DOSSIER

CYBER
ET
RESEAUX SOCIAUX

espritcors@ire

observatoire de la défense et de la sécurité

Réalisé par l'association espritcors@ire
https://espritsurcouf.fr

Que contient ce monde du CYBER que nous avons décrit à plusieurs fois dans ESPRITSURCOUF ? C'est l'objectif « ambitieux » de ce dossier ?
Le terme cyber recouvre l'ensemble des activités liées à l'utilisation offensive du cyberespace :
Cyber sécurité, les actions de piratage informatique et les moyens de s'en protéger.
Cyber défense, l'utilisation du piratage informatique à des fins militaires et les moyens de s'en protéger.
Cyber espionnage, l'utilisation du piratage informatique à des fins de renseignement économique, technologique, politique ou militaire.
Cyber surveillance, les actions menées par un Etat pour surveiller sa population par des moyens numériques (par exemple : la reconnaissance de visages en Chine) et où par la censure d'internet et des réseaux sociaux.
Cyber guerre, affrontement entre plusieurs Etats, utilisant des moyens cyber.
Cyber criminalité, criminalité constitutive d'une infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau ».
La manipulation offensive des réseaux sociaux en les utilisant à des fins d'influence politique par la diffusion massive d'infox (***fake news***) ou d'informations confidentielles compromettantes.

SOMMAIRE

Discours de Florence Parly, ministre des Armées lors du Forum international de la cybersécurité

Source : **Ministère des Armées**

Monsieur le préfet,
Mesdames et messieurs les élus,
Mesdames et messieurs,

Chers amis,

La cybersécurité, c'est un sport collectif.

La faille peut venir de partout. Les hackers sont plein d'inventivité. Aussi puissants que peuvent être nos pare-feu, une simple inattention peut ouvrir une brèche dans laquelle bien des personnes, des groupes et des Etats voudront s'engouffrer.

Alors, oui, nous devons agir ensemble pour la cybersécurité de nos réseaux. Nous devons, ensemble, concevoir et échanger les bonnes méthodes et les bonnes pratiques. Nous devons bâtir pour chaque entreprise, chaque ministère, chaque personnel, une culture et une hygiène cyber irréprochable.

Nous parlons aujourd'hui de cybersécurité « by design », par essence presque. C'est précisément ce qu'il nous faut construire. Chaque système doit être conçu en pensant à sa cybersécurité. Chaque réseau doit être pensé dès l'origine en se demandant comment le protéger.

Le ministère des Armées le sait bien car les chiffres sont là. En 2017, les réseaux de la défense ont subi 700 événements de sécurité dont 100 cyberattaques. En 2018, les chiffres ont encore augmenté et dès septembre, nous dépassions ce chiffre de 700. Mon petit doigt me dit que cela ne va pas baisser en 2019.

Et non seulement le nombre d'attaques augmente mais les attaquants ont toujours des profils aussi variés. Un adolescent peut pirater les mails de la chancelière allemande pour s'amuser, presque par hasard. Un groupe anonyme peut s'en prendre à nos industries, nos transports, nos hôpitaux sans raison apparente. Un Etat, enfin, peut chercher à affirmer sa puissance en nous espionnant, nous manipulant ou même en sabotant nos capacités.

Et derrière chaque ordinateur, comment identifier avec certitude l'agresseur ? Tout le monde peut se cacher derrière son ordinateur et l'impunité est presque totale.

Voilà la réalité du cyberespace. Ce sont des opportunités inouïes pour nos quotidiens comme pour notre défense. Ce sont aussi des risques, des risques majeurs qui peuvent mettre en péril notre sécurité.

Mesdames et messieurs, la guerre cyber a bel et bien commencé.

Nous ne serons ni naïfs ni aveugles, et nous allons nous y préparer.

L'année dernière sur cette même estrade, je vous annonçais que la France se dotait d'une cyberdéfense renforcée avec 1000 recrutements de cybercombattants supplémentaires d'ici 2025 et 1,6 milliard d'euros pour la lutte dans le cyberespace.

Depuis ces investissements sont entrés dans le marbre de la loi puisque la loi de programmation militaire a été votée puis promulguée par le Président de la République le 13 juillet.

J'avais l'année dernière parlé d'innover, de dénicher et d'attirer tous les talents et toutes les bonnes volontés. Le premier défi cyber du ministère des Armées était lancé. Son objectif était de répondre à une urgence opérationnelle du Commandement cyber en développant rapidement un outil de confiance avec un accès distant pour rechercher les traces d'attaques cyber sur un parc informatique.

12 candidats ont relevé ce défi et j'ai le plaisir d'annoncer les deux lauréats : les PME Harfanglab et Gatewatcher d'un côté et AMOSSYS, de l'autre. Ils ont mis au point des projets novateurs, protecteurs et d'une remarquable efficacité. Nous allons poursuivre le travail avec eux pour s'assurer que leurs solutions soient très vite expérimentées, challengées et intégrées sur nos réseaux. Je veux remercier tous ceux qui ont permis ce défi et qui y ont participé.

Vous avez prouvé qu'on pouvait agir vite et bien. Prouvé qu'on pouvait acquérir des technologies utiles différemment. Je veux tous vous en remercier.

Et ce défi est une méthode nouvelle qui vient de prouver son efficacité, c'est bien qu'il faut continuer ! D'autres arrivent et je pense, en particulier au défi sur l'intelligence artificielle lancé tout récemment par l'Agence Innovation Défense et auquel je le sais, vous êtres très nombreux à avoir répondu.

Nous avons montré notre volonté. Notre capacité à nous mettre en ordre de marche, vite. Et vendredi, à Paris, avec le chef d'état-major des Armées, nous avons encore franchi une étape supplémentaire. J'ai annoncé devant le Commandement cyber, notamment, que la France revendiquait d'utiliser l'arme cyber au même titre que toutes les armes conventionnelles. J'ai pu énoncer les grands principes de notre nouvelle doctrine cyber offensive et le renforcement de notre défense cyber.

L'arme cyber n'est pas seulement pour nos ennemis ou nos fictions. Non. Nous aussi, en France, pouvons défendre, répliquer et attaquer.

Alors, vendredi nous avons révélé une partie de notre doctrine offensive. En opération, nous employons déjà l'arme cyber. Nous avons publié les grandes lignes de cette doctrine pour le faire savoir et nous donner un cadre d'emploi.

Il faut maintenant intégrer l'arme cyber à tous nos programmes, et je compte sur la DGA. Il faut aussi plus de coopérations, de partenariats, de convergences avec nos alliés européens. S'il y a bien une menace qui nous touche tous et se moque éperdument des frontières, c'est bien la menace cyber. Alors nous devons créer une culture commune, des remparts plus forts et agir ensemble, y compris avec de la lutte informatique offensive en opérations.

S’agissant de notre doctrine défensive, mon message est clair : ne pas tendre la joue.

Le ministère des Armées a entamé sa révolution numérique. Il en est même à la pointe et c’est un mouvement qui me tient à coeur. Aujourd’hui, grâce au numérique, le ministère des Armées devient plus simple, plus rapide, plus efficace.
C’est une opportunité extraordinaire. Une opportunité que tout l’Etat saisit. Mais une opportunité qui n’est pas sans dangers.

Alors, le ministère des Armées se prépare, renforce sa défense. Le Commandement cyber a été conforté, son organisation renforcée. Nous redoublons de vigilance et nous dotons des meilleurs outils. Mais une chose est sûre, plus les Armées se protègent, plus les industriels, les sous-traitants sont susceptibles d’être des proies toutes désignées pour pénétrer dans nos systèmes d’information. Alors, c’est toute une chaîne de défense qui doit être protégée de bout en bout.

J’ai donné une instruction en la matière fin décembre. Toute notre communauté de défense doit se protéger et toute notre chaîne de défense se responsabiliser. Le COMCYBER, avec la DGA, sera la tour de contrôle de cet effort et j’appelle tous nos industriels à s’engager pour consolider encore notre cybersécurité.

C’est pourquoi je veux aujourd’hui faire une proposition à nos industriels de défense. Unissons nos forces pour protéger notre chaîne d’approvisionnement de la menace cyber. A l’été, je souhaite que nous puissions formaliser, en en étroite liaison avec l’ANSSI, les engagements mutuels sur la cybersécurité. Il nous faudra mieux définir les rôles et les responsabilités de chacun pour protéger nos systèmes et réagir en cas d’attaque. Cette démarche collective est une absolue nécessité. Elle seule permettra de protéger le développement, la fabrication et la maintenance de nos équipements de défense.

Elle nous permettra de répondre ensemble à plusieurs grands défis.

D’abord, la mise en place d’une coordination : c’est une évidence. Nous devons dialoguer en permanence et joindre à cet échange nos services de renseignement. Nous allons identifier un cadre et une démarche claires pour faire avancer nos travaux de concert. Nous devrons échanger nos informations sur telle ou telle menace, tel ou tel incident. Nous pourrons partager nos outils, aussi, les mutualiser.

Nous établirons une stratégie ambitieuse de sécurisation de nos systèmes. C’est la finalité même de notre démarche, alors il nous faudra cartographier, identifier les priorités.

Nous devons enfin réfléchir à comment aider et protéger efficacement notre chaîne de sous-traitance. Nous ne pouvons pas les laisser devenirs les chevaux de Troie de nos adversaires. Il faudra donc les soutenir, à la fois en méthode et en technique. Il nous faudra aussi être extrêmement exigeant et imposer dans les critères d’achat des clauses sur la cybersécurité.

Je parle de cette chaîne de confiance cyber. Elle passe également par les PME, les start-up. Par leurs idées et leur inventivité. J’ai eu le plaisir de voir quelques démonstrations à l’instant, d’échanger avec nos entrepreneurs. Alors, je veux aussi vous dire une chose : nous avons besoin de vous. Nous avons besoin de vous pour concevoir et produire des produits de sécurité utilisables en toute confiance par nos Armées. Nous avons besoin de vous pour préserver notre autonomie stratégique.

Car les outils de confiance que nos entreprises développent, tous en Europe pourront en profiter. Je veux saluer ici les responsables internationaux présents aujourd'hui. Ils sont nombreux. Et c'est bien au FIC, forum international s'il en est, que nous devons en profiter pour nous inspirer et laisser sa chance à la vitalité des PME européennes.

Et au ministère des Armées, la confiance donnée aux PME et aux entrepreneurs, ce ne sont pas que des mots, c'est du concret.

