l'industrie en apportant avec eux un savoir-faire et une compétence assez unique de pilotage de grands projets à forte profondeur technique.

Près de 200 occupent des fonctions « exécutives ».

Leurs employeurs hors DGA

Bien sûr, cette liste est très restreinte et ne saurait représenter la diversité des parcours et des compétences personnelles. Elle donne simplement une image de cette communauté d'hommes et de femmes qui ont choisi d'œuvrer pour leur pays à travers la fonction de défense et de sécurité.

Pour les portraits plus individuels, nous vous laissons les découvrir au fil des pages de nos magazines, ou à travers les rencontres que vous pourrez faire.

JDD

Le magazine
des Ingénieurs de l'Armement