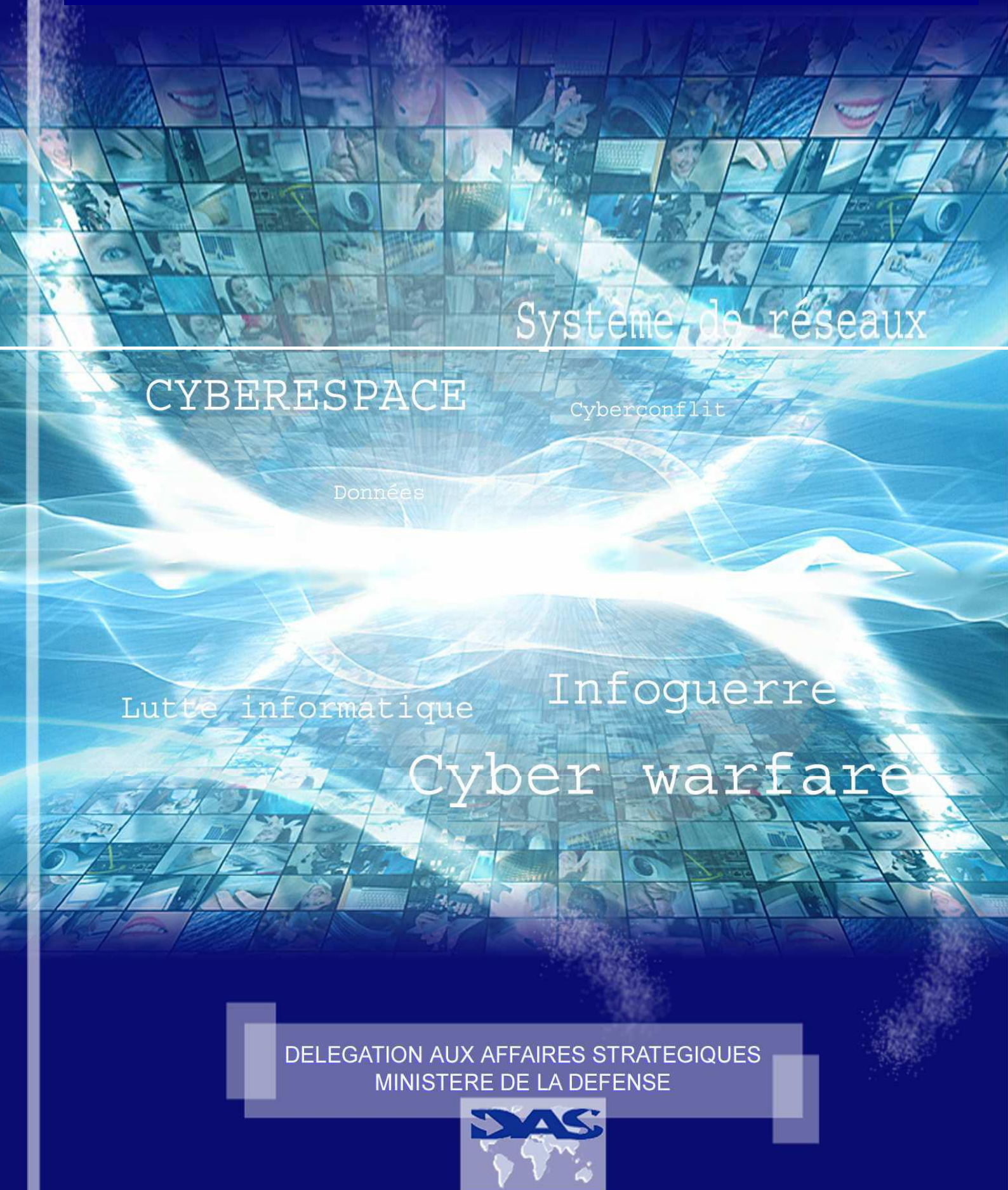
Observatoire du Monde Cybernétique
Trimestriel

Septembre 2012



DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

La Délégation aux Affaires Stratégiques propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation.

Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** cet Observatoire du Monde Cybernétique, sous le numéro de marché 1502492543.

Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Sommaire

1 Hacktivisme, quelles évolutions ?

Etat des lieux et perspectives à travers l'exemple des Anonymous et de leur écosystème

Le 15 septembre dernier étaient publiés en ligne les plans d'une base navale américaine. L'auteur de ce forfait : un individu se réclamant proche d'Anonymous, collectif de hacktivistes difficilement appréhendable. Début 2011, les médias annonçaient le piratage, encore par des individus se réclamant d'Anonymous, des comptes de l'entreprise de sécurité et défense américaine HBGary. Peu de temps après, son dirigeant, Aaron Barr, démissionnait.

Le potentiel de nuisance du hacktivisme n'est plus à démontrer. Pour défendre leurs valeurs et objectifs politiques que sont, par exemple, la liberté d'expression et le partage de la connaissance, certains n'hésitent pas à porter atteinte, à l'aide de moyens informatiques, aux intérêts étatiques, économiques, voire de particuliers. C'est pourquoi les autorités gouvernementales se sont saisies du sujet, en procédant à de nombreuses arrestations[1], faisant du hacktivisme une de leurs priorités.

Mais le hacktivisme, insaisissable par nature, évolue en permanence. Cette insaisissabilité pourrait être source de faiblesse : comment être efficace, cohérent, crédible auprès de l'opinion publique sans organisation spécifique ? En réalité, cela fait incontestablement leur force : imprévisibles, diffus, usant parfois de méthodes illégales, certains collectifs hacktivistes ne peuvent être démantelés par de simples arrestations ; leurs accointances avec la cybercriminalité en font des acteurs potentiellement dangereux ; il est également extrêmement difficile d'en établir des profils et de prévoir leurs prochaines cibles.

Afin de mieux cerner le phénomène, il est nécessaire d'en identifier les tendances actuelles, résultant d'une évolution constante depuis 4chan et les origines de collectifs tels que les Anonymous (1.1). Aujourd'hui, le hacktivisme semble tiraillé entre une radicalisation de ses modes opératoires, une coordination croissante de ses actions et une démocratisation de son idéologie et de sa communication (1.2). Cet état des lieux laisse entrevoir des mutations importantes à venir. Quel est l'avenir de ces mouvements ? Comment anticiper et appréhender leur potentiel de nuisance ? Sans trancher ces questions, il est toutefois possible de proposer des pistes de réflexion.

Si le hacktivisme ne se réduit pas aux Anonymous et aux collectifs gravitant autour de cette nébuleuse, c'est sur ces collectifs que porteront principalement ces travaux, l'ensemble de la sphère hacktiviste ne pouvant faire l'objet d'une seule et unique étude.

[1] http://www.madwatch.net/arrestation-de-25-hacktivistes-relies-a-anonymous/

1.1 Le hacktivisme, un mouvement de nature hétérogène

1.1.1 Tentative de définition d'un socle commun aux mouvements hacktivistes

Le hacktivisme, anglicisme apparu vers 1996 et issu de la contraction de *hack* (piratage) et d'*activism* (activisme), désigne à première vue l'usage de moyens informatiques afin de promouvoir des objectifs politiques. Les hacktivistes postulent en effet qu'ils pourraient produire des résultats similaires à ceux qu'entraînent l'activisme ou la désobéissance civile traditionnels.

Plus précisément, Alexandra Samuel propose[2] la définition suivante : *« le hacktivisme est l'utilisation non-violente d'outils digitaux illégaux ou transgressifs à des fins politiques ».* Cette définition permet tout d'abord de distinguer le hacktivisme des actes de cyberterrorisme, en tant qu'action non violente pour la vie humaine ; elle précise d'autre part la frontière entre hacktivisme et cyber-activisme, lequel n'emprunte pas de formes transgressives pour s'exprimer : le cyber-activiste se contente de transposer son « activisme » dans le cyberespace (par l'envoi de mail, par ses publications sur Twitter ou Facebook, par l'animation d'un blog…) tandis que le hacktiviste va au-delà, en utilisant ses compétences techniques pour passer outre les systèmes de sécurité et ainsi augmenter l'impact de son message. Si le cyber-activiste est l'internaute invitant à signer en ligne des pétitions contre le réchauffement climatique, le hacktiviste est celui qui pirate les comptes mails d'employés d'Exxon Mobil, BP, ou Gazprom et signe automatiquement ladite pétition avec ces comptes[3].

Le hacktivisme se distingue enfin des formes d'activisme dites « traditionnelles » qui ne se matérialisent pas « en ligne ». Sa finalité politique lui permet de se différencier du hacking pur et simple, dénué de motivation politique. C'est pour cette raison que le groupe Lulzsec n'est que rarement qualifié de hacktiviste, puisqu'il ne justifie ses actions que par le « Lulz », c'est-à-dire pour un amusement impertinent (« lulz » est une déformation employée par les hackers de l'expression « lol » - *loughing out loud* – qui représente plus ou moins le rire dans les discussions sur Internet et par SMS).

Le hacktivisme est une forme de participation « non-conventionnelle » à la vie publique et une des conséquences du déclin des partis politiques, de la désaffection générale des citoyens envers les institutions. L'essor d'Internet a non seulement renforcé cette réorientation citoyenne, les nouveaux mouvements contestataires - cyberactivistes - s'emparant de cet outil pour mieux se coordonner et s'informer, mais il a surtout généré une culture et des pratiques spécifiques, dont le hacktivisme est justement un produit.