Il y a quelques mois, cinq PME issues du cluster Hexatrust ont ainsi remporté face à des grands groupes, un marché de prestations cyber pour aider nos opérationnels à sécuriser les systèmes d'information et les réseaux du ministère.
Nous protégeons les PME, nous leur donnons leur chance. Aussi, j'ai lancé cette année un Plan Action PME qui comprend 40 mesures concrètes pour mieux prendre en compte les PME dans notre stratégie d'achat, pour renforcer le soutien à l'innovation et le dispositif RAPID, en particulier. Pour établir également une relation équilibrée entre les PME et les grands groupes.

Je sais que notre souveraineté numérique passe par les PME et j'ai bien l'intention de les choyer.

Et quand je parle de confiance, cela va loin. Un partenariat a été noué entre le COMCYBER et une start-up, « YesWeHack ». Alors, oui, je l'annonce, nous allons lancer fin février le premier « bugbounty » du ministère des armées. Des hackers éthiques, recrutés au sein de la réserve opérationnelle cyber, pourront se lancer à la recherche des failles dans nos systèmes et s'ils en découvrent en être comme il se doit, récompensés.

Mesdames et messieurs,

Nous avons devant nous des défis et des opportunités.

Nous devons créer des liens entre le ministère des Armées et nos industriels de défense, entre le ministère et les PME, œuvrer pour une Europe de la cyberdéfense. Nous devons agir de concert pour une irréprochable cybersécurité.
Et pour y parvenir, il existe un dernier défi que nous devons collectivement relever. Le défi des talents, le défi du recrutement.

Le ministère des Armées doit faire savoir, partout, qu'il cherche des personnes prêtes à coder pour la France. Les industriels mettre en avant les compétences fines qu'ils cherchent. Nous devons tendre la main aux entrepreneurs, aux innovateurs, leur dire que la défense leur ouvre ses portes et qu'elle est prête les soutenir et les pousser vers des parcours, des missions, des vies passionnantes.

L'année 2018 a été riche pour notre cybersécurité. L'année 2019 commence sur les chapeaux de roue. Alors, réfléchissons ensemble. Agissons ensemble. Assurons ensemble notre cyberdéfense. Cette 11e édition du FIC en est une nouvelle opportunité. Saisissons-la pleinement. Je vous souhaite un excellent FIC 2019.

Vive la République ! Vive la France !

Retour au sommaire

Dérives cyber et réseaux sociaux

par René Occhiminuti(*)
Directeur de la publication

paru dans ESPRITSURCOUF.fr

Face au développement du « monde CYBER » et à l'utilisation des réseaux sociaux, nous avons échangés récemment avec plusieurs membres d'**espritcors@ire** et lecteurs d'**ESPRITSURCOUF.fr**. Ils estiment que c'est notre rôle de sensibiliser le plus grand nombre à cette révolution et à ces conséquences pour notre vie personnelle et pour l'avenir politique de nos démocraties.

Ce sujet concerne les informations que nous recueillons quotidiennement. C'est à partir de ces éléments que nous nourrissons nos réflexions, forgeons nos opinions et par la suite nos décisions. C'est la même démarche que suivent nos dirigeants, les leaders de groupe d'opinions, de partis politiques, de syndicats, de groupe de pression. Ils sont donc soumis au même Fake News que l'ensemble des citoyens.

Les manipulations incontrôlables des informations devraient rendre, tous les citoyens honnêtes du monde, sensibles aux risques qu'ils courent.

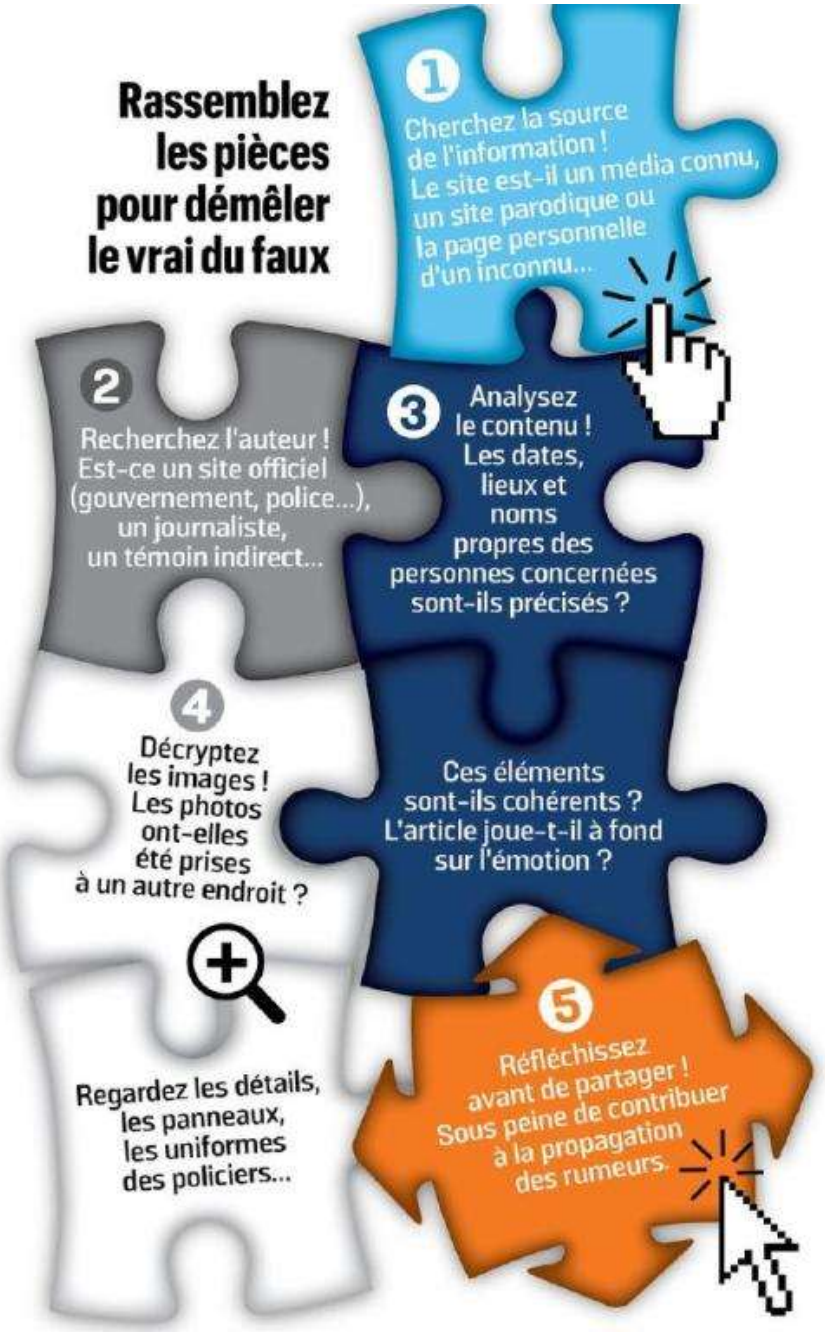
Les réseaux sociaux sont par nature et conception « anarchistes » car on n'y trouve aucune autorité, ni chef ni personne pour réguler ou interdire quoi que ce soit. C'est bien le cas des gilets jaunes dont les mots d'ordre et les querelles internes montrent qu'ils ne supportent aucune autorité.

L'influence des réseaux sociaux est grandissante, selon l'étude « Conspiracy and Democracy » de l'université de Cambridge, (réalisée en aout 2018, avant l'apparition des « Gilets Jaunes », grands utilisateurs de Face book..) les français pour s'informer utilisent 2 à 3 fois par semaine à 75% la Télévision, à 49% la radio, à 43% un réseau social(Facebook, Twitter…), 31% le site internet d'un journal, 21% un magazine, 18% un site d'information sans lien avec un journal , 15% une newsletter par email **(ESPRITSURCOUF est à la fois un site d'information et une newsletter)** et 4% par Podcasts.

Que contient ce monde du CYBER que nous avons décrit à plusieurs fois dans ESPRITSURCOUF ?

Le terme cyber recouvre l'ensemble des activités liées à l'utilisation offensive du cyberespace :
Cyber sécurité, les actions de piratage informatique et les moyens de s'en protéger.
Cyber défense, l'utilisation du piratage informatique à des fins militaires et les moyens de s'en protéger.
Cyber espionnage, l'utilisation du piratage informatique à des fins de renseignement économique, technologique, politique ou militaire.
Cyber surveillance, les actions menées par un Etat pour surveiller sa population par des moyens numériques (par exemple : la reconnaissance de visages en Chine) et où par la censure d'internet et des réseaux sociaux.
Cyber guerre, affrontement entre plusieurs Etats, utilisant des moyens cyber.
Cyber criminalité, criminalité constitutive d'une infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau ».
La manipulation offensive des réseaux sociaux en les utilisant à des fins d'influence politique par la diffusion massive d'infox (***fake news***) ou d'informations confidentielles compromettantes.

Quelles sont les contre-mesures qui peuvent être prises ?
Par exemple les chinois ont fermés leur portes à Google et aux GAFAM américains (Google, Apple, Facebook, Amazon et Microsoft), y a -t-il d'autres moyens ?
Faudra t- il lancer une campagne de déstabilisation des réseaux sociaux ?
Nous ne devons pas nous contenter de l'analyse des conséquences, nous devons rechercher à remonter aux causes pour trouver les voies et moyens pour combattre ces dérives tout en conservant ses acquis positifs comme l'Intelligence Artificielle.
VADEMECUM pour ne pas se laisser « intoxiquer »



Pour l'agrandir, **cliquez ICI**

Retour au sommaire

Cybernétique « excursion » numérique

par **Xavier Raufer (*)**
Criminologue français

paru dans ESPRITSURCOUF.fr

La criminologie parcourt désormais deux univers – distincts mais qui toujours s'observent, se copient et souvent s'entremêlent : le *physique* et le *numérique*. Or si la criminalité du monde physique, terrorisme inclus, est vaguement sous contrôle, le chaos numérique est à présent déchaîné. Non-seulement les cyber-attaques d'ampleurs n'entraînent presque jamais de riposte et donc s'amplifient mais, surtout, aucun moyen efficace n'a été conçu pour les contrer. Cela tient notamment à la difficulté pour les États de définir les agressions numériques ainsi que les lignes rouges marquant une déclaration de guerre.

Or en France, cette inquiétante réalité tend à disparaître derrière une autosatisfaction de façade. Dans ses rapports, notre appareil officiel de lutte contre les cyber-menaces semble content de lui mais survole dans ses texte le cœur du problème, , tout comme la récente "Revue Stratégique de cyber-défense" (168 pages, février 2018) qui ne s'intéresse malheureusement guère à l'ennemi (pirate, État hostile, mafieux). A ignorer l'ennemi, comment "construire la paix et la sécurité du cyberespace international" ? Comment "anticiper", "prévenir", "détecter" des attaques, si on ignore QUI regarder et surveiller ; si l'on néglige la NATURE de la cyber-menace ?

Enfin, cet irénisme face aux cyber-bandits affecte toute l'Union européenne (UE), qui veut bien sûr instaurer un marché digital commun à ses pays-membres. Pour le "mois de la cyber-sécurité en Europe" d'octobre 2015, l'organisme dédié de l'UE, l'ENISA (*European Union Agency for Network and Information Security*) publie une liste de 40 enseignements et diplômes, au total 375 cours différents, dispensés dans la plupart des pays de l'UE. Leurs thèmes ? Là encore, que du calculable (…). On combat des nuées.

PROLOGUE – L'HOMME DE *SILICON VALLEY* – FRAGILE O COMBIEN [1]

"Sans patrie ni frontières" – étrange retour du rêve du Komintern. Dans le kaléidoscope post-hippie californien de *Silicon Valley* la bonne vie est sans attaches, mobile, flexible, fluide. Nouveau royaume des élus ? En fait, proies rêvées pour réseaux criminels, pirates, services spéciaux avides de piller cet aimable monde numérique.

DÉMONS ET MERVEILLES DE LA *SILICON VALLEY*

D'abord ceci : qui a su s'extraire de ce que la phénoménologie nomme "sphère des évidences courantes" est tout, sauf étonné de la domination des "titans du tech'" ci-après dépeinte. Bien au contraire, il s'en est convaincu, notamment en lisant ceci (1966) : "Nous méditons sur le phénomène du gouverner. Le phénomène est justement devenu aujourd'hui, à l'ère de la cybernétique, si fondamental qu'il met en cause et détermine toutes les sciences de la nature et le comportement de l'homme… Que les sciences de la nature et notre vie soient aujourd'hui

dominées dans une mesure croissante par la cybernétique n'est pas un hasard, mais est prédéterminé dans l'histoire de la naissance de la science et de la technique moderne"[2].

Dans notre monde un peu éloigné de la philosophie, les institutions, services, coordinations, états-majors, etc., instaurés pour combattre les nuisances numériques adhèrent plutôt à une logique d'ingénieur. Pour l'ingénieur, le cybermonde est dans l'idéal une vertueuse et fiable horloge ; des nuisibles en perturbant les rouages, il faut les réparer pour qu'après, tout aille bien. Or si une roulette du casino est *par construction* truquée au détriment du joueur, les meilleurs techniciens du monde ne pourront rendre "vertueuse" une machine dont la norme est de tricher. Exagération ? Non : d'emblée, ces frappants exemples de la vraie nature du GAFA *Facebook*, les autres (Google Apple, Amazon) ne valant guère mieux : à ses débuts, un journaliste demande à Mark Zuckerberg, PDG de *Facebook*, pourquoi le public lui confierait toutes ses données privées. Limpide réponse du libertarien assumé Zuckerberg "*They trust me – dumb fucks*" ("les pauvres cons me font confiance"), début 2018, sur *Facebook*, un expert découvre quelque 120 forums et groupes de discussion (± 300 000 – bien, *trois cent mille* – participants au total) consacrés au cyber-crime, au piratage, proposant à tout un chacun des logiciels et outils d'intrusion ou de vol numérique ; au vu et au su de tout le monde. Pourquoi se planquer sur le *Dark Web* ? Facebook est si accueillant…

Les formidables titans du net ont une idéologie et une pratique de pirates : là est le fondement de toute la cyber-criminologie. Commençons donc par là notre étude, en incitant nos lecteurs à bien ouvrir les yeux.

DES TITANS DU TECHNO-CAPITALISME, PLUS PUISSANTS QUE DES ETATS-NATIONS

Du seul fait des GAFA, la bourse américaine est en croissance continue depuis désormais 9 ans. De janvier à juin 2018, 50% des profits réalisés par les entreprises de l'indice *Standard & Poors 500*proviennent de Facebook, Alphabet (Google), Apple, Amazon et Netflix.

Amazon avait 17 000 salariés en 2007, 542 000 en 2017 ; la MOITIÉ de tout le *e-commerce* mondial passe par ses méga-serveurs. Apple et Google fournissent le *software* (logiciels, applications, etc.) de 99% des *smartphones* du monde. Google détient 81% du marché mondial des moteurs de recherche sur Internet. Sur tout dollar de publicité en ligne, Facebook et Google en raflent 59 cents. Ces deux sociétés captent par ailleurs 63% de la publicité digitale diffusée aux Etats-Unis. Croissance du chiffre d'affaires de la publicité digitale en 2017 : 89% au profit des deux mêmes.

LA GAFA-IDÉOLOGIE : CELLE DU RENARD DANS LE POULAILLER

Une récente étude (*NYTi* – 18/10/2017, cf. sources) révèle les opinions politiques de 600 influents patrons et hauts cadres du *high-tech* américain (1/3, de la Silicon Valley & environs). S'ils sont massivement libertaires, pour une dérégulation absolue et une immigration totalement libre (besoin d'esclaves à bon marché…), ils sont aussi hostiles à tout contrôle étatique et pour le licenciement sans limite. Le sociétal ne leur coûtant rien, ces sommités en suivent ardemment toutes les modes : stupéfiants et avortements libres, glorification LGBT etc.

Néanmoins, côté business ces patrons et hauts cadres du *high-tech* sont nettement moins sympa-progressistes. Chacun des deux milliards d'usagers Facebook possède sa propre fiche (race, sexe, revenu, pratique religieuse…) dont les données sont vendues à des fins publicitaires. Ces intrusives "*Ad Preferences*" rapportent à *Facebook* de un à trois milliards de dollars chaque trimestre. Toutes ces données privées extorquées dotent les GAFA de la plus formidable concentration de pouvoirs coercitifs de l'histoire du monde.

L'INCESTE DES "LIBERTAIRES" GAFA AVEC LE PENTAGONE, LA CIA, ETC.

Amazon a créé le *cloud* de la communauté américaine du renseignement ; *Microsoft* a suscité le *cloud*"*Azure Government Secrets*" (à usage du gouvernement fédéral, des Etats, du Pentagone, etc.) ; *Google*pilote le projet d'intelligence artificielle du Pentagone, etc. Quel comique a dit "neutralité du Net" ?

UNE POIGNE DE FER SUR LES MEDIAS ET L'INFORMATION PLANÉTAIRE

Facebook est le vrai "rédacteur en chef de la Terre" : 45% des Américains s'informent sur cette plateforme, 70%, sur *Facebook* et *Google*, deux entreprises privées contrôlant ainsi le paysage informatif de milliards de terriens. Une preuve de plus de la justesse du jugement de Karl Marx & Friedrich Engels (*L'idéologie allemande*, Ed. sociales, Paris 1962) : "Les pensées de la classe dominante sont aussi les pensées dominantes de chaque époque ; autrement dit, la classe qui est la puissance *matérielle* dominante de la société, en est aussi la puissance dominante *spirituelle*"[3].

DERRIÈRE LES MIRAGES DU NEO MONDE, DE CLASSIQUES TURPITUDES

Les techno-titans du jour agissent comme les bons vieux capitalistes d'hier : aliénation du personnel par voie d'ingénierie sociale ; faveurs sexuelles extorquées par chantage à l'emploi ou au fric ; ignorance des filous et escrocs de son genre.

- *La Silicon Valley fait "suer le burnous"* – (*NYTi* – 6/09/2017 – cf. sources) le monde de la tech fait l'apostolat de l'addiction au travail… Le *Burnout* suicidaire, expérience extatique… T Shirt populaire à *Silicon Valley* : "*9 to 5 is for losers*". Marche ou crève – quelle importance ? Des milliers de juvéniles gogos affluent chaque année dans la *Valley*. La propagande y pourvoit.
- *Puritanisme et "diversité", pour la galerie* – En surface, les élites de *Silicon Valley* adhèrent à toutes les inclusives "valeurs" du jour : droits des LGBT (etc.), "diversité", antiracisme, féminisme, véganisme, etc. Sous la pudibonde surface de la *Silicon Valley*, de récentes enquêtes dévoilent la culture de la partouze imprégnant ces *Boy's Clubs*. Le week-end, ces titans "invitent" leurs employées, ou celles de *start-up* adjacentes, à des soirées sexe-drogues-pouvoir dans de discrètes villas ou suites d'hôtels. Comment refuser des "invitations" lancées par qui régit votre avenir ? Quel public enfin, pour ces secrètes orgies ? Deux fois plus de jeunes femmes que d'hommes mûrs – tous blancs-hétérosexuels. La "Diversité", c'est pour la revue de presse.
- *Cyber-arnaques, arnaques quand même* – Juvénile *self-made-woman,* Elisabeth Holmes avait fondé et dirigeait la *start-up* Theranos, vouée à révolutionner les tests sanguins.

Permettant des centaines de millions d'économies aux systèmes de santé américains. Le banc-de-sardines médiatique s'embrase : couverture de *Fortune Magazine*… de *Forbes*… du *Time*… Coqueluche des médias ! Henry Kissinger au conseil de Theranos ! Des fonds de capital-risque déversent 900 millions de dollars sur la start-up-miracle. Tout était faux. *Silicon Valley*, médias, investisseurs, clients – tous bernés. A l'ancienne.

(*) **Xavier Raufer** Criminologue français, Directeur des études au Département de recherches sur les menaces criminelles contemporaines à l'Université Paris II.
Xavier Raufer écrit régulièrement dans http://www.atlantico.fr/

[1] Lire d'urgence le splendide "Beyond the map, Unruly enclaves, ghostly places, emerging lands and our search for new utopias" Alastair Bonnett – University of Chicago Press – 2018.
[2] Martin Heidegger (avec Eugen Fink) Séminaire "Héraclite",hiver 1966-1967, Gallimard, 1973.
[3] K. Marx et F. Engels disent aussi dans le *Manifeste du parti communiste* (1847) : "Que démontre l'histoire des idées, si ce n'est que la production intellectuelle se transforme avec la production matérielle ? Les idées dominantes d'une époque n'ont jamais été que les idées de la classe dominante".

Retour au sommaire

La défense et la sécurité de la France vue par le nouveau président Monsieur Macron.

par **Patrick Toussaint**

paru dans ESPRITSURCOUF.fr

Monsieur Macron vient tout juste d'être élu comme Président de la République Française mais il va devoir agir vite sur ces problèmes dont nous avions déjà rappelé l'urgence dans un précédent article.