Nous pouvons résumer les différents concepts évoqués par le schéma suivant :

---

[2] Alexandra SAMUEL, *Hacktivism and the Future of Political Participation*, Thèse de l'"Université de Harvard, Cambridge Massachusetts, septembre 2004, p.2 : "hacktivism is the non violent use of illegal or legally ambiguous digital tools in pursuit of political ends"

[3] http://pastebin.com/b79cJV5f

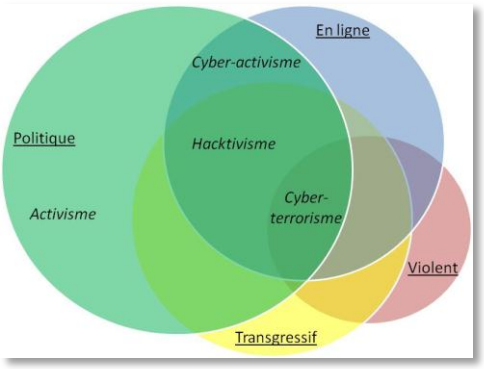


Figure 1. Source : CEIS

1.1.2 Des acteurs divers aux motivations variées

1.1.2.1 Une diversité d'acteurs

Le « hacktivisme » n'est pas un concept clair car il regroupe des individus aux profils très différents, aux compétences distinctes (qu'il s'agisse de *script kiddies* ou d'ingénieurs chevronnés). Le fait que, par nature et par nécessité, certains hackers dissimulent leur identité rend leur profilage moins aisé. Il est toutefois possible de distinguer les hacktivistes selon certains critères :

- **Mode opératoire :**
  - Certains « hackent » les médias, l'information (exemple : Anonymous)
  - D'autres sont des hackers de terrain, avec une logique de service[4] (exemple : Telecomix œuvre pour rétablir le net là où il est arbitrairement coupé)
- **Causes défendues :**
  - Altermondialisme
  - Liberté d'expression et neutralité du Net
  - Extrémisme religieux
  - Cause ethnique, transposition de conflits préexistants dans le cyberespace
  - Revendications autres (droits sociaux, conditions de travail, etc.)
  - Amusement (ils sortent ainsi du champ de l'« hacktvisme »)
  - Cause politique de façade permettant de mener des activités cybercriminelles (également hors champ)
- **Indépendance :**
  - Totale
  - Instrumentalisés / soutien étatique plus ou moins assumé
  - Origine purement étatiques : cybermilices
- **Compétences techniques :**
  - Script kiddies

[4] Frédéric Bardeau et Nicolas Danet, « Anonymous »

- Minimum de connaissances informatiques
- Véritables hackers
- Cadres (autorité historique de certains hacktivistes)

- **Anonymat :** plus ou moins prononcé.

Notons que l'âge importe peu, dans un contexte de « do-ocratie »[5], où seuls les actes comptent. Ainsi, des hackers âgés de 14 ou 15 ans peuvent rejoindre des groupes de hacktivistes et mener des actions essentielles. Frédéric Bardeau, auteur de l'ouvrage « Anonymous », relève cependant une tendance au sein de ce collectif de hacktivistes. Les membres arrêtés ont entre 15 et 40 ans, et sont issus de milieux professionnels variés. Les « N00b » ou « sang neuf » sont en général très jeunes et disposent d'un minimum de connaissances informatiques.

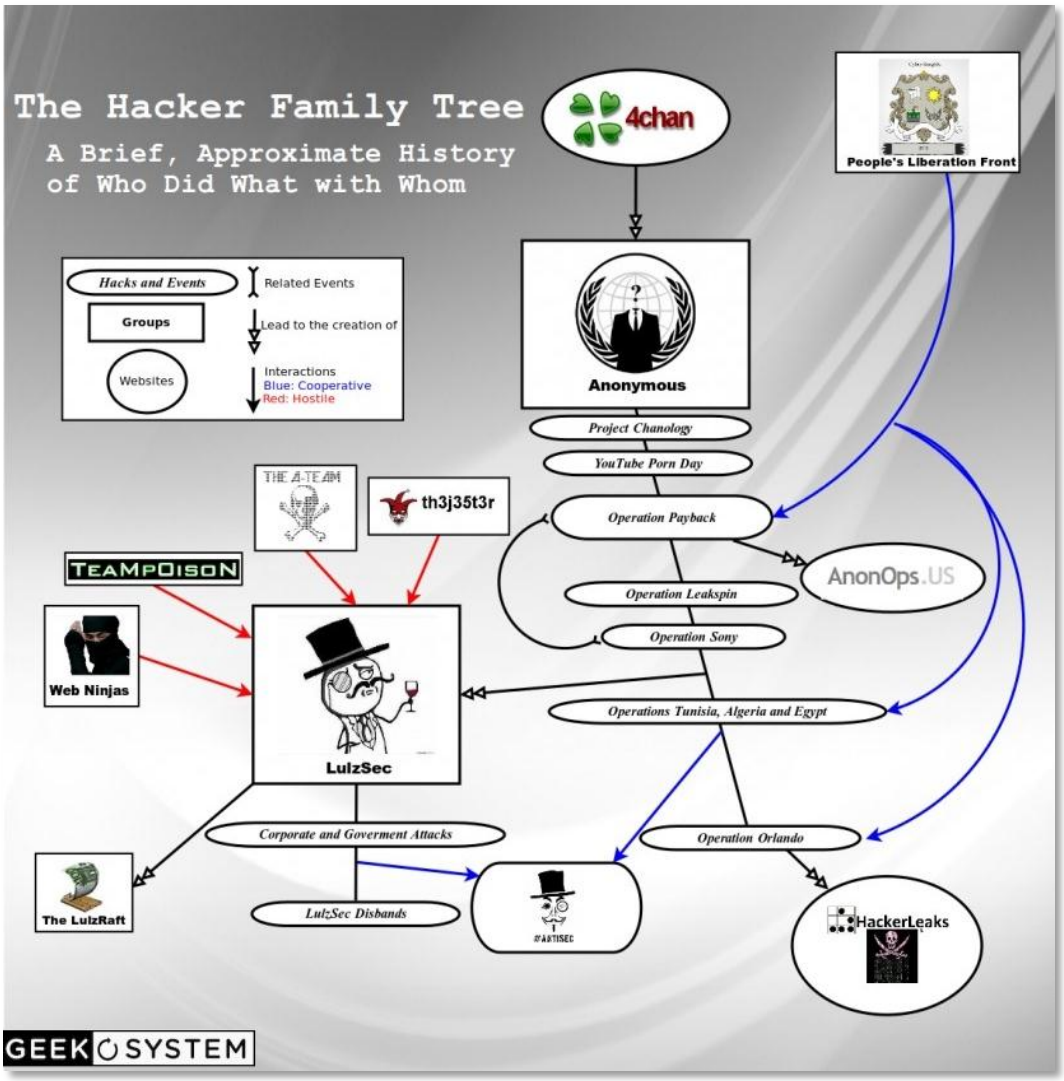


Figure 2. Schéma des principales opérations hacktivistes

[5] Les rapports entre membres ne sont influencés que par les actes, et non l'âge ou l'origine sociale.

Pour illustrer la diversité des acteurs ayant pris part aux opérations hacktivistes les plus connues jusque-là, des internautes ont schématisé un « arbre généalogique » représentant les groupes et sous-groupes gravitant autour des Anonymous et de 4chan[6] (voir ci-dessus). Si ce schéma est loin d'être exhaustif, y sont représentées les principales opérations d'Anonymous (Chanology, Youtube Porn day, Payback, Leakspin, Sony), les actions de soutien du *People Liberation Front* à certaines de ces opérations, la chronologie de création des sous-groupes Hackerleaks, Antisec , Lulzsec, et The LulzRaft, ainsi que l'hostilité qu'ont manifesté les groupes Web Ninjas, TeaMp0isoN, The A-Team, et Th3j35t3r à l'égard de Lulzsec.

1.1.2.2 Des motivations hétérogènes

Le hacktivisme se résume à l'usage de moyens informatiques transgressifs ou illégaux afin de faire faire valoir un message politique. Si l'objectif est le même, le message politique porté ou les modes opératoires adoptés divergent selon les collectifs.

Sur la question des moyens, les Telecomix ou les précurseurs du hacktivisme qu'ont été *The Cult of the Dead Cow* s'opposent par exemple frontalement aux Anonymous, dont ils jugent les méthodes illégitimes car illégales, donc dangereuses pour l'avenir du hacktivisme et des causes associées.

Sur la question des finalités, certains hackers souhaitent détruire le système dans son ensemble, comme les hackers soutenant les Illuminati :

Figure 3. Capture de tweet du compte @TheIlluminati

À l'inverse, les Telecomix revendiquent une action fondamentalement non-violente, ce qui se traduit concrètement par l'exigence du partage de l'information sans restriction et d'une liberté totale de communication (quelle que soit la nature de la communication), exigences regroupées sous le **concept de *datalove*** *:*

[6] http://www.geekosystem.com/wp-content/uploads/2011/07/phpTFPs66PM2.jpg

Figure 4. Capture de tweet du groupe Telecomix

Certains hackers, au premier rang desquels les Anonymous, prennent part à un grand nombre d'opérations (repérées par le préfixe #Op, par exemple #OpfreeAssange), tandis que d'autres ne deviennent hacktivistes que très ponctuellement, comme c'est le cas des membres de cyberpunks.com, ou de @_TeaMp0isoN, qui se sont notamment fait connaître par l'attaque par déni de service téléphonique contre les services du MI6.

Seul l'objectif de garantir la liberté d'expression semble faire consensus parmi les hacktivistes. Les mouvements hacktivistes semblent en effet souvent diriger leurs actions contre les multinationales, en particulier dans les domaines de la sécurité-Défense (comme HBGary), de la finance (banques notamment) et de l'énergie (par exemple #OpColtan[7]), ainsi que contre tous les instruments de surveillance et de répression (armée, police, services de renseignement, voire institutions de l'Etat en général). Nous savons ainsi que le collectif Telecomix est parvenu à rétablir l'accès à Internet d'un certain nombre de citoyens égyptiens ou syriens ainsi qu'à sécuriser leurs connexions lors des révolutions début 2011. La mise en place de sites miroir ou le détournement des lignes de téléphonie fixes pour les connecter à Internet et diffuser des outils de chiffrement a permis de contourner les censures gouvernementales.

En somme, les hacktivistes estiment que toute surveillance est néfaste. Si cette position semble radicale, elle participe d'une certaine forme de théorie du complot à laquelle de nombreux citoyens (grâce à l'essor de la société de l'information, entre autres) semblent[8] adhérer[9].

S'il est impossible de généraliser quant aux profils présents au sein de ces collectifs, force est de constater que les hacktivistes disposent d'un socle commun, et se rejoignent quant à leur conception du cyberespace privilégiant la liberté d'expression ou encore la neutralité d'Internet. Surtout, cette diversité intrinsèque au concept de hacktivisme s'illustre par les évolutions qu'ont connues ces mouvements durant ces dernières années.

[7] http://anonymouslegionops.blogspot.com/2012/09/opcoltan-other-datas-found-by.html

[8] Médiapart du 10 au 16 août : *Enquête sur les théories du complot*

[9] Numéro 47 de la revue Agone, coordination Miguel Chueca (maître de conférences en langue et civilisation hispanique à Paris Ouest-Nanterre).

1.2 Un mouvement aux évolutions ambivalentes – entre radicalisation, structuration et démocratisation du hacktivisme

Deux tendances majeures caractérisent les récentes évolutions des mouvements hacktivistes. Le cas des Anonymous est, à cet égard, l'illustration parfaite d'une posture illégale assumée, de plus en plus revendiquée. La première tendance est donc le renforcement des accointances des hacktivistes avec des pratiques illégales, plus radicales (1.2.1). La seconde est l'émergence de structures, d'outils permettant aux hacktivistes de se coordonner, de maximiser l'impact de leurs actions (1.2.2). Enfin, le hacking ne semble plus être l'unique moyen de diffusion de l'idéologie « hacker ». Certains souhaitant emprunter des voies plus classiques et légales (1.2.3).