Il a déjà défini la politique qu'il entend suivre dans ces domaines par des discours, des conférences de presse et de réponses faites dans des revues spécialisées dans ces domaines.

Il en ressort quelques axes de réflexion qui peuvent cependant évoluer car il souhaite faire une révision des menaces et avoir, pour la fin de l'année 2017, un nouveau Livre blanc.

Il est donc possible que de nouvelles priorités se dégagent de ce Livre blanc mais on peut en avoir quelques idées par son programme développé en tant que candidat à l'élection.

Il entend « donner aux armées les moyens d'assurer la souveraineté stratégique de la France ». Pour cela, il part de de la constatation des données stratégiques qu'il discerne à savoir :

- Un environnement en Europe modifié par le retour de la menace à l'est avec la Russie qui annexe la Crimée et provoque et soutient un séparatisme en Ukraine,
- La sortie de la Grande –Bretagne de l'Union européenne ce qui modifie les rapports entre les pays de l'Union notamment ceux de l'Europe de l'Est,
- La politique des Etats Unis avec le nouveau Président Monsieur Tromp et, de ce fait, la possibilité d'adaptation au niveau de l'OTAN sans pour autant envisager un départ de cet organisme ;
- La politique étrangère de la Chine qui cherche notamment à contrôler la Mer de Chine du Sud par où passe la moitié du trafic maritime mondial,
- Le réarmement des pays en Extrême Orient mais aussi au Moyen Orient qui change radicalement les données stratégiques dans cet espace
- La menace des terroristes qui se maintient aussi bien en France qu'en Europe et en Afrique et dans l'Extrême-Orient à partir de ses bases au Moyen Orient avec des groupes mieux équipés, plus réactifs et mieux entrainés,
- La nécessité de répondre aux Etats africains qui se heurtent à ces groupes terroristes,
- Les nouvelles menaces en matière de cyberguerre.
- Au plan national, il identifie les lacunes les plus criantes de la défense et de la sécurité notamment en matière de projection de forces et de matériels modernes.

D'où

1/ Au plan national et international :

- La réaffirmation que la France continuera à garder, maintenir et moderniser sa force de dissuasion nucléaire en gardant les deux composantes : la force sous-marine, la force aérienne et aéronavale.
- L'engagement de porter le montant du budget militaire au niveau de 2 % du PIB en 2025 avec une croissance tous les ans.
- La surveillance de l'emploi des fonds budgétés de sorte que tous les financements prévus soient investis selon le budget et réellement mis à la disposition du Ministère de la Défense.

2/ Les axes de renforcement de la défense et de sécurité sur le plan purement national :

- La lutte contre le terrorisme doit rester une priorité mais il faut avoir les moyens nécessaires – or, il fait le constat que cette lutte doit se faire tant à l'intérieur du territoire national que sur le terrain des terroristes à l'extérieur
- Sur le plan intérieur :
  - Cela implique de maintenir des troupes en France au montant de celui qui est en vigueur soit 7.000 à 10.000 hommes mais il faut, d'une part, repenser les modes d'interventions et d'autre part, les moyens nécessaires en termes de commandement, de logements et de véhicules et matériels, le dispositif actuel étant trop coûteux et mal adapté.
  - Ensuite, développer une garde nationale qu'il fixe à 85.000 hommes qui viendront des réservistes des armées, de la gendarmerie, de la police et des forces de sécurité : pompiers, sécurité civile …
  - Enfin compléter ces ressources par des engagements de réservistes qui sont actuellement dans la vie civile et qui pourront le faire grâce à une législation favorable aux chefs d'entreprise par le biais de financement et d'avantages permettant ainsi de laisser leurs employés avoir la possibilité de venir renforcer la garde nationale sans perdre leur emploi
- Sur le plan extérieur : les renforcements serviront à la fois sur le plan de la lutte contre le terrorisme et contre les autres nouvelles menaces
- Révision des menaces et vérification de l'adaptation des matériels à la menace,

Accélérer les programmes d'armement prévus en conséquence

Rendre le Maintien en condition –MCO-des matériels qui coûtent extrêmement cher afin d'avoir des taux de disponibilité à des niveaux acceptables

Renforcement des hommes et des matériels dans le domaine de la cyber guerre.

Développement des moyens de renseignement tactiques et stratégiques dans tous les milieux : terre, air, mer, espace et cybernétique.

3/ Monsieur Macron entend également agir sur le plan européen :

- Création d'un Quartier Général européen avec un réel pouvoir d'action et de suivi des opérations en liaison avec les états -major des pays européens et l'OTAN ;
- Un réel partage des services de renseignements,
- Activation des groupements tactiques – 1500 hommes prévus et jamais utilisés,
- Création d'un Conseil de Sécurité européen auquel participeront les militaires, les diplomates et les experts en renseignement,
- Un Fonds européen de Défense afin de financer des programmes militaires communs notamment les drones.
- Et de la sorte renforcer la base industrielle de défense européenne – BITD-

Cette action en faveur d'une politique de défense et sécurité au niveau européen sera proposée et mise en œuvre avec les états européens intéressés tout en restant ouverte aux autres états.

Retour au sommaire

Cybermenaces :
l'état français peut mieux faire

par **Xavier Raufer**
Criminologue français
Directeur des études au Département de recherches sur les menaces criminelles contemporaines à l'Université Paris II

paru dans ESPRITSURCOUF.fr

- ***1/ Le ministère de l'Intérieur souhaite renforcer les capacités numériques d'investigation des policiers, gendarmes et douaniers. Aujourd'hui, les moyens alloués aux autorités pour lutter contre le cyber crime sont-ils suffisants selon vous ?***

Le sommet de notre Etat est peuplé de gens nés avant l'ère digitale, comprenant mal l'immense révolution en cours. Pour eux, le cyber-crime est un problème parmi d'autres, une malfaisance de plus. Sauf exception, ces gouvernants n'ont pas digéré que toute l'architecture de la société n'est plus qu'un immense et proliférant enchevêtrement d'ordinateurs de toute taille, du calculateur géant à l'ordinateur portable et que là est l'effort de sécurité majeur des décennies à venir.
Votre banque, la météorologie nationale, l'hôpital qui vous soigne, la caisse qui verse vos prestations, la compagnie aérienne de vos vacances et l'aéroport où stationnent ses avions, tous ces prestataires de services, entreprises, etc. gardent peut-être des façades d'avant la société de l'information – mais désormais, leur cœur est à 100% numérique donc leurs fragilités et les nôtres, aussi.
Partant, l'appareil d'Etat devrait diviser en deux ses budgets de défense-sécurité : moitié pour le monde physique, moitié pour le numérique. Faire l'un sans l'autre est absurde. Hier, le *General Accounting Office*de Washington (une super-Cour des comptes américaine) révélait que les systèmes d'armes d'avant-garde des Etats-Unis – nucléaires y compris (facture, plus de 1 000 milliards de dollars) – avaient été piratés par des *hackers* qui, ayant percé leurs "protections", avaient changé leurs écrans en façade de flipper, exigeant deux pièces de 25 cents pour continuer la partie…
La vérité – nous le disons depuis des années – est qu'aujourd'hui le cybermonde c'est la Banque de France moins les coffres forts. Il suffit de se servir quand on sait faire. Voyez les géant *Facebook*, et *Google*, leurs centaines de milliards de dollars de capitalisation et la foule de cyber-génies à leur solde. Cette semaine, on apprenait que *Facebook* s'était fait piquer 14 millions de comptes de ses clients, avec données personnelles. D'usage, on réalise ensuite que c'est le double ou le triple. Il suffit d'attendre. Et *Google* obligé de fermer *Google+*, désossé par des pirates. C'est pareil toutes les semaines.

- ***2/ Comment expliquer cette pénurie ? Est-ce un problème de "vision", au sommet ?***

Tant que la prise de conscience évoquée ci-dessus ne sera pas faite, on mégotera. On continuera à édifier une ligne Maginot numérique, confiée à des ingénieurs super-compétents – mais sans culture criminologique, donc un peu naïfs face aux pirates. C'est une classique affaire de décision politique. Chacun sait qu'"est souverain celui qui désigne l'ennemi".

Plus largement : pénurie de moyens ? J'ignore – et je soupçonne que nul ne sait vraiment. Il faudrait d'abord un audit, suivi d'un diagnostic – après, déterminer l'effort financier à faire. Là, j'ai le pénible sentiment qu'on évoque des sommes, en plein brouillard.

- ***3/ Quels investissements prioritaires devraient être faits à la fois pour lutter contre le "grand" cyber crime mais aussi contre la délinquance numérique au quotidien ?***

L'investissement crucial est humain. Il faut créer ouvertement une unité de renseignement numérique – pas une bureaucratie de plus, un groupe expert dans un dispositif existant, l'ANSSI irait bien ; groupe voué à étudier l'ennemi numérique *et le dire* : qui sont les pirates dangereux ? Ou sont ils et que font-ils ? On devrait y arriver : dès 1914, l'Amirauté britannique créait "*Room Forty*", la "salle 40", pour percer les secrets de la flotte allemande de haute mer – ce que la "salle 40" fit fort bien. Identifions d'abord les pirates les plus toxiques ; sachons clairement attribuer les actes hostiles. Une *Room Forty* numérique, voilà pour moi ce qu'il nous faut.

- ***4/ Est-ce que des pays réussissent mieux que la France en l'espèce ?***

Je n'ai pas à procéder à une distribution des prix. J'observe que les pays qui réussissent en la matière ne sont pas paralysé par le politiquement correct, ni fascinés par les préciosités de langage. Des menaces de paralysie totale de notre pays existent bel et bien. Les voici, pour que ça soit clair. L'état d'un pays moderne, peu après un *blitzkrieg* réussi sur ses infrastructures énergétiques critiques, désormais à 100% informatisées. Le pays est débranché, effondré, avant même le premier coup de feu :

Quelques conséquences :
– Effacement de données cruciales,
– Pillage d'informations sensibles,
– Paralysie d'infrastructures critiques,
– Capacités militaires atteintes,
– Plus de réseaux financiers, cartes de paiement ni distributeurs de billets,
– Comptes en banque inaccessibles
– Plus d'appels possibles à la police (d'où, émeutes et pillages de masse),
– Plus de réfrigérateurs ni d'approvisionnement des grandes surfaces (nourriture épuisée en une semaine).
– Plus de contrôle des barrages hydrauliques, éoliennes, fermes solaires, etc.
– Plus d'électricité au bureau ni à la maison,
– Plus de services télécom, de téléphones portables ni d'Internet,
– Plus de services d'urgence ni de sécurité civile,
– Plus de trains ni de métros,
– Panne des dispositifs hospitaliers et de santé publique,
– Plus d'essence dans les stations,
– Arrêt des usines de traitement des eaux & ordures (ménagères, industrielles),
-….
Au lecteur de décider si le cyber est une menace fantôme.
Et si la politique de l'autruche est le moyen optimal de l'éluder.
Xavier Raufer écrit régulièrement dans http://www.atlantico.fr/

Retour au sommaire

Cyberdéfense,
la composante militaire indispensable

par les députés **Bastien Lachaud**
et **Alexandra Valetta-Ardisson**

paru dans ESPRITSURCOUF.fr

D'après un Rapport d'information déposé par la commission de la défense nationale et des forces armées en conclusion des travaux d'une mission d'information sur la cyberdéfense, rédigé par les députés Bastien Lachaud et Alexandra Valetta-Ardisson.