1.2.1 Une posture illégale assumée, appelée à s'amplifier

1.2.1.1 Des modes d'action qui ne peuvent être qu'illégaux

Du point de vue de certains hacktivistes, la sécurisation, la régularisation et la militarisation du cyberespace, la mise en place d'outils de surveillance et le vote de projets de loi considérés comme liberticides [comme SOPA (*Stop Online Piracy Act*), PIPA (*Protect Intellectual Property Act*), ACTA (*Anti-Counterfeiting Trade Agreement*), ou encore la *McCain Cybersecurity Bill* et CISPA (*Cyber Intelligence Sharing and Protection Act*)] entretiennent un sentiment de répression sur Internet[10]. Face à ces initiatives jugés oppressives, les groupes comme Anonymous arguent n'avoir de moyen de révolte qu'illégaux :

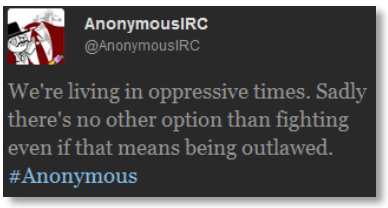


Figure 5. Capture de tweet

Ils s'arrogent alors le devoir moral de désobéir à des lois qu'ils jugent injustes :

[10] Par ailleurs, il semble que le développement de programme de surveillance n'ait pas vraiment été réfréné, seulement rendu plus discret, comme l'explique un agent démissionnaire de la NSA[10] et comme l'indique le stockage mentionné plus haut d'identifiants Apple.

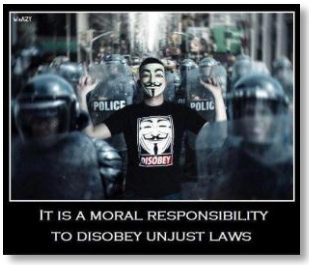


Figure 6. Capture de tweet

Ils retournent même l'accusation d'illégitimité en affirmant *« utiliser leurs connaissances, non pour violer la confidentialité des données des internautes, mais pour résister au système qui lui viole cette confidentialité »* :

Figure 7. Capture d'un message d'Anonymous

Enfin, en certaines occasions, comme celle de la tentative d'arrestation de Julian Assange réfugié dans l'ambassade d'Équateur, les moyens illégaux utilisés par les hacktivistes auraient pour finalité de « forcer » des Etats à respecter la loi (en l'occurrence la Convention de Vienne).

Figure 8. Capture de tweets

Ces hacktivistes semblent donc assumer et revendiquer l'usage de moyens illégaux afin de mener à bien leurs actions. Cette tendance, sur le point de se confirmer, pourrait toutefois desservir leurs finalités initiales, car instrumentalisées et décrédibilisées auprès de l'opinion publique.

1.2.1.2 Entre instrumentalisation et dérives des mouvements hacktivistes

François Paget chercheur chez McAfee, considère que certains hacktivistes sont manipulés par des gouvernements ou des criminels en raison de leur diversité et leur incohérence[11]. Deux groupes se distinguent alors : les cybercriminels, dont la motivation politique n'est qu'un vernis masquant des intentions bien plus pécuniaires, et les « hacktivistes d'Etat » parfois appelés cyber-patriotes qui, au contraire des hackers libertaires et « antisystème », intègrent pleinement l'Etat pour en devenir les hommes de main.

1.2.1.2.1 Le hacking patriotique, ou l'instrumentalisation du hacktivisme à des fins étatiques

Tendances majeures du hacktivisme aujourd'hui, les actions de hack « patriotiques » et associées aux conflits interétatiques sont désormais fréquentes. L'indépendance relative de certains groupes par rapport à l'Etat qu'ils défendent sous-entendent même une nature militaire de leurs actions. Ces groupes - souvent autoritaires - prétendent faire face à ce qu'ils décrivent comme des ingérences. Qu'il s'agisse de patriotes indiens, chinois, pakistanais, russes, défenseurs d'Israël ou de la Palestine, ces petits groupes mènent des actions systématiques et radicales contre toute personne portant atteinte aux intérêts ou à l'image de leur pays. Regroupés en « cyber-armées », ils louent ou mettent en place des réseaux de zombies (*botnets*), défigurent et détruisent les sites et messages de leurs adversaires.

Les opérations de ces « cyber-armées » sont cependant peu médiatisées : elles ne sont traitées que lorsqu'elles touchent des sites institutionnels critiques ou des figures politiques. Si leur manifestation la plus fréquente est la défiguration de sites, il n'est pas exclu que ces cyber-armées passent un jour à la vitesse supérieure avec des modes opératoires bien plus nocifs.

Ci-dessous quelques statistiques sur les sites défigurés[12] par les cyber-armées :

Motif de l'attaque	Nombre de sites touchés
Juste pour s'amuser	829975
« être le meilleur défaceur »	289630

[11] http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf
[12] http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf

Non disponible	94017
« Patriotisme »	58970
Autres raisons politiques	57083
Vengeance	45093
Défi	44457

Parmi les actions remarquables des cyber-armées, résultant souvent de la transposition de conflits préexistants au cyberespace, notons :

- Les attaques répétées de pirates indiens (*Indian Cyber Army*) et pakistanais (*Pakistan cyber Army*) les uns contre les autres depuis 2010 ;
- La défiguration de sites anglais par des pirates Roumains, après que les médias britanniques ont affirmé que Roumains et Tsiganes pourraient être un seul et même peuple ;
- La défiguration de sites palestiniens affiliés au Hamas ayant diffusé un dessin-animé mettant en scène le père du soldat israélien Gilad Shalit ;
- La défiguration de sites philippins le 27 août : les auteurs ont exigé une enquête après que huit touristes hongkongais ont été tués (le 23 août) à Manille, lors d'un assaut dans un bus où 15 personnes étaient retenues en otage ;
- une campagne de protestation lancée par des hacktivistes turcs contre le processus de reconnaissance du génocide arménien en France. Plus de 6000 sites ont été touchés, dont celui de Valérie Boyer, députée ayant initié le texte, et Patrick Devedjian, membre arménien du Parlement français ;
- L'attaque d'environ 40 sites gouvernementaux sud-coréens par déni de service distribué au cours de la première semaine de mars dernier.

Quelques exemples :

La Chine. Fin mars 2012, une campagne de hameçonnage vraisemblablement chinoise a visé des ONG[13] liées à la cause tibétaine : ces dernières reçurent un document Word exploitant une faille du bulletin de sécurité MS09-027. Le troyen infectant la cible permettait à l'attaquant d'avoir un contrôle total sur cette dernière. Selon des sous-traitants travaillant pour les services de renseignement occidentaux[14], certains salariés de Nanhao Group, (basé à Hengshui, province du

[13] http://www.comss.info/page.php?al=MacControl&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+comss%2Fsecurity-news+%28Comss.info+%7C+%D0%9D%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8+%D0%B8+%D0%9E%D0%B1%D0%B7%D0%BE%D1%80%D1%8B%29

[14] http://www.intelligenceonline.fr/intelligence-economique/2012/08/23/nanhao-group-la-victoire-en-hackant,106538295-ART-REC

Hebei), seraient hackers « à mi-temps » pour le compte de l'Armée Populaire de Libération (APL), tout en restant payés par leur employeur. Les pirates de Nanhao cibleraient plutôt des entreprises privées que les administrations d'Etats étrangers, cette dernière tâche étant réservée aux pirates informatiques travaillant directement pour l'APL. Le centre d'apprentissage de Nanhao est l'école de commerce international de Zhongxing (*Zhongxing Foreign Trade School*), et servirait de centre de formation au hacking pour les salariés du groupe, mais également pour des fonctionnaires d'Etat.

Le Moyen-Orient. En Syrie, les partisans de Bachar al-Assad, sous la forme de la « cyber-armée syrienne », livrent une guerre féroce aux activistes de l'Armée Syrienne Libre. Ils ont ainsi piraté le site AnonPlus[15], en représailles de la défiguration du site du Ministère de la Défense syrien le 09 août dernier. Ils ont alors remplacé la page d'accueil par des photos de soldats morts, accompagnées d'un message laissant entendre qu'en soutenant les opposants au régime de Bachar al-Assad, Anonymous soutenait l'organisation des Frères Musulmans (syriens).

1.2.1.2.2 Les dérives cybercriminelles du hacktivisme

Le 30 août 2012, le site blizzard.com.ua, site d'une communauté de joueurs ukrainiens dédiée aux produits de l'éditeur Blizzard, a été piraté[16] par des membres du collectif Antisec. 19 000 comptes ont été obtenus grâce à une injection SQL, dont 15277 emails valides. L'objectif de cette action n'a pas été précisé, mais les pirates ont toutefois annoncé : « *About time you get you Content Management Systems updated son?!* ».

Dans cet exemple, le vol de données personnelles n'est pas justifié, et bien qu'Antisec se revendique parfois hacktiviste, leur acte relève ici du piratage pur et simple. Et c'est bien ce pied dans l'illégalité qui pose problème aux hacktivistes. Certains d'entre eux allant jusqu'à alterner actes de piratage à des fins politiques et d'autres à des fins de renflouement financier.

C'est le cas d'Hector Xavier Monsegur (plus connu sous le pseudonyme « Sabu »), arrêté le 7 mars 2012 et ayant plaidé coupable pour les 12 chefs d'accusations requis à son égard (pour une peine maximale de plus de 124 années de réclusion)[17]. Il est notamment accusé d'avoir participé entre décembre 2010 et début 2011 à des attaques DDoS contre Mastercard, Visa, Paypal, ainsi que contre les gouvernements tunisien, algérien, et yéménite. Il aurait également défiguré le site du gouvernement tunisien, et tenté de voler des données confidentielles du gouvernement zimbabwéen. Sabu a admis avoir participé au piratage d'HBGary mentionné plus haut, ainsi qu'à celui de Sony Pictures et des sociétés de sécurité Infragard Atlanta (liée au FBI) et Unveillance.