Une succession logique de 0 et de 1 au sein d'un code informatique binaire pourra-t-elle demain provoquer autant de dégâts qu'un missile de croisière naval ou qu'un obus tiré par un canon Caesar en rendant inutilisables des équipements, des matériels ou des infrastructures militaires ? Un virus aux effets systémiques, par la désorganisation massive qu'il provoquera, aboutira-t-il à la mort d'êtres humains, y compris des civils ? Comme le souligne la Revue stratégique de cyberdéfense publiée en février 2018 par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) : « Il est probable qu'une attaque informatique de cette nature [actes de blocage ou de sabotage des systèmes informatiques] aura, un jour, des conséquences létales. »

Ce qui pouvait relever hier encore de la science-fiction ou, du moins, de scénarios catastrophes dont on peinait à envisager le caractère réalisable à un horizon prévisible apparaît dorénavant comme une possibilité sérieuse, comme une menace tangible et comme une éventualité stratégique à prendre en considération en termes de doctrine militaire, de conduite des opérations et, plus globalement, d'organisation de la protection et de la résilience de l'ensemble de la société.

Les fondements de notre système de cyberdéfense ont majoritairement été posés dans le cadre des différentes lois de programmation militaire (LPM) adoptées depuis 2009. La prochaine LPM 2019-2025, votée les 27 et 28 juin successivement à l'Assemblée nationale et au Sénat, ne fait pas exception : un chapitre spécifique, le chapitre III du titre II, est consacré à la cyberdéfense.

Il faut souligner que :

- le cyber est par nature une réalité « universelle », globale, qui concerne peu ou prou tous les champs de l'activité sociale, aux niveaux local, national, européen, international.
- il s'agit d'un domaine extrêmement mouvant, en perpétuelle évolution ;
- les analyses menées dans ce domaine se heurtent vite à l'obstacle du secret de la défense nationale ;
- la Revue stratégique de cyberdéfense précédemment évoquée a déjà dressé un panorama très complet de la question, nous ne reviendrons pas sur son contenu.

Cet article s'attache plus particulièrement aux problématiques intéressant la défense, mais pas exclusivement, dès lors que le cyber irrigue tous les domaines et brouille les frontières traditionnelles entre les États, entre les acteurs, entre les secteurs.

De fait, le cyberespace est essentiellement composé d'éléments non militaires. Proportionnellement, seul un petit nombre de systèmes et d'équipements spécifiques est exclusivement de nature militaire les caractérisant comme des cibles légitimes au regard du droit des conflits armés. Dans le cyberespace, le rapport entre cibles militaires et cibles civiles s'inverse, du moins du point de vue quantitatif. Il s'agit là d'une réalité dont il faut tenir compte.

Le cyberespace n'en est pas moins devenu un champ d'affrontement supplémentaire, qui vient s'ajouter aux champs traditionnels : terre, mer, air et espace. Sa spécificité est qu'il existe en tant que tel, mais qu'il est également présent *à l'intérieur* de ces champs traditionnels, dès lors qu'une cyberattaque peut produire des effets non seulement dans le cyberespace, mais également sur les théâtres physiques.

La dimension cyber est donc dorénavant une dimension à part entière du domaine de la défense. Comme le rappelle le rapport annexé à la LPM 2019-2025 : « *En matière de lutte informatique offensive, de nouvelles capacités d'action, intégrées à la chaîne de planification et de conduite des opérations, seront systématiquement déployées en appui de la manœuvre des armées.* »

PARMI LES RECOMMANDATIONS de la Commission

Élaborer une loi « cyber »

- Élaborer une loi « cyber » portant sur la globalité des problématiques et des acteurs.

Recouvrer notre souveraineté numérique

- Créer des espaces de stockage souverains nationaux et européens afin de rapatrier et de stocker les données sensibles dans des territoires sous juridiction nationale ou européenne.
- Favoriser l'émergence de solutions techniques nationales et européennes de confiance.

Renforcer la résilience de l'ensemble des acteurs nationaux

- Durcir les dispositifs de prévention et de protection des autorités publiques et diffuser culture et prise de conscience du risque cyber par des actions ad hoc.
- Développer le recours aux bug bounties (1) au sein des autorités publiques.

Consolider une base industrielle et technologique de défense cyber

- Encourager la « cyber solidarité » entre grands groupes et sous-traitants.
- Financer la montée en gamme cyber des sous-traitants par un fonds cyber alimenté par les acteurs de la BITD (2) et une partie des recettes issues des exportations d'armement.
- Établir une cartographie régulièrement mise à jour des entreprises et compétences critiques au sein de la BITD.
- Améliorer la régulation concernant certains produits pour limiter la prolifération de technologies offensives et les risques cyber systémiques.
- Renforcer les capacités propres du COMCYBER (3) en matière d'expertise numérique.
- Renforcer les moyens budgétaires et humains de l'ANSSI (4).

- Soutenir le développement de la cryptographie et du chiffrement et investir, dans le développement de solutions « cyber-offensives ».
- Assurer le maintien en condition de sécurité des matériels d'ancienne génération. Ajuster la « ressource humaine cyber »

Soutenir la coopération internationale, par le partage des données et de l'analyse des menaces, l'approfondissement et la conclusion d'alliances.

(NDLR :Les extraits et notes complémentaires sont de la Rédaction d'ESPRITSURCOUF)

- Un **bug bounty** est un programme proposé par de nombreux sites web et développeurs de logiciel qui permet à des personnes de recevoir reconnaissance et compensation après avoir reporté des bugs, surtout ceux concernant des exploits et des vulnérabilités. Ces programmes permettent aux développeurs de découvrir et de corriger des bugs avant que le grand public en soit informé, évitant ainsi des abus. Les premiers bugs bounty ont été mis en place par de grandes sociétés américaines, en particulier les GAFA.

(2) OnNdivise traditionnellement la **BITD** (Base industrielle et Technologique de Défense) d'un pays en trois groupes d'entreprises :

- Ceux qui produisent des équipements stratégiques, à savoir le matériel militaire à proprement parler (systèmes d'armes et équipements létaux).
- Ceux qui fournissent des produits stratégiques non létaux mais permettant le fonctionnement des équipements de l'armée nationale, comme le carburant.
- Ceux qui fournissent toutes sortes de produits qu'utilisent les armées, comme les médicaments, les vivres.

Au sein de l'Union européenne par exemple, certains Etats membres, dont la France, militent pour le renforcement de la BITD de l'Union Européenne

- Le **Commandement de la cyberdéfense** (COMCYBER), placé sous l'autorité du Chef d'Etat-Major des armées rassemble à compter du 1er janvier 2017 l'ensemble des forces de cyberdéfense des armées françaises sous une même autorité opérationnelle, permanente et interarmées. Le COMCYBER est responsable de la protection des systèmes d'information placés sous la responsabilité du chef d'état-major des armées, de la conduite de la défense des systèmes d'information du ministère (à l'exclusion de ceux de la DGSE et DRSD) et de la conception, de la planification et de la conduite des opérations militaires de cyberdéfense, sous l'autorité du sous-chef d'état-major "opérations". Il est également responsable de la préparation de l'avenir et de la politique RH du domaine cyber.

Le COMCYBER assiste et conseille le ministre des Armées dans son domaine de compétence. Il dispose d'un état-major (EM-CYBER) avec un centre des opérations CYBER (CO-CYBER). Basé à Paris et disposant d'une antenne à Rennes, l'état-major est resserré et structuré en 3 pôles.

- L'**Agence nationale de la sécurité des systèmes d'information** (ANSSI) est un service français créé par décret en juillet 2009. Ce service à compétence nationale est rattaché au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale.

SUR CE SUJET VOUS POUVEZ AUSSI CONSULTER :

FOCUS

- Du N° 29 Cybersécurité, Cyberdéfense « La cybersécurité prise en charge par l'Etat »
- Du N°30 Cybersécurité, Cyberdéfense « Les sociétés de service : Risques pour les entreprises françaises ?
- Du N° 72 Innovation – Transformation numérique

VIDÉOS

- N°55 Souveraineté numérique
- N°72 les combattants du numérique

Retour au sommaire

Innovation-transformation numérique

Par le **GCA (2s) Alain Bouquin**

paru dans ESPRITSURCOUF.fr

Après le Billet du GCA(2s) Alain Bouquin dans le n°69 et le Focus du GCA(2s) Jean Paul Perruche dans le n°70 et du général (2s) Olivier Becdelièvre dans le n°71 nous continuons la publication d'articles sur l'avenir de l'armée de terre de la France.

De l'apport de l'innovation et du support numérique à l'outil de combat militaire

L'innovation semble être devenue **un thème particulièrement important** dans les déclarations récentes des autorités du ministère des Armées : le discours tenu illustre à la fois une ambition forte et une volonté de faire bouger les lignes. À juste titre car elle est la condition première du changement, des remises en cause, des progrès à accomplir pour demeurer en mesure de remplir les missions confiées, dans un environnement en perpétuel renouvellement. L'innovation n'est pas le simple synonyme de l'évolution technologique ; car la technologie n'est ni le seul vecteur, ni le seul objet de la transformation innovante des armées.

L'innovation est bien plus que cela : elle est **un état d'esprit, une culture**, dont l'objectif est la performance accrue dans tous les domaines. Elle repose sur la remise en cause, la curiosité, l'imagination, l'ingéniosité, l'esprit pratique. Elle traite des équipements, des organisations, des processus, des outils… Elle s'adresse à des domaines aussi variés que les capacités militaires, les soutiens, les ressources humaines, l'infrastructure, la santé ou l'organisation du commandement.