Bien qu'ayant dirigé l'équipe Lulzsec, Sabu a montré qu'il avait réalisé des piratages pour de toutes autres raisons que le « lulz ». Il a notamment pénétré les systèmes d'une entreprise de pièces détachées automobiles pour se faire expédier quatre moteurs d'une valeur totale de 3450 dollars ;

[15] http://www.branchez-vous.com/techno/actualite/2011/08/anonplus_anonymous_defacage_cyber_armee_syrie.html

[16] http://www.peoplesliberationfront.net/anonpaste/?67afe56b63542031#eVbJpmINHVCZlQQySCiNeNmxq/nOzOhyM0kAgQznAEU=

[17] http://nakedsecurity.sophos.com/2012/03/07/sabus-sordid-story-detailed-in-fbi-indictment

dérobé les informations bancaires de deux organisations afin de payer plus de 1000 dollars de factures et revendre ces cartes à des tiers ; et usurpé l'identité de plus d'une douzaine d'internautes.

Les interactions entre cybercriminels et activistes se traduisent également par la fourniture d'outils de hack par les premiers aux seconds. Les hacktivistes fréquentent en effet les marchés noirs afin d'y trouver les outils nécessaires à leurs opérations : faux papiers, location de botnets, numéros de cartes bancaires permettant de financer d'autres projets, etc.

Le concept du cyberterrorisme

Le cyberterrorisme se distingue du simple usage d'Internet (blogs, forums…) à des fins de diffusion de messages politiques ou de recrutement dans le but de mener des actions terroristes classiques. Il pourrait être défini comme l'utilisation de cyberattaques à des fins de perturbation massive. Le terme est fortement discuté dans son acception, le terrorisme étant une notion elle-même controversée (usage de la terreur à des fins politiques) et les actes « cyber » difficiles à caractériser.

Comme le précise François Bernard-Huygue[18], les organisations terroristes ne semblent pas avoir franchi ce seuil - qu'elles soient religieuses, indépendantistes ou autres - bien que cela ne préjuge pas de leurs actions futures. Par conséquent, ainsi que l'interprète le vice-amiral Arnaud Coustillière, à la tête du commandement des forces de cyberdéfense françaises[19], si le concept du cyberterrorisme n'a jamais été observé en pratique, il constitue tout de même une menace, et doit être anticipé. Le concept reste toutefois une projection.

1.2.1.3 Des activités aux conséquences dommageables

Ces évolutions décrites ci-dessus ne sont pas sans conséquences. Conséquences pour la victime de d'abord. L'exemple de la chute de HBGary est à cet égard symptomatique. Conséquence pour les hacktivistes eux-mêmes ensuite, qui se voient décrédibilisées aux yeux de l'opinion publique.

1.2.1.3.1 L'impact pour la victime : l'exemple de la chute de HBGARY

HBGary Federal a attiré l'attention des Anonymous après que son CEO Aaron Barr a clamé qu'il était prêt à les divulguer l'identité de certains membres du collectif. Cette annonce devait avoir lieu lors de la conférence de sécurité BSides à San Francisco prévue alors pour Février 2011[20], au cours d'une intervention d'ailleurs intitulée « *Who needs NSA when we have Social Media?* » *(« Qui a besoin de la NSA lorsque nous avons des réseaux sociaux »*).

[18] http://www.huyghe.fr/actu_379.htm

[19] Discours prononcé lors du forum cyberdef-cybersec au salon de l'armement terrestre Eurosatory, 13 juin 2012

[20] http://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousandpaid-a-heavy-price

Les Anonymous ont rapidement pu accéder, grâce à une injection SQL menée sur le site www.hbgaryfederal.com, à une série de mot de passe critiques. Ces mêmes mots de passe étaient utilisés sur divers comptes sociaux tels que Twitter ou LinkedIN, et surtout sur les messageries électroniques des membres de la société, dont celle d'Aaron Barr, CEO de la société. C'est ainsi que les Anonymous accédèrent à des quantités astronomiques de sauvegardes (sur le serveur SSH support.hbgary.com). Après avoir obtenu, par ingénierie sociale, un accès administrateur au serveur de rootkit.org, les Anonymous subtilisèrent des documents révélant des activités jusque-là très discrètes de la société. HBGary Federal avait en effet travaillé étroitement avec *Bank of America* afin de répondre à la publication de documents confidentiels diffusés par Wikileaks. Ces révélations ternirent l'image de HBGary, et poussèrent l'ensemble des sociétés impliquées (dont la chambre de commerce américaine, Palantir Technologies, et Berico) à se distancer du géant de la sécurité. Ces révélations ont précipité la démission d'Aaron Barr de son poste de CEO et engendré des pertes financières catastrophiques pour la société.

1.2.1.3.2 Un impact négatif pour les hacktivistes

En fait, les « déviances » des hacktivistes ont des répercussions sur leur propre action, et sur celles des organisations qu'ils prétendent parfois défendre (syndicats, ONG…). Or la communication et le positionnement vis-à-vis des médias est au cœur de la stratégie de la plupart des mouvements hacktivistes : maîtriser leur image devient dans ce contexte un enjeu fondamental.

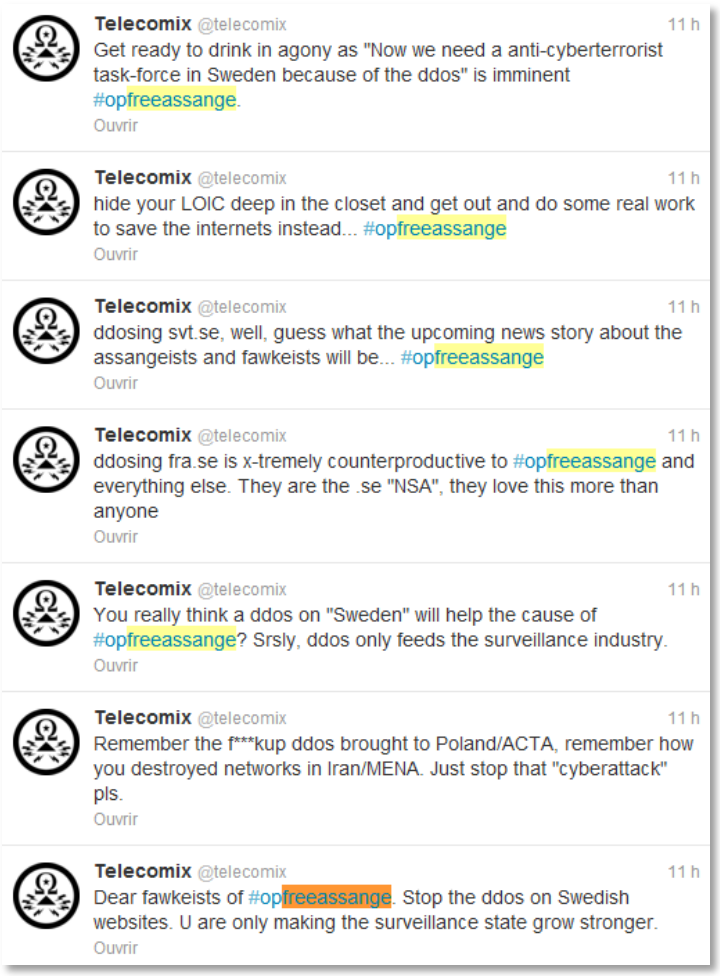
Le caractère illégal de l'action des hackers remet d'abord en cause la légitimité de leur action et nuit à leur propre image auprès du public, pouvant les considérer comme des cybercriminels se cachant derrière des motivations politiques. Il peut ensuite nuire aux hacktivistes et activistes traditionnels qui auront choisi de rester dans le cadre de la loi.

Cela est source de controverses entre hacktivistes, comme l'illustre le débat qui a opposé Telecomix et Anonymous, les premiers dénonçant notamment les attaques *DDoS* des seconds :

Figure 9. Capture de tweet des Telecomix

Telecomix n'est pas seul à rejeter ce mode d'action puisque sur le lien proposé par ce tweet - torrentfreak.com/… - le site de partage de torrents The Pirate Bay (TPB) promeut un Internet *« libre et ouvert, où chacun peut exprimer ses vues »,* et réprouve par conséquent les blocages - auxquels participent les attaques DDoS - comme autant de manifestations de censure. Les premiers acteurs du hacktivisme se montrent eux-mêmes réticents à l'endroit des modes opératoires d'Anonymous. Depuis décembre 1998 où des hackers ont attaqué l'Iraq et la Chine au motif que ces pays ne respectaient pas la liberté d'expression, les mouvements Cult of the Dead Cow (cDc), L0pht, Chaos Computer Club et hacker mags 2600 s'opposent fermement *« à toute tentative d'utiliser le pouvoir*

du piratage pour menacer de détruire l'infrastructure informationnelle d'un pays. » Car, selon eux : *« on ne peut légitimement espérer améliorer le libre accès à l'information d'une nation en travaillant à endommager ses réseaux de données*[21] *».*



« Soyez prêts à boire dans la douleur. Attendez-vous à des déclarations telles : « Maintenant nous avons besoin d'une force anti-cyberterroriste en Suède en raison des [attaques] DDoS ».

Cachez votre LOIC profondément dans vos armoires et dotez-vous d'un véritable emploi pour sauver les internets à la place…

Attaquer par DDoS fra.se est extrêmement contre-productif pour #opfreeassange et tout le reste. Ils sont la « NSA » du .se, ils aiment ça plus que quiconque.

Vous pensez vraiment qu'un ddos sur « la Suède » aidera la cause #opfreeassange ? Sérieusement, les ddos nourrissent uniquement l'industrie de la surveillance.

Souvenez-vous du ddos fou en Pologne pour ACTA, souvenez-vous comme vous avez détruit les réseaux en Iran pour MENA. Stoppez cette « cyberattaque » svp.

Chers « partisans de Fawkes » d'#opfreeassange. Stoppez les ddos sur les sites suédois. Vous ne faites qu'accroître l'Etat de surveillance

Figure 10. Capture de tweets relatant la position des Telecomix

Cette radicalisation des modes opératoires de certains hacktivistes ne fait donc pas l'objet de consensus. Bien au contraire, elle divise et oppose les hacktivistes entre eux. Mais à côté de cette image d'un mouvement désorganisé, diffus et incohérent émergent certaines initiatives traduisant une structuration et une organisation croissante des hacktivistes.

1.2.2 Un hacktivisme qui se structure et s'organise à des fins d'efficacité collective

Les activités de hacking menées par certains groupes hacktivistes se coordonnent grâce à de nouveaux outils aux usages presque standardisés. Mieux encore, ces hacktivistes développent des capacités de renseignement et d'infiltration considérables.