La haute technologie en constitue certes un des axes majeurs. On présente parfois la haute technologie comme une fatalité subie ou comme une forme de surenchère coûteuse. Elle est en fait tirée par le besoin d'efficacité des forces : mieux percevoir, mieux comprendre, décider plus vite, être plus précis, se déplacer plus rapidement, disposer de plus de puissance d'agression, être mieux protégé…E lle vise en règle générale à donner **un avantage décisif**, sur le terrain, dans chaque duel tactique. Sachant que ces avantages ne sont toujours que relatifs et temporaires. Ce qui pousse à vouloir en permanence explorer de nouvelles pistes, pour maintenir un écart significatif avec l'adversaire.

La transformation numérique, pour sa part, est probablement le principal moteur de l'innovation des années à venir. Tous les secteurs d'activités de notre pays sont touchés et tous ont compris qu'elle est incontournable pour rester compétitifs.

Il convient en premier lieu de dire ce qu'elle n'est pas : il ne s'agit pas d'une simple numérisation des processus ou des méthodes existants ; il ne s'agit pas de remplacer le papier et le crayon par l'ordinateur pour exécuter des tâches identiques ; car cela a déjà été fait. Il s'agit de profiter des opportunités offertes par le numérique pour transformer nos méthodes et gagner en efficacité. Ce n'est pas une révolution des outils, c'est une révolution des mentalités, des manières de faire ; c'est une transformation des forces armées en profondeur et en devenir.

Elle doit s'appliquer **dans deux directions** :

Organique, pour fluidifier au quotidien les tâches de la vie courante dans tous les domaines (RH, soutien, organisation…) ;

Opérationnelle, car elle est susceptible de provoquer une véritable transformation de la guerre, en particulier au niveau tactique.

Elle s'appuie sur quatre piliers désormais connus :

La connectivité : elle va permettre de généraliser l'Internet des objets, y compris sur le terrain, avec la mise en place à terme d'un véritable réseau des *« objets connectés du champ de bataille »* ; ces *« objets »* seront aussi bien les plates-formes que les capteurs ou les armes, mais également les hommes qui les servent ;

L'intelligence artificielle : ses deux applications majeures pour les armées sont l'aide à la décision et la robotisation ; elle permet d'aller vers le temps réel pour conduire à la fois les tâches de réflexion tactique et celles d'exécution, en acceptant des modes automatisés lorsque le tempo de la manœuvre l'impose ;

Le *"Big Data Analytics"* : c'est une technologie qui a pour objet de faciliter le traitement des masses de données produites ; ses attendus sont essentiels pour la tenue de situation opérationnelle et pour le renseignement : comprendre plus rapidement, disposer d'une vision plus claire de la situation, extraire les signaux faibles, synthétiser et fusionner les informations pertinentes…

Les technologies cyber : elles sont indispensables car sans elles les trois autres piliers peuvent se transformer en fragilités ; elles doivent être envisagées à la fois en mode défensif, pour assurer la résilience de nos forces, et en mode *« actif »*, pour intervenir sur les capacités de commandement de l'adversaire.

Le *« combat collaboratif »* est le fruit attendu de cette transformation. On pourra rétorquer que le combat a toujours été collectif… Il faut donc préciser cette notion. Elle doit viser à transformer divers actes tactiques élémentaires en actes *« réflexes »*, facilités par un bon usage des technologies numériques(protection mutuelle, suivi de situation amie, répartition des objectifs ou des appuis entre différents effecteurs…) afin de permettre aux chefs de concentrer leur réflexion sur ce qui fait l'essence de leur manœuvre et de l'atteinte de leur effet majeur. L'innovation à mettre en œuvre dans les quinze ou vingt années à venir, au profit de l'armée de terre, doit s'appuyer sur la transformation numérique pour en faire un amplificateur d'efficacité guerrière, dans le but de conserver un avantage sur les adversaires qui lui seront opposés. C'est une transformation qui s'articulera autour des notions de temps réel, de collaboratif, de souplesse tactique, de réactivité accrue… Elle ne pourra pas s'affranchir d'une réflexion profonde sur la transformation du commandement opérationnel.

Cet article fait partie du dossier n°22 réalisé par Le Cercle de réflexions du G2S « Réflexions pour l'armée de terre de demain » publié en juillet 2018 et consultable sur : http://www.gx2s.fr/

Retour au sommaire

Reportage
du journal de la défense

#JDEF

paru dans ESPRITSURCOUF.fr

« LES COMBATTANTS DU NUMÉRIQUE »

Date : 13 février 2018

Vidéo réalisée par : #JDEF

Durée : 00:13:25

#JDEF – Attaques informatiques, e-mails piégés, intrusions et tentatives de contrôle d´ordinateurs à distance… Tous les jours entreprises, particuliers ou services de l´État sont victimes de cyberattaques. Grâce à une veille de ses systèmes 24h/24, le ministère des Armées en déjoue chaque année des milliers. L´espace numérique est désormais devenu un champ de bataille comme les autres. Afin de mener à bien ses missions dans ce domaine, un commandement exclusivement consacré à la Cyberdéfense a été créé en 2017. Ce commandement met en œuvre des stratégies numériques inédites… avec un recrutement massif de « combattants » spécialisés. Qui sont ces soldats singuliers et comment sont-ils intégrés ? Nos équipes du Journal de la Défense (JDEF) vous emmènent à la rencontre de ces nouveaux profils.

Pour visionner la vidéo, cliquez sur le visuel

Retrouvez l'article **INNOVATION-TRANSFORMATION NUMÉRIQUE du GCA (2s) Alain Bouquin**

Retour au sommaire

Cybersécurité, cybercriminalité… quels défis posés a la sécurité intérieure par les opérateurs privés et publics ?

(partie n°2/2)

par **Olivier Chorand**
Sarah Pineau
23/10/2017

paru dans ESPRITSURCOUF.fr

Nous présentons cette analyse en 2 parties :

- *La semaine dernière « La cybersécurité prise en charge par l'Etat »*
- *Cette semaine « Les sociétés de service : Risques pour les entreprises françaises ? »*

2ème partie :« Les sociétés de service : Risques pour les entreprises françaises ? »

SOCIÉTÉS DE PRESTATIONS INTELLECTUELLES : UNE ACTIVITÉ A DOUBLE TRANCHANT POUR LA BONNE SANTÉ DES GRANDES SOCIÉTES FRANCAISES.

Dans les métiers du service, tout comme l'audit, celui dit du conseil est de plus en plus utilisé prenant la forme de prestation intellectuelles diverses. Les sociétés spécialisées se regroupent aussi bien sous le nom de sociétés d'audit ou de conseil que d'Entreprise de Service du Numérique (ESN), ex Société de services en ingénierie informatique (SSII). Elles se retrouvent sous la forme de grands groupes internationaux, de grandes et très grandes entreprises, ETI, PME, TPE, et aussi d'indépendants. Ces sociétés peuvent intervenir dans tous les secteurs d'activité, aussi bien sur le marché privé que public. L'action de ces acteurs spécialisés touche aussi bien les entités privées (Total, Axa, Thales, etc.) que publiques (ministères de l'Education, de la Défense, de l'Economie, etc.)

Sur le marché français, l'activité de prestation intellectuelle est devenue incontournable ou presque. De plus en plus, les sociétés privées et organismes publics – les « clients » – font appel aux services de ces sociétés – les « prestataires ». Les groupes étrangers sont nombreux sur ce marché, que ce soit de grands noms – Boston Consulting Group, Ernst & Young, Deloitte, Price Waterhouse Coopers, KPMG, IBM, Accenture, etc.- ou de plus modestes, qui représentent tout de même de grosses parts de marché : Bearing Point, Kurt Salmon, CGI, CSC… La France n'est pas en reste avec des acteurs comme Atos, Capgemini, Solucom, Sopra Group ou encore Orange Business Consulting. Au-delà du critère national, il est important de considérer le degré de notoriété de ces entreprises, ainsi que leur(s) secteurs d'activité. En effet, meilleure est la réputation d'une société, meilleur sera son positionnement sur des projets sensibles ou au sein de départements critiques d'entreprises ayant un lien direct avec les intérêts français. Par

exemple, les acteurs tels que BCG, EY ou encore Accenture, interviennent régulièrement sur des sujets stratégiques (intelligence économique, défense…) auprès des entités de direction.

Les failles cyber : entre menaces et opportunités

Bien sûr l'activité de services ne s'arrête pas à celles citées précédemment. L'entreprise privée ou l'entité publique sous-traite généralement une activité dont elle ne maîtrise pas le savoir-faire ou qui n'est pas son cœur de métier. C'est pourquoi peuvent être associés aux cabinets de conseil ou d'audit et ESN des cabinets d'avocats, pour des expertises en fusion acquisition par exemple, -ou encore des sociétés de sécurité ou de nettoyage. De fait, un cabinet d'avocats peut jouer un rôle parfois décisif à propos de décisions d'avenir de sociétés françaises s'il intervient dans les procédures de vente, d'achat, de cession etc.

Or si l'aspect cybersécurité n'est pas le premier sujet qui intervient dans ces activités, il facilite pourtant grandement l'apparition de vulnérabilités, voire les accentue. Prenons l'exemple d'une société américaine prestigieuse qui réalise l'audit des finances d'une société du CAC 40. Si celle-ci concurrence d'autres sociétés de cette même nation étrangère, il n'est pas impossible que des actions soient entreprises afin d'avantager les intérêts nationaux. En effet, un rapport sur l'état de santé financier de cette société française, pourrait être opportun pour le concurrent étranger dans le cadre d'un marché concurrentiel. Tout en restant sur le terrain des suppositions, la finalité serait similaire dans le cas d'un service Droit d'une société de service qui gère les cas de fusion acquisition de groupes français où les acteurs accèdent à des éléments stratégiques et vitaux.

Il est donc aisé de considérer qu'en termes d'intelligence économique, et même d'espionnage industriel, le champ des possibles est large. Ces scenarii ne sont certes pas nouveaux, mais les moyens qu'apportent les systèmes d'informations en tant qu'outils facilitent considérablement l'acquisition, la centralisation et le transfert d'informations.

Un couple soumis à aléas: une dépendance mutuelle et une cohabitation à risques

Bien sûr, les risques qu'encourent les sociétés françaises sur le plan des cyber-vulnérabilités et des failles intrinsèques aux sociétés de prestations ne sont pas uniquement de l'ordre du vol prémédité ou intéressé d'informations. Il suffit parfois d'observer le fonctionnement de procédures commerciales ou bien des comportements imprudents pour se rendre compte que le risque peut naître de nombreuses situations différentes.