[21] http://news.cnet.com/8301-27080_3-57406793-245/old-time-hacktivists-anonymous-youve-crossed-the-line

1.2.2.1 La coordination de cyberattaques grâce à Loïc, Hoïc, Slowloris et l'usage de serveurs IRC.

Parmi les outils d'attaque collaboratifs utilisés par un groupe comme les Anonymous, se distingue le plus connu : LOIC (*Low Orbit Ion Cannon*). C'est une application de test de réseau développée par Praetox Technologies. Elle permet d'inonder un serveur cible avec des paquets TCP ou UDP ; elle a notamment été exploitée au cours du projet Chanology qui visait les sites de l'Eglise de scientologie, puis à partir de septembre 2010 et de la version 1.1.1.3, pour l'opération #OpPayback[22].

LOIC est extrêmement simple d'utilisation. Son option « Hivemind » permet par exemple de récupérer les coordonnées d'un serveur IRC cible et de lancer automatiquement une attaque à son encontre. Rappelons que les serveurs IRC (du nom du protocole qu'ils implémentent : *Internet Relay Chat*) sont la base structurelle de la communication entre hacktivistes : il s'agit de serveurs sur lesquels sont installés un programme (appelé IRC daemon[23]) permettant aux utilisateurs connectés de discuter en temps réel par le biais du protocole IRC. L'inconvénient de LOIC est la facilité avec laquelle l'adresse IP de l'attaquant est repérable. C'est pour s'affranchir de cette vulnérabilité que HOIC (*High Orbit Ion Cannon*) a été développé. N'importe qui peut utiliser HOIC, et c'est bien cette capacité de démocratisation qui le rend dangereux. Avec ce logiciel, lancer une attaque se résume à entrer les coordonnées (l'adresse IP) de la cible et cliquer sur « feu ».

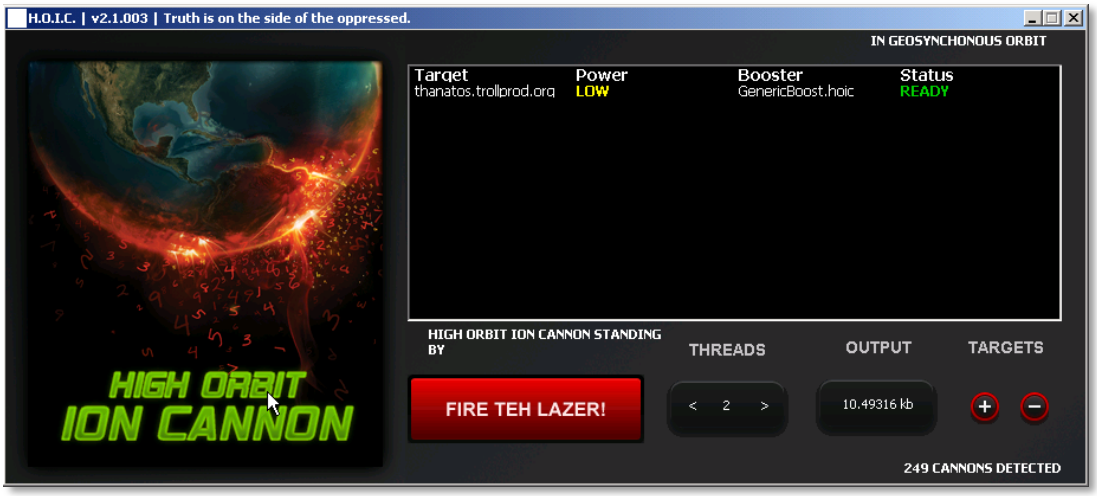


Figure 11. Capture de HOIC

HOIC délivre des requêtes HTTP à un rythme qui dépasse largement celui permis par LOIC et permet d'envoyer des requêtes à plusieurs sites cibles simultanément. Concrètement, ce sont des scripts personnalisés - dits « boosters » - qui alimentent un trafic malveillant à travers plusieurs pages d'un même site : par exemple, au lieu d'attaquer « site.com », un script booster attaquera

[22] http://fr.wikipedia.org/wiki/Operation_Payback

[23] processus qui s'exécute en arrière-plan plutôt que sous le contrôle direct d'un utilisateur : http://fr.wikipedia.org/wiki/Daemon_(informatique)

« site.com/about.htm », « site.com/news.htm », etc. ; le tout en faisant provenir les attaques d'une multitude de points distincts, afin de limiter le traçage (et de blocage par les pare-feu) de l'attaque.

Enfin, l'outil SLOWLORIS permet à un attaquant unique de réaliser à lui seul un déni de service[24]. SLOWLORIS, bien que plus efficace que LOIC et HOIC, est cependant aussi peu anonyme que LOIC. Son usage se fait donc en général à l'aide d'un VPN ou de proxys d'anonymisation.

Ces outils, largement diffusés au sein des communautés hacktivistes, permettent à tous ceux souhaitant rejoindre un mouvement, d'apporter leur pierre à l'édifice. L'action des membres des collectifs de type Anonymous est donc cadrée, canalisée par des outils fédérateurs et extrêmement simples d'utilisation.

Mais ces groupes hacktivistes vont plus loin que le simple DDoS et le vol de données en développant, à l'image d'une agence structurée, des capacités de renseignement, voire d'infiltration.

1.2.2.2 Le développement de capacités de renseignement et d'infiltration

1.2.2.2.1 Par:Ano IA

Il s'agit de l'agence de renseignement du collectif Anonymous. Son ambition : révéler toutes les informations qu'ils découvrent. Selon les administrateurs de la plateforme, l'information est un bien libre qu'une certaine « aristocratie » s'efforcerait par tous les moyens de contrôler, au détriment des citoyens.

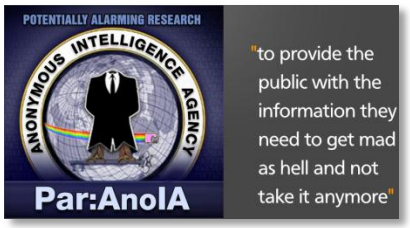


Figure 12. ***Pour fournir au public les informations dont ils ont besoin, et les rendre fous furieux au point qu'ils ne supportent plus une telle situation***

« Vos secrets seront révélés à chaque paysan que vous connaissez. Chaque pièce de parchemin sur laquelle sont écrits de sales mensonges nous rendra plus coléreux et plus forts. Nous nous honorerons nos marins tombés et ne changerons pas de cap. Vous ne nous stopperez pas car vous ne le pourrez pas. Méfiez-vous de nous », ont-ils eu l'occasion de diffuser sur leur site.

[24] SLOWLORIS étouffe les sockets d'un serveur donné en envoyant périodiquement un header (partie minimale d'une requête HTTP) avec une période juste en-dessous du délai d'expiration du traitement de ce header par le serveur distant. Et ce jusqu'à ce que le serveur ne puisse plus attribuer de socket à une connexion légitime.

L'objectif du site Par:AnoIA est également d'éduquer et d'impliquer les citoyens dans l'analyse des données révélées, ce qui représente une innovation considérable par rapport à Wikileaks, considérée comme une source d'information certes vaste, mais inexploitable.

1.2.2.2.2 L'infiltration dans les services de renseignement

Certains collectifs de hacktivistes disposeraient également d'entrées dans certains services de renseignement. Selon Christopher Doyon (alias Commander X) accusé d'avoir organisé une attaque par déni de service distribué l'année dernière aux côtés des Anonymous, le collectif aurait accès à n'importe quelle information classifiée aux Etats-Unis[25], le général Keith Alexander et le Secrétaire Général à la Défense ne contrôleraient en réalité plus rien, ce que l'affaire Bradley Manning (Wikileaks) illustrerait. Ces allégations ne peuvent cependant être vérifiées en raison de l'anonymat caractérisant les actions de certains collectifs de hacktivistes.

Autre exemple : le groupe de hackers turcs RedHack (composé de 12 membres et des millions de supporters), prétend[26] compter parmi ses membres et sympathisants des ingénieurs de l'agence de cybersécurité turque, dépendant du Conseil de Recherche Technologique et Scientifique (TÜBITAK).

La tendance est donc au renforcement, à la coordination de l'activité des collectifs de hacktivistes tels qu'Anonymous. Ils se structurent et s'appuient sur des méthodes rodées, éprouvées, et se dotent d'infrastructures de renseignement. D'autres souhaitent cependant aller plus loin, emprunter d'autres voies afin de diffuser autrement les valeurs « hacker » telles que la liberté d'expression et le partage de l'information. Leur objectif étant de peser au sein du paysage politique, soit à travers une formation politique, soit à travers la défense de la nature militante de leurs actes.

1.2.3 La diffusion de l'idéologie « hacker » par des canaux de revendication plus classiques

Le hacktivisme semble emprunter des voies plus traditionnelles à travers la volonté exprimée par certain de se « légaliser » et l'émergence de partis politiques diffusant leurs valeurs de liberté d'expression.

1.2.3.1 L'émergence de partis politiques défendant des valeurs « hacker »

L'idéologie hacker peut être véhiculée par d'autres moyens. Les différents Partis pirates en sont l'illustration. S'ils sont encore minoritaires en France, ils organisent déjà de nombreuses actions en Suède et en Allemagne[27].

---

[25] http://rt.com/usa/news/anonymous-us-doyon-world-219

[26] http://www.hurriyetdailynews.com/hacker-group-says-to-have-friends-in-anti-hacker-team.aspx?pageID=238&nID=28489&NewsCatID=338#.UDcbWp8-dvA.twitter

Le paysage politique allemand, longtemps stable, subit en effet actuellement des modifications profondes[28]. Les partis traditionnels ont de plus en plus de mal à attirer les électeurs et de nouveaux partis obtiennent désormais régulièrement des mandats aux élections locales et régionales. Depuis son affirmation à l'automne 2011, le Parti pirate est au cœur de ces évolutions, étant le seul en mesure de réussir son entrée au Bundestag. Cette formation politique qui fédère initialement les partisans de la défense des libertés liées à Internet, a également attiré un électorat protestataire qu'il tente désormais de stabiliser. Notons toutefois que si leur mode de fonctionnement multi-centré a été un réel atout pour les périodes électorales, il s'est révélé très peu efficace lorsqu'il s'est agi de formuler un programme politique complet. Pourtant, leurs succès électoraux récents (9% aux élections du Land que représente la ville de Berlin) ont montré qu'il faudra nécessairement les intégrer dans la formation de gouvernements futurs.

1.2.3.2 Vers une évolution du statut juridique des actions hacktivistes ?

Certains souhaitent légitimer les opérations menées par les hacktivistes, notamment en proposant la légalisation des attaques DDOS[29]. C'est le cas du parti hollandais « Démocrates 66 », associé à la gauche libérale. Les cyberattaques seraient en réalité des formes de protestation similaires à un *sit-in* ou une manifestation[30]. Les hacktivistes n'auraient qu'à prévenir en amont les autorités et les propriétaires du site avant de lancer les attaques DDOS, à l'image d'une grève ordinaire. Ce qui laisserait le temps aux intéressés de se préparer à l'attaque et d'en limiter l'impact. Mais la mesure défendue par les « D66 », si elle était adoptée, interdirait également la divulgation d'informations sensibles, de données client ou d'emails, privilégiant ainsi le respect de la vie privée. S'agirait-il du parfait compromis ?