Le point commun de ces sociétés de service est leur Business Model. Si l'on simplifie à l'extrême, on peut dire qu'elles tirent leur chiffre d'affaire de l'obtention de missions de prestation intellectuelle. Deux cas de figure se présentent : un engagement d'assistance technique ou un engagement au forfait. Le premier cas consiste en une obligation ressource : une activité interne est sous-traitée à un prestataire externe qui rapporte de l'argent pour chaque jour effectué (une mission peut avoir lieu au sein des infrastructures du client ou en dehors), alors que le second cas consiste en une obligation de résultats. Pour l'assistance technique, le chiffre d'affaires correspond au coût journalier du prestataire (taux journalier moyen) multiplié par le nombre de jours vendus, alors que pour un forfait le chiffre d'affaires ne tient pas compte des ressources ni de la charge allouée mais du résultat convenu. Dans un cas comme dans l'autre, un consultant qui n'est pas positionné sur une mission est considéré comme un centre

de coût pour l'entreprise, qui doit alors éviter d'avoir trop de salariés non positionnés en clientèle, sur une trop longue durée. Cette notion met ainsi en évidence les intérêts économiques des sociétés de service tout comme leurs objectifs stratégiques pour les remplir : multiplier les missions, s'assurer d'une pérennité d'affaires, absorber du savoir, élargir son réseau, avoir connaissance des besoins du client ou les « créer », se rendre indispensable… Cela permet de considérer aussi les méthodes de rentabilité et de se rendre compte des biais possibles et des divergences compréhensibles d'objectifs entre une société prestataire et un client.

Ces deux parties ont besoin l'une de l'autre : le client a besoin de ressources et de savoir-faire qu'il ne peut ou ne veut pas assumer, le prestataire de contrats de prestation pour « vendre » ses ressources et compétences, raisons pour lesquelles elles collaborent logiquement et de façon répétée. A l'heure actuelle en France, il existe donc une réelle dépendance des sociétés privées et entités publiques à la prestation intellectuelle. Aussi, nonobstant que la majorité des clients (grandes entreprises françaises ou entités publiques) possèdent une politique et une infrastructure de sécurité généralement de bon niveau, il est important d'évaluer leurs potentielles vulnérabilités en rapport avec les activités concernées par les besoins de prestations externes.

Une complexité qu'il est possible d'identifier relève de la nature même de cette collaboration. Des individus externes à la société cliente sont engagés pour travailler sur une matière interne parfois sensible. Il y a donc un déséquilibre notable. De plus, un prestataire travaillant pour une société de prestation est amené à intervenir chez plusieurs clients au cours de sa carrière et, par la suite peut être embauché par d'autres sociétés de service. Il devient alors légitime de se poser la question du respect de la confidentialité et de la loyauté vis-à-vis des clients. En outre si on en revient aux objectifs de chaque partie, la société de prestation acquiert une plus-value capitale des connaissances sectorielles et métiers, informations organisationnelles et fonctionnelles, qu'elle absorbe à travers ses salariés. Cette absorption se fait naturellement via l'apprentissage et l'expérience, mais aussi par récupération et extraction non autorisée (documents, organigrammes, données, codes, etc.).

Finalement, les vulnérabilités plus évidentes à identifier à propos des systèmes d'informations se retrouvent dans toutes les situations présentées (qui pour la plupart ne sont pas propres à la prestation intellectuelle) et concernent d'une part le matériel introduit (PC portables externes, clés USB externes) et d'autre part les comportements (comportements non responsables ou qui ne respectent pas les règlementations, utilisation non vigilante ou non appropriée des outils informatiques ou d'autres applications/sites, branchement de téléphones portables sur les ordinateurs, télétravail etc). Ces nombreux risques peuvent être négligeables mais peuvent également s'avérer catastrophiques et impacter gravement la santé de la société cliente s'ils ne sont pas correctement pris en compte.

Ainsi, bien que des clauses de confidentialité protègent ces collaborations, elles sont finalement limitées à la fois dans leur mise en œuvre et par la complexité d'identification des fautes. Il serait illusoire de contrôler toutes les activités des prestataires externes, que ce soit au sein de leurs locaux, de leurs outils informatiques nomades (contrôler l'extraction de données sur les disques durs ou via une plateforme en ligne de stockage de données, qui plus est étrangère car généralement le stockage est situé en dehors du pays et toute donnée est soumise à la législation du pays où elle est stockée, mais aussi qu'aucun fichier ne vienne affecter le système informatique), à travers un filtrage du réseau (extraction de données depuis la boîte mail externe

connectée au navigateur ou encore la réception de mails vérolés). Il est très compliqué pour la société cliente de s'affranchir de tous ces risques dont l'origine est généralement humaine. S'il est toujours possible de maximiser la protection des infrastructures d'une entreprise, le risque « zéro » n'existe pas. Aussi, la sensibilisation aux enjeux de cybersécurité, du côté du client comme du côté du prestataire, semble être une priorité voire une condition requise pour que la collaboration soit la plus sûre possible. Pourquoi ne pas imaginer une labellisation ou une certification des sociétés de service, à l'image du label « France Cybersécurité » existant et déjà remis par Axelle Lemaire, secrétaire d'Etat du Numérique, lors de l'édition 2015 du Forum International de la Cybercriminalité à Lille (1) ? Ce nouveau label ou cette nouvelle certification permettrait d'apporter une garantie supplémentaire sur la sensibilisation du prestataire aux enjeux de cybersécurité ainsi qu'un niveau d'exigence sécuritaire en termes de comportements et de confidentialité.

Avec la numérisation d'un grand nombre de processus métiers où pratiquement tous les secteurs d'activité sont concernés, il apparaît clairement que les systèmes d'informations et la place qu'ils tiennent dans la transformation des organisations et des métiers dans les entreprises, jouent un rôle critique au sein même de la chaîne de valeur de ces sociétés. Les entreprises sont aujourd'hui numériques et connectées et, de fait, leur savoir et leurs richesses sont à la merci des vulnérabilités du système et des interventions humaines : la cybersécurité est un enjeu de taille. En effet, d'une part beaucoup d'entreprises sont devenues dépendantes de telles collaborations avec des sociétés de service, et d'autre part, même si le critère de souveraineté est respecté, les autorités doivent s'adapter aux enjeux cyber, tout particulièrement en ce qui concerne les OIV. Il ne suffit plus de porter attention à la façade d'une société, il devient nécessaire afin d'évaluer plus complètement les risques cyber, de s'intéresser à ce qu'il se passe en coulisse, c'est-à-dire au cœur des interventions de ces sociétés de service qui interviennent au sein des opérateurs publics et privés. Le secteur de la cybersécurité a donc encore de beaux jours devant lui, car ces observations mettent en évidence de nouvelles problématiques sur lesquelles devront se pencher les acteurs leaders de ces marchés, que ce soit par le biais de formations, de solutions logicielles mais surtout de partenariats établis sur une culture de la cybersécurité. Il en va de la sécurité intérieure, économique comme stratégique, de notre pays.

Olivier CHORAND, Membre des Comités Sécurité intérieure et Cyberdéfense de l'ANAJ-IHEDN Auditeur Jeune de la 87e session, Paris, 2013
Sarah PINEAU, Membre du Comité Sécurité intérieure et Cyberdéfense de l'ANAJ-IHEDN Auditeur Jeune de la 91e session, Nîmes, 2015

1 J. Lausson « Un label France Cybersécurité remis à 17 entreprises », numerama.com, 21.01.2015, [en ligne], URL : http://www.numerama.com/magazine/31950-label-france-cybersecurity.html.

Retour au sommaire

Cybersécurité, cybercriminalité… quels défis posés a la sécurité intérieure par les opérateurs privés et publics ?

(partie n°1/2)

par **Olivier Chorand**
et **Sarah Pineau**
16/10/2017

paru dans ESPRITSURCOUF.fr

Nous présentons cette analyse en 2 parties :

- *Cette semaine « La cybersécurité prise en charge par l'Etat »*
- *La semaine prochaine « Les sociétés de service : Risques pour les entreprises françaises ? »*

1ère partie : La cybersécurité prise en charge par l'Etat

144 milliards de mails échangés dans le monde chaque jour, 30 gigaoctets de données publiées chaque seconde, 800 000 nouveaux sites web apparaissant quotidiennement, doublement de la quantité d'informations disponibles tous les deux ans… Ces chiffres (1) ont beau faire partie de notre quotidien, ils continuent à donner le vertige. Surtout lorsqu'on sait qu'à l'heure actuelle, moins de la moitié de la population mondiale est connectée.

Rouages essentiels de l'économie, porteurs d'innovations constantes et d'opportunités multiples… parce qu'ils sont désormais indispensables ou presque à la bonne marche d'une grande partie du monde, les systèmes d'information et de communication sont devenus en contrepartie à la fois cibles et responsables de menaces accrues, regroupées selon l'aspect que l'on veut mettre en lumière sous l'appellation « cybersécurité » (opportunité) ou « cybercriminalité » (menace). Un rapide état des lieux du champ de la cybersécurité telle qu'elle est définie en France permettra de rendre compte de l'importance de la problématique à traiter. Si le sujet est en partie pris en charge par des opérateurs étatiques ad hoc au vu de son importance stratégique dans un contexte mondial où la concurrence libre et non faussée est censée être la règle, il est également investi par des acteurs privés, ce qui est à la fois nécessaire, difficilement évitable mais non exempt de menaces pour la bonne santé des grandes sociétés françaises.

LA CYBERSÉCURITÉ, UN ENJEU MAJEUR

Selon le ministère des Affaires étrangères, la cybersécurité « recouvre l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre les nouvelles pratiques destructrices qui se développent dans le cyberespace : utilisations criminelles d'internet (cybercriminalité), espionnage à visée politique ou économique, attaques contre les infrastructures critiques (transport, énergie, communication…) à des fins de sabotage (2) ». En

2014, le coût de la cybercriminalité était estimé, au niveau mondial, à 445 milliards de dollars US par année (environ 400 milliards d'euros), soit l'équivalent du budget total de la France (3) . Et les prévisions futures ne sont guère réjouissantes : selon la société d'études Juniper Research, le coût des violations des données à l'échelle mondiale pourrait atteindre, d'ici 2019, 2100 milliards de dollars pour les entreprises (4) .
La France, et particulièrement ses entreprises, n'est pas épargnée par cette menace : dans 20% des cas, ce sont les organisations professionnelles qui sont visées et ceci leur coûte environ 3,36 milliards d'euros par an. Pour les banques et les entreprises françaises, le cybercrime est devenu la seconde source de fraude, derrière le détournement d'actifs. Selon une enquête menée par le cabinet de conseil PricewaterhouseCoopers «PwC» (5) , 45 % des sociétés de ce secteur qui ont été victimes d'un préjudice économique au cours des 24 derniers mois ont été touchées par des actes de piratage informatique. Une proportion à comparer à celle observée dans les autres secteurs économiques qui se limite à 17 %. Ces attaques, qui ont doublé en moins de deux ans (6) , touchent désormais autant les grandes entreprises que les TPE/PME : par exemple, ces dernières sont devenues la première cible des hackers dans le cadre de ransomwares (demandes de rançons pour récupérer des informations cryptées) car elles sont nombreuses à ne pas disposer de dispositifs de sécurité renforcés, et in fine, le taux de paiement de rançon y est plus élevé. L'importance des pertes qui en découlent s'explique par la valeur des données volées : brevets, plans stratégiques, etc. De fait, parce qu'elle est « un pays fortement industriel avec beaucoup de propriété intellectuelle, de grandes entreprises qui ont des secrets et des brevets qui intéressent des Etats ou des groupes qui visent la récupération d'informations confidentielles (7) », la France a, en 2015, fait son retour dans le top 10 des pays où la cybercriminalité est la plus active.

Face à ces attaques, les entreprises semblent bien démunies comme en témoigne le premier baromètre de la cybersécurité et de ses enjeux au sein des grands comptes français, réalisé par le Club des experts de la sécurité de l'information et du numérique (Cesin) en février 2016 (8) . Leurs doléances portent autant sur les moyens humains que matériels : 69% des entreprises sont mécontentes des niveaux de recrutement sur les postes de personnes en charge de la sécurité des systèmes d'information (SSI) que ce soit à la direction des systèmes d'information (DSI) ou à la direction des risques et de la sécurité et 58% des Responsables de la sécurité des systèmes d'information (RSSI) eux-mêmes s'estiment insatisfaits des outils informatiques disponibles sur le marché pour protéger leur système d'information. Au final, 93% des entreprises sondées n'ont, pour l'heure, confiance ni en leurs outils informatiques, ni en leurs fournisseurs, ni en leurs hébergeurs.

Le cyberespace, au vu de son étendue et de ses coûts, tant en termes de menaces que d'opportunités, est un enjeu grandissant pour les entreprises qui le prennent de plus en plus au sérieux. En France, la filière de cybersécurité représente plus de 600 acteurs et emploie 90 000 personnes dans le monde, dont 40 000 dans l'hexagone9 – Cette importance se mesure également à l'aune de la démarche volontariste de l'Etat en la matière, compte tenu des conséquences éventuelles pour la sécurité intérieure.

CYBERSÉCURITÉ ET SÉCURITE INTÉRIEURE

La Gendarmerie Nationale a été la première force de sécurité intérieure à se préoccuper de la cybersécurité, avant même qu'une stratégie nationale globale ne soit établie. Ainsi, alors que des discussions s'étaient engagées au niveau européen pour inscrire le renforcement de la lutte

contre la cybercriminalité comme priorité de l'Union européenne dans le programme européen de Stockholm de 2010-2015, elle a lancé dès 2007 la première édition du Forum International de la Cybercriminalité. Cet événement européen, qui se tient tous les ans à Lille, est dédié aux professionnels de la cybersécurité issus des sphères publiques et privées afin qu'ils confrontent leurs points de vue et leurs expériences. Le thème de 2017 est « Smarter Security for future technologies10 ». Les enjeux internationaux, filière cybersécurité, sécurité en entreprise, lutte anticybercriminalité, nouvelles technologies, questions de société ou encore technologies de sécurité seront quelques-uns des thèmes abordés lors de cette 10e édition.

Ce mouvement initié par la Gendarmerie s'est rapidement vu consolidé par une action gouvernementale et parlementaire. Lors de la révision en profondeur de la politique de défense et de sécurité nationale qui a donné lieu à la publication de deux Livres blancs en 2008 et 2013, la prévention et la réaction aux cyberattaques ont été identifiées comme priorités majeures dans l'organisation de la sécurité nationale, avec la création de nouvelles instances chargées de leur donner corps.

Tout d'abord, la mise sur pied en 2009 de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), agence interministérielle rattachée aux services du Premier ministre qui deviendra, deux ans plus tard, l'Autorité Nationale de défense des Systèmes d'Information. C'est également en 2011 que la France a publié une « stratégie nationale de défense et de sécurité des systèmes d'information » et créé un poste d'Officier général chargé de la cyberdéfense au ministère de la Défense. Cet Officier général coordonne l'action du ministère dans ce domaine et sert d'interface principale en cas de crise cyber. Par la suite, un Pacte Défense Cyber a, en février 2014, fixé les ambitions du ministère de la Défense jusqu'en 2019. Du côté du ministère de l'Intérieur, qui s'occupe de la lutte contre la cybercriminalité, un poste de préfet en charge de la lutte contre les cybermenaces a été créé en 2014.

Dernière avancée en date, l'actualisation en octobre 2015 de La Stratégie nationale pour la sécurité du numérique11, qui a fait l'objet de travaux interministériels coordonnés par l'ANSSI. Cinq objectifs y figurent : garantir la souveraineté nationale, apporter une réponse forte contre les actes de cybermalveillance, informer le grand public, faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises, renforcer la voix de la France à l'international.

La lecture de ces cinq objectifs fait comprendre que la politique nationale de cybersécurité ne s'arrête pas à la protection de la vulnérabilité de l'Etat et de celle de ses infrastructures, mais entend également intervenir dans celle des entreprises, avec plus ou moins de vigueur, selon l'enjeu critique de ces dernières.

De fait, en mars 2015, un décret renforçant les obligations en matière de cybersécurité des opérateurs d'importance vitale (OIV), à savoir les entreprises dont l'activité est jugée stratégique pour la nation, a été publié. Les 218 entreprises concernées, présentes dans des secteurs très divers (banques, opérateurs télécoms, grande distribution, etc.), doivent mettre en place des systèmes de détection des intrusions dont elles font l'objet et procéder à des audits, soit via l'Agence nationale de la sécurité des systèmes d'information (ANSSI), soit via des prestataires labellisés comme Thales. Ce texte, prévu par la loi de programmation de 2013, a tardé à voir le jour compte tenu de réticences fortes de la part des entreprises concernées, à la fois sur le fond et sur la forme. En effet, d'une part le coût des investissements à réaliser pour

se mettre en règle est conséquent, d'autre part, rendre publiques des attaques dont elles seraient victimes risque, selon elles, d'écorner leur image et in fine, de leur ôter des opportunités de contrats. Il existe donc un réel besoin de pédagogie pour faire comprendre l'intérêt d'une telle coopération entre l'Etat et les entreprises. Intérêt pourtant assez évident quand on voit les dégâts qu'a pu faire en 2010 le virus Stuxnet sur les centrifugeuses iraniennes de Natanz, ou, plus récemment le groupe de hackers baptisé « Dragonfly »,qui est parvenu à pénétrer les systèmes d'entreprises espagnoles américaines et françaises travaillant dans le secteur de l'énergie, à des fins d'espionnage.

Considérant les impacts majeurs de la cybersécurité sur la sécurité intérieure, l'Etat s'est efforcé de construire un cadre solide pour traiter cette problématique, à son niveau mais également à celui des entreprises, à partir du moment où celles-ci sont engagées dans des domaines d'importance stratégique. Reste à savoir comment les entreprises gèrent ce sujet en interne et, plus précisément les relations complexes qu'entretiennent les sociétés de prestations intellectuelles et les entreprises qui font appel à elles.

Olivier Chorand
Membre des Comités Sécurité intérieure et Cyberdéfense de l'ANAJ-IHEDN Auditeur Jeune de la 87e session, Paris, 2013

Sarah Pineau
Membre du Comité Sécurité intérieure et Cyberdéfense de l'ANAJ-IHEDN Auditeur Jeune de la 91e session, Nîmes, 2015

1 « 25-26 janvier 2016 : Forum International de la Cybersécurité (FIC 2016) à Lille » , supelec.fr, URL : http://www.supelec.fr/offres/gestion/actus_428_26320-1018/25-26-janvier-2016-forum-international-de-lacybersecurite-fic-2016-a-lille.html.
2 « La France et la cybersécurité », www.diplomatie.gouv.fr, [en ligne], URL http://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/defense-et-securite/cybersecurite/.
3 « Coût de la cybercriminalité : 400 milliards d'euros », www.ab-consulting.fr, [en ligne], URL : http://www.abconsulting.fr/blog/securite/cout-cybercriminalite.
4 « Cybercrime : un coût de 2100 milliards de dollars pour les entreprises d'ici 2019 », www.silicon.fr, [en ligne], URL http://www.silicon.fr/cybercrime-2100-milliards-dollars-entreprises-2019-116112.html#1Lwvwfq92Tq8cYPU.99.
5 « Sécurité : le cybercrime est la deuxième cause de fraude financière en France »,www.silicon.fr, [en ligne], URL http://www.silicon.fr/securite-pirates-ciblent-banques-france-93067.html#c6EEpWbpBV0rDARu.99.
6 « La cybercriminalité 2015 en 8 chiffres », www.solutions-numeriques.com, 01.04.2016, [en ligne], URL http://www.solutions-numeriques.com/la-cybercriminalite-2015-en-8-chiffres/.
7 « Cybercriminalité : La France dans le top 10 des pays les plus touchés», www.begeek.fr, 13.04.2016, [en ligne], URL : http://www.begeek.fr/cybercriminalite-france-top-10-pays-plus-touches-199627.
8 « Les grandes entreprises françaises ne se sentent pas prêtes à faire face à la montée des cyberattaques », [en ligne], URL www.expoprotection.com, 17.02.2016.
9 « 17 entreprises recoivent le label « France cybersecurity », 21.01.2016, [en ligne], URL http://www.solutionsnumeriques.com/17-entreprises-recoivent-le-label-france-cybersecurity/.
10 Une sécurité plus intelligente pour les technologies d'avenir

11« La Stratégie nationale pour la sécurité du numérique : une réponse aux nouveaux enjeux des usages numériques » www.ssi.gouv.fr, [en ligne], URL : https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/.

Retour au sommaire

Vidéo Marine nationale
« Présentation du Centre Support Cyberdéfense »

paru dans ESPRITSURCOUF.fr

Date : 27 mars 2017
Titre de la vidéo : « Présentation du Centre Support Cyberdéfense »
Source : Marine nationale
Thème de la vidéo : Cyberdéfense

Pour visionner la vidéo, cliquez ICI

Retour au sommaire