Le parti politique néerlandais n'a cependant pas précisé les critères qui distingueraient les attaques DDoS légales et illégales ; ni le caractère licite ou non de l'exploitation de botnets pour de telles « protestations ». L'adoption de ce texte reste donc hautement improbable. D'autant plus que le mode opératoire consistant à saturer de requêtes un site Internet fait encore débat au sein même de la communauté hacktiviste. Les Telecomix jugent notamment que la légalisation de ces offensives sur Internet justifierait la volonté des autorités de se protéger en investissant Internet, surveillant, militarisant les réseaux, quitte à mettre en péril sa neutralité ou la liberté d'expression des internautes. Notons toutefois que plusieurs journalistes et avocats spécialisés[31] ont eu l'occasion d'avancer des hypothèses concrètes quant à une éventuelle légalisation des moyens hacktivistes.

---

[27] http://www.optoutday.de/orte-und-planungen/

[28] IFRI, note du CERFA n°97

[29] https://xakepy.cc/content.php?r=4040-%D0%92-%D0%9D%D0%B8%D0%B4%D0%B5%D1%80%D0%BB%D0%B0%D0%BD%D0%B4%D0%B0%D1%85-%D0%BF%D1%80%D0%B5%D0%B4%D0%BB%D0%B0%D0%B3%D0%B0%D1%8E%D1%82-%D0%BB%D0%B5%D0%B3%D0%B0%D0%BB%D0%B8%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D1%8C-DDoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B8

[30] http://rt.com/news/dutch-party-d66-ddos-legalized-protest-541/

[31] Amber Lyon (Journaliste), de Gabriella Coleman, Marcia Hoffman (Avocat, membre de l'EFF), Mercedes Haefer (étudiante en droit), Jay Leiderman (Avocat), Gráinne O'Neill (National Lawyers Guild)

1.3 Conclusion et pistes de réflexion

Les évolutions précédemment décrites laissent entrevoir une dynamique allant vers le renforcement, la radicalisation des capacités des groupes de hacktivistes. Mais il en découle également l'idée selon laquelle les valeurs défendues par ces hacktivistes peuvent compter sur l'échiquier politique, car partagées par une quantité non négligeable d'électeurs. Les pistes de réflexion ci-dessous emprunteront ces deux axes principaux.

1.3.1.1 Des sujets de revendications et de contestation toujours d'actualité

Les mouvements hacktivistes sont appelés à durer, au moins dans la contestation de textes de loi visant à réguler le cyberespace, les réseaux et leurs contenus ; contestation des multinationales liées de près ou de loin à l'exploitation abusive de travailleurs et de ressources naturelles ; contestation enfin des forces de cybersécurité et de renseignement. La volonté croissante exprimée par les Etats à travers le monde de renforcer leur cybersécurité, leur vigilance sur Internet ainsi que leur législation (droit d'auteur, pénalisation des cyberattaques…) donnera du grain à moudre aux contestations hacktivistes.

1.3.1.2 Le rapprochement entre hacktivisme et activisme

Les similitudes caractérisant les revendications de hacktivistes et d'activistes pourront entrainer leur rapprochement.

Figure 13. Tweet sur les conditions de travail en Chine

Figure 14. Soutien d'Anonymous aux grèves dans la Lufthansa

Déjà, certains hacktivistes et hackers se joignent aux causes plus classiques (soutien de grèves, de revendications sur les conditions de travail, etc.), afin de mobiliser le soutien populaire, d'attirer l'attention en médiatisant l'affaire. Mais la question de savoir si les ONG pourraient recourir au

« hack » pour faire valoir leurs idées reste en suspens. Le problème de la respectabilité d'un mode d'action transgressif ou illégal est essentiel. Dans un questionnaire mené par Céline Pigot[32], analyste chez CEIS, il ressort que les individus contestent les pratiques hacktivistes quand celles-ci violent clairement la loi. Pour autant, ils reconnaissent que c'est cette illégalité même, ou du moins le caractère transgressif du hacktivisme, qui renforce l'impact des actions et la médiatisation des causes défendues. À la question de savoir si les ONG ou les associations devraient avoir recours à des hackers, les personnes interrogées sont mitigées : la moitié d'entre elles pense qu'il s'agirait d'une bonne chose tandis que l'autre moitié rejette cette possibilité avec force.

Clémence Lerondeau, Responsable Internet de Greenpeace, reconnaît bien que la question des attaques DDoS est fortement débattue au sein de l'organisation[33], mais souligne néanmoins[34] la nécessité pour les hackers de respecter une éthique de *« recherche de la vérité et de la transparence ».*

1.3.2 Le hacking, futur moyen de pression des revendications en tout genre ?

La dépendance croissante de la société aux nouvelles technologies de communication, la numérisation et la dématérialisation des activités quotidiennes font de l'outil de piratage informatique un moyen de pression destiné à être de plus en plus prisé. L'usage de l'outil « hacking » à des fins de pression par les salariés contre leur employeur lors de grèves classiques, de manifestations ou de revendications de toutes sortes, n'est pas à exclure.

Le hacking comme nouvelle forme de contestation sociale ?

Il n'existe à ce jour pas d'exemple d'utilisation du piratage informatique dans le cadre d'une grève ou d'un conflit social. Il est toutefois possible d'envisager plusieurs cas de figure où l'utilisation d'outils informatiques comme moyens de pression serait redoutable.

Le système d'information d'une entreprise constitue aujourd'hui le cœur de son patrimoine informationnel. Il permet le bon fonctionnement de l'entreprise et supporte ses fichiers (fichiers clients, documents sensibles, etc.), etc.

- Priver une entreprise de l'accès à Internet pourrait avoir un impact considérable, voire plus important que le piquet de grève ;

- Destruction de fichiers sensibles, le sabotage du SI, la fuite et diffusion de données sensibles (par vengeance notamment) sont autant de perspectives extrêmement dangereuses et, par conséquent, des moyens de pression majeurs (diffusion de secrets d'affaires, de brevets, mais

[32] Sondage réalisé auprès de 49 personnes dans le cadre d'un mémoire de Master 2 à l'École des hautes études en sciences de l'information et la communication (Université Paris IV) et intitulé « *L'hacktivisme ou le renouveau de l'Internet militant* »

[33] http://techethique.blog.youphil.com/tag/croix-rouge

[34] http://www.zdnet.fr/blogs/social-media-club/communication-de-crise-20-quels-leviers-pour-les-marques-39769890.htm

aussi de documents financiers prouvant la bonne santé d'un groupe souhaitant licencier, ou encore de documents personnels discréditant les dirigeants) ;

- L'utilisation du concept de ransomware pourrait également être transposé aux conflits sociaux : le salarié exigerait une négociation en sa faveur plutôt que de l'argent ;

- DDoS et défacement de site pourraient être redoutables à l'encontre, par exemple, d'une société de e-commerce ou tout autre type de société ne réalisant ses activités que grâce à son site Internet vitrine. Le piquet de grève devant les locaux de ce type d'entreprise presque totalement « en ligne » n'est en effet plus pertinent. Rendre indisponible le site Internet d'une e-entreprise provoquerait une chute du chiffre d'affaires de la société et pourrait également nuire à son image ;

- Le blocage de boite mail, le ralentissement de la vitesse de connexion, etc. permettrait de ralentir la productivité d'une entreprise, à l'image du concept de « grève perlée » (les salariés, sans interrompre leur activité professionnelle, la ralentissent considérablement).

Ces scénarios sont d'autant plus crédibles que : les salariés (notamment de la génération Y) sont de plus en plus familiers des nouvelles technologies ; certains salariés disposent d'accès administrateurs (DSI, RSSI…) dont ils pourraient abuser en cas extrême (cas de l'informaticien syndicaliste) ; les conflits sociaux se déroulant au sein de grands groupes sont très médiatisés et s'insèrent dans une problématique plus générale de revendications quant aux conditions de travail, de délocalisations, de suppressions de poste et, plus généralement de crise économique. Autant de causes susceptibles d'être défendues par des collectifs hacktivistes.

1.3.3 L'accroissement de la dangerosité des opérations hacktivistes

Si les Anonymous et d'autres groupes hacktivistes ne représentent pas une menace du plus haut niveau, ils disposent toutefois d'un potentiel considérable et ce pour plusieurs raisons :

- Même superficielles (sites Internet vitrines pris comme cibles), les opérations des hacktivistes tels que les Anonymous ciblent déjà des infrastructures critiques et des cibles sensibles (ressources minières[35] avec l'#OpGreenrights ; banques, cabinets de conseil, agence gouvernementales, grands groupes industriels[36]). Il s'agit là d'une tendance qui risque de perdurer dans le temps ;

- Il est possible que des groupes existant ou des groupes issus de scissions souhaitent passer d'une logique d'attaques superficielles (attaques DDOS contre sites vitrines) et de vol de données sensibles, à une logique plus nocive d'attaques en profondeur, de sabotage, etc.

[35] http://www.ibtimes.co.uk/articles/350683/20120611/anonymous-intel-opcoltan-operation-green-rights-coltan.htm

[36] http://blog.imperva.com/2012/08/analyzing-the-team-ghostshell-attacks.html

- Cette évolution vers des cyberattaques plus sophistiquées profiterait de champs d'action nouveaux, en raison de la forte dépendance de la société aux nouvelles technologies de l'information et de la communication (IPv6[37], Smart grids[38], automobile connectée[39], numérisation des activités de santé, etc.). Le tout connecté, l'Internet des objets, l'accessibilité de certains SCADAs *via* Internet, autant d'évolutions déjà enclenchées qui élargissent le champ des possibles ;

- Il n'est pas exclu que certains hacktivistes gagnent en compétences. Par définition, ces groupes comptent dans leurs membres des profils extrêmement divers et complémentaires. L'anonymat est également un facteur permettant à tout type de profil de les rejoindre (qu'il s'agisse d'un ingénieur ou expert en cybersécurité, etc.) ;

- Il est enfin possible de supposer que la dynamique enclenchée par la diffusion d'outils de Crime as a Service tels que LOIC ou HOIC se poursuivra et s'amplifiera ; Les interactions croissantes avec le monde cybercriminel faciliteront également l'utilisation d'outils relativement dangereux par des individus de profil « script kiddies ». La diffusion d'outils extrêmement simples d'utilisation et capables de viser, en profondeur, ou se saboter des infrastructures critiques est donc une perspective à anticiper, même si elle ne reste que projection.

1.3.4 La montée en puissance des partis diffusant l'idéologie hacker sur l'échiquier politique

Si les moyens employés par les hacktivistes sont illégaux et contestables, les valeurs défendues sont en revanche largement partagées par une partie de la société. Les notions de neutralité du net et de liberté d'expression font partie des priorités des plus hautes instances, notamment à l'échelle européenne. La montée en puissance de ces partis reste donc une évolution plausible. D'autant plus que la prise en compte de ces valeurs à l'échelle parlementaire, lors du processus législatif, permettrait de désamorcer certaines tensions menant aux mobilisations et aux manifestations virtuelles (par DDOS).

[37] http://news.cnet.com/8301-1009_3-57445157-83/fbi-ipv6-rollout-could-hinder-police-investigations/?part=rss&tag=feed&subj=News-Security&Privacy=&utm_source=dlvr.it&utm_medium=twitter

[38] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/eu-us-open-workshop

[39] http://www.computerworld.com/s/article/9229919/Car_hacking_Bluetooth_and_other_security_issues?taxonomyId=17&pageNumber=1

2 Ressources humaines et cybersécurité

Une demande accrue et transformée, des formations rares – Où en sont les ressources humaines de la cybersécurité ?

> *« [Le plan d'augmentation des effectifs de l'ANSSI] devrait s'accompagner de l'instauration d'une politique de ressources humaines au sein des services de l'Etat concernant les spécialistes de la sécurité informatique, en encourageant le recrutement, la formation, les mobilités et le déroulement des carrières au sein et entre les différents services de l'Etat. »*
>
> Rapport du sénateur Jean-Marie Bockel, juillet 2012.

2.1 Introduction

La sécurité de l'information n'est pas une discipline nouvelle. En entreprise comme en administration, on lui attribue des moyens techniques et humains dédiés depuis plusieurs décennies. La fonction de « responsable de la sécurité des systèmes d'information » (RSSI) est aujourd'hui le fruit de cette longue expérience, tout comme les nombreuses formations et normes professionnelles qui structurent les ressources humaines de la sécurité de l'information. Si le métier de RSSI est en constante évolution, on semble assister tant en France qu'à l'étranger à une véritable structuration de ses formations, modes de recrutements et parcours de carrière.

Mais en parallèle de ce champ bien structuré s'est développée au cours des dix dernières années une exploration en terrain quasi-inconnu d'une cybersécurité dont les enjeux dépassent de loin la continuité de l'information en entreprise. Là où les hackers avaient fait d'Internet leur terrain de jeu, les Etats ont choisi de mener dans le cyberespace une course à l'armement et une guerre qui ne dit pas son nom. Les techniques et outils d'attaque informatique évoluent extrêmement rapidement. Il y a seulement dix ans, il était inimaginable que l'on puisse détruire des réacteurs nucléaires ou que l'on prenne le contrôle d'avions grâce à des cyber-armes. Aussi, le décalage du privilège de l'attaquant se fait sentir. Une poignée de hackers peut mettre sur pied une véritable cyberarme capable de paralyser des économies entières ou d'endommager des infrastructures critiques. Dans les pays développés, c'est chaque administration, chaque entreprise, chaque réseau qui peut être ciblé et doit se protéger en conséquence. Les Etats tentent ainsi depuis quelques années de mettre en place des unités de lutte informatique dans leurs différentes agences de défense et de sécurité. Si l'on peut facilement proclamer la création d'une agence où d'un centre de commandement dédié à la cybersécurité, trouver les milliers d'experts en sécurité informatique nécessaires à la protection d'un pays tout entier n'est pas chose aisée. En France comme ailleurs, le « cybersoldat » est une denrée rare.

En Europe et en Amérique du Nord, la réduction drastique des budgets de Défense n'entame pas la croissance inexorable des moyens alloués à la cybersécurité. Pourtant, les ressources humaines de la

cybersécurité sont un champ complexe, qui recouvre des métiers très différents et affecte des entités de nature hétéroclite. On ne trouve pas en la matière de formations et carrières typiques ou immuables. En entreprise, le rôle des responsables de la sécurité des systèmes d'information (RSSI) est établi mais se trouve être en recomposition permanente. Du côté de la cybersécurité dans son aspect plus politique et militaire, tout reste à faire.

Les outils et techniques des systèmes d'information évoluent extrêmement rapidement, et les dangers du monde cybernétique avec eux. Ainsi, du côté du recrutement, la demande en experts en sécurité informatique est en train d'exploser, tant au sein des entreprises qu'au service de l'Etat. Pourtant, la mise en place de filières de formations et de recrutement qui puissent répondre à cette demande est longue et complexe à mettre en place. **A l'aune de ce décalage entre une demande accrue d'experts en sécurité informatique et une offre trop embryonnaire, comment s'organisent et se structurent les ressources humaines de la cybersécurité ?**

Quelques définitions

Sécurité de l'information : « La sécurité de l'information est l'ensemble des mesures adoptées pour empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le refus d'utilisation d'un ensemble de connaissances, de faits, de données ou de moyens. Le terme sécurité de l'information désigne donc les mesures préventives que nous mettons en place pour préserver nos informations et nos moyens. »[40]

Cybersécurité : « La cybersécurité concerne les usages défensifs et offensifs de ces systèmes d'information qui irriguent désormais nos organisations modernes. Elle prend en compte les contenants, c'est-à-dire les moyens techniques (réseaux informatiques, téléphoniques, satellitaires…) utilisés pour l'échange de données, qui peuvent faire l'objet d'opérations d'infiltration, d'altération, du suspension voire d'interruption, comme les contenus, c'est-à-dire l'ensemble des informations qui circulent ou sont stockées sur des supports numériques (sites Internet bases de données, messageries et communications électroniques, transactions dématérialisées...) »[41]

Cyberdéfense : « Ensemble des mesures techniques et non techniques permettant à un Etat de défendre dans le cyberespace les systèmes d'information jugés essentiels. Ces mesures peuvent être défensives (surveiller un ordinateur, le protéger avec un anti-virus, réparer les dommages causés par ce virus) ou offensives (créer son propre virus pour attaquer celui qui envahit son ordinateur) »[42].

Afin de mieux étudier les ressources humaines de la cybersécurité, nous faisons une distinction relativement arbitraire entre les métiers de la protection des données en entreprise et en administration et ceux de la cybersécurité des Etats et des économies dans son aspect plus politique

[40] Stéphane Gill, « La sécurité de l'information », 2005. Accessible ici : http://sgill.ep.profweb.qc.ca/spip/IMG/pdf/01_SecuriteInformation.pdf

[41] Nicolas Arpagian, 2010, La cybersécurité, Collection Que Sais-je, p. 9-10.

[42] Site web officiel du ministère de la Défense, « Plongée dans la cyber-terminologie », 06/09/2011. Accessible ici : http://www.defense.gouv.fr/actualites/dossiers/sept-2011-cyberdefense-enjeu-du-21e-siecle/cyberespace/voir-les-articles/plongee-dans-la-cyber-terminologie

et militaire. Alors que le premier champ est relativement structuré avec par exemple le métier établi de RSSI, les ressources humaines du second commencent à peine à prendre forme.

Malgré cette distinction entre les métiers de sécurité de l'information et ceux de la cybersécurité, il faut garder à l'esprit qu'il n'y pas la moindre forme d'étanchéité entre ces deux mondes. Une PME du secteur industriel, une société de service en sécurité informatique et le ministère de la Défense sont autant d'entités distinctes. Pourtant, elles font face à des cyber-menaces souvent similaires et leurs experts informatiques sont amenés à communiquer et à circuler entre elles au cours de leur carrière.

Cette note est consacrée aux métiers de RSSI et d'expert en cybersécurité. Notons que certains métiers (pentesteurs, équipes de réponse à incidents pratiquant le reverse engineering ou l'informatique légale) ont une vocation transverse, touchant à la fois la SSI et à la cyberdéfense.

Au final, la cybersécurité des entreprises participe à la cyberdéfense dans son ensemble. La sécurité des données recoupe la sécurité des infrastructures critiques. Ainsi, les distinctions opérées dans les pages qui suivent servent simplement à mettre en lumière des états de structuration et d'avancement inégaux dans les ressources humaines de la cybersécurité.

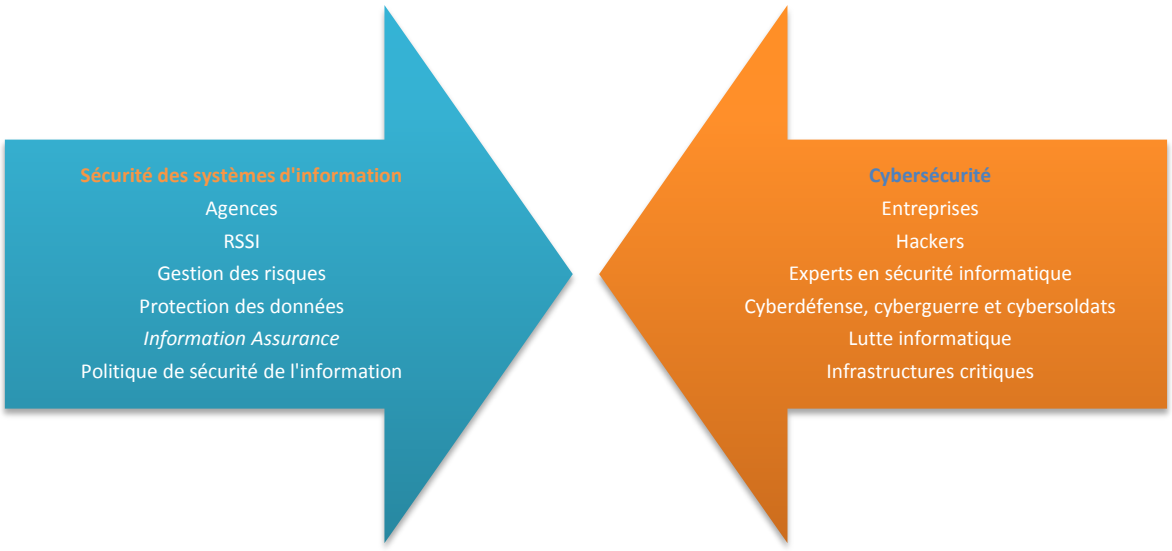


Figure 15. Les mots-clés de la SSI et de la cybersécurité - Source : CEIS

2.2 Le RSSI et la sécurité de l'information en entreprise

En entreprise comme en administration, la sécurité de l'information n'est pas une discipline nouvelle. Mais l'avènement et l'utilisation massive de l'informatique en milieu professionnel a au cours des quinze dernières années entraîné la création d'un métier dédié à la protection des données informatiques, celui de Responsable de la sécurité des systèmes d'information (RSSI).

2.2.1 Les nouvelles menaces pour la sécurité des systèmes d'information

Le métier de RSSI, en permanente évolution, doit faire face à des menaces sans cesse plus dangereuses pour la sécurité des données de son environnement de travail.

2.2.1.1 La protection des systèmes d'information comme gestion des risques

Les RSSI font face à des menaces variées et doivent apprendre à composer avec les habitudes des utilisateurs des réseaux qu'ils sécurisent. Les menaces sur l'intégrité des données n'ont pas nécessairement une origine malveillante ou extérieure mais peuvent provenir de négligences de la part des employés. Patrick Pailloux, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), insiste fréquemment sur la « *nécessaire application de règles d'hygiène informatique élémentaire*» en matière de sécurité[43]. Ainsi, certaines études présentent la perte d'équipement comme la première cause de fuite de données[44]. Une simple erreur d'inattention peut compromettre certaines informations vitales pour l'entreprise. Les exemples sont nombreux de pertes de matériel ou de périphériques de stockages (disque dur, clé USB, etc…) contenant des données non-chiffrées[45], le plus célèbre étant sans doute la disparition de deux CD-Rom par l'administration fiscale britannique contenant les données personnelles d'environ 25 millions de personnes[46] [47]. Une fausse manipulation[48] ou un simple oubli peuvent avoir des conséquences importantes. Récemment, le Canard Enchaîné[49] publiait un article concernant l'existence d'une faille dans plusieurs sites internet du gouvernement alors que celle-ci était connue et corrigée depuis 2010. Enfin, on constate souvent une forme de résistance chez certains employés, y compris parmi les responsables, face aux contraintes imposées par mesure de sécurité. Maintenir un niveau de sécurité correct nécessite en effet de s'astreindre à une certaine discipline, ce qui implique par exemple de ne pas contourner certaines règles pour « gagner du temps » ou par habitude. Les principales menaces viennent des changements de pratique en matière informatique, avec l'émergence du Bring Your Own Device (BYOD)[50] et la généralisation de Cloud. L'usage de terminaux

---

[43] Undernews, « Sécurité : l'ANSSI tire la sonnette d'alarme », 9 octobre 2011. Accessible ici : http://www.undernews.fr/culture-web-emploi/evenements/securite-l%E2%80%99anssi-tire-la-sonnette-d%E2%80%99alarme.html

[44] L'Info ExpoProtection, « Sécurité informatique, 70% des entreprises françaises auraient subi une perte de données en 2010… », 23 juin 2011. Accessible ici : http://www.info.expoprotection.com/?IdNode=1308&Zoom=d60b6f4272c8de639c7acbe98b4598cc&KM_Session=35313ff46ccc5392a8b2147903fe6976

[45] Les exemples sont nombreux, qu'il s'agisse d'une clé USB contenant des mouvements de troupes égarées ou de disques durs stockant des informations confidentielles dans le domaine militaire ou spatiale mis en vente sur Internet : http://news.bbc.co.uk/2/hi/uk_news/england/cornwall/7605923.stm et http://www.stuff.co.nz/national/809947 et http://www.lesmotsontunsens.com/defense-antimissile-americaine-disque-dur-internet-ebay-4495

[46] Le Monde, « Le scandale de la perte des données de 25 millions de Britanniques scandalise outre-Manche », 21.11.2007. Accessible ici : http://www.lemonde.fr/international/article/2007/11/21/la-perte-des-donnees-de-25-millions-de-britanniques-scandalise-outre-manche_980778_3210.html

[47] LeMagIT , « Les entreprises françaises ont mal à leur sécurité IT », 08.11.11. Accessible ici : http://www.lemagit.fr/article/securite-france-entreprises-etude-pwc/9831/1/les-entreprises-francaises-ont-mal-leur-securite-it/

[48] Par exemple, des millions de données personnelles ont été envoyées par erreur aux médias en Norvège : http://www.lefigaro.fr/flash-actu/2008/09/17/01011-20080917FILWWW00522-divulgation-de-donnees-confidentielles.php

[49] Canard Enchaîné du 5 septembre 2012

[50] http://www.globalsecuritymag.fr/Pascal-Gaillot-Dimension-Data,20120907,32226.html

personnels sur le lieu de travail ou pour travailler en dehors du travail amène les employés à manipuler des informations parfois sensibles dans le cadre d'un réseau qui n'est pas toujours conforme aux prescriptions du RSSI. On constate une forme de dispersion que l'on retrouve également dans le Cloud computing, avec des données qui peuvent échapper à la vigilance des employés.

2.2.1.2 L'accélération du vol de données à des fins économiques

Les entreprises n'ont pas attendu l'ère informatique pour convoiter les données confidentielles de leurs concurrentes[51]. Mais avec les nouvelles techniques de piratage informatique, qu'il s'agisse d'informations d'ordre économique, stratégique ou technique, certaines entreprises sont parfois prêtes à entrer dans l'illégalité pour avoir un temps d'avance sur leurs concurrents. La condamnation d'EDF à 1.5 million d'euros d'amende et à plus de 2 millions d'euros de dommages et intérêts, ainsi que la condamnation de trois individus à de la prison ferme pour la mise en place d'une écoute illicite des systèmes informatiques de Greenpeace témoigne de l'existence de dérives de la guerre économique. Les vols de données peuvent intervenir depuis l'intérieur de la société, par des employés, malintentionnés[52] ou non. Si les collaborateurs s'emparent de secrets d'entreprise dans la moitié des cas, un rapport de Symantec souligne que ces vols sont souvent le fait de négligences ou de méconnaissance[53]. Les sociétés peuvent également être la cible de pirates informatiques dont les motivations sont multiples : chantage, revente des données à un concurrent[54], etc. Les motifs d'une attaque peuvent être extrêmement variés, mais outre le vol d'information pour les diffuser au public (ce qu'on appelle un « leak »), ces groupes peuvent chercher à altérer le fonctionnement des systèmes d'informations. Le déni de service distribué est un moyen simple et peu coûteux de perturber l'accès à un site internet et est couramment utilisé par certains internautes. Le défaçage consiste à modifier le contenu et la mise en page d'un site internet, le plus souvent pour y placer des textes de revendications. A la différence des vols d'informations pour des motifs économiques, qui cherchent le plus souvent à rester discrets, ces individus cherchent à faire un maximum de dégâts avec une visibilité médiatique importante.

2.2.1.3 La SSI à l'épreuve des guerres idéologiques du net

Autre forme de menace, le vol de données par des pirates pour des raisons autre qu'économiques. Cette menace est assurément la plus médiatique, c'est-à-dire la plus dangereuse pour la réputation de l'entreprise ou de l'administration. Lorsque l'objectif est désintéressé, les pirates cherchent soit à faire parler d'eux, soit à assouvir une passion pour la sécurité informatique qui dans ce cas les amèneront à l'informer de l'existence de failles le cas échéant. Ils peuvent enfin agir par militantisme

---

[51] http://www.industrie.com/it/demain-les-pirates-informatiques-pourraient-cibler-votre-r-d.13277

[52] http://blog.lefigaro.fr/crequy/2011/10/premiere-sanction-dun-vol-de-donnees-numeriques-par-un-tribunal.html

[53] http://www.lemondeinformatique.fr/actualites/lire-symantec-decrypte-le-vol-de-donnees-par-les-collaborateurs-de-l-entreprise-47105.html

[54] http://www.francemobiles.com/actualites/id/201208031343709863/coree_du_sud_des_pirates_informatiques_s%E2%80%99attaquent_aux_donnees_de_kt_.html

ou conviction politique. On peut citer l'exemple du soldat Bradley Manning qui a volé des informations à l'US Army pour les communiquer à Wikileaks : celui-ci n'a rien gagné dans cette opération si ce n'est le sentiment d'avoir fait ce qu'il devait penser être juste. Autre exemple, les Anonymous ont également lancé une opération contre des compagnies pétrolières, « Save The Artic »[55], qui a conduit à la révélation d'un millier de login d'employés. Les attaques d'origine hacktiviste menacent donc la réputation et la pérennité des entreprises.

2.2.2 Le RSSI, une vision globale de la protection de l'information

Face à ces menaces cyber et à l'évolution des ressources humaines, le RSSI est contraint de s'adapter. Il doit trouver sa place dans un organigramme professionnel qui n'accorde pas toujours de place dédiée à ce profil hybride. En ce sens, le métier connaît des évolutions tant au niveau de l'exercice de la fonction en entreprise que de son environnement professionnel.

2.2.2.1 Le RSSI d'aujourd'hui : un manager et un communiquant plutôt qu'un technicien

Le responsable sécurité informatique évalue la vulnérabilité du système d'information de l'entreprise et met en place des solutions pour protéger les applications et les données. Plusieurs tendances viennent compléter cette affirmation :

2.2.2.1.1 Première tendance : de la gestion du sinistre à la lutte contre la malveillance ; intégration avec la gestion des risques

Une première tendance que l'on peut dégager au sein du rôle du RSSI concerne la gestion du risque et de la malveillance plutôt que la gestion du sinistre. Le CLUSIF estime que quand le métier de RSSI et Internet n'existaient pas en 1986, la malveillance représentait seulement 45% de la sinistralité informatique. La gestion de risques accrus par le RSSI le pousse à travailler étroitement avec le *risk manager*. Ainsi, un document collaboratif CLUSIF-AMRAE datant de 2006 indique que *« cette prise en compte des attentes réciproques initie un processus de communication interactif. De ce schéma vertueux, le RSSI retirera un support supplémentaire pour la gestion des risqués liés au SI et une reconnaissance accrue de son domaine d'intervention. »*[56]

2.2.2.1.2 Deuxième tendance : la montée en puissance du RSSI non-technicien

Le terme « RSSI » recouvre une réalité complexe puisque de l'aveu général des professionnels interrogés sur le sujet, il n'y a pas de profil-type pour devenir RSSI. En particulier, la question de savoir si le RSSI en entreprise doit être un technicien ou non revient très fréquemment dans les

[55] http://www.zataz.com/news/22256/Save-The-artic--anonymous--hack--exxon--esso--mobil--shell.html

[56] AMRAE-Clusif, publication collaborative « RM et RSSI : deux métiers s'unissent pour la gestion des risques liés au Système d'Information », page 35, Juin 2006. Accessible ici : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-RM-RSSI-GESTION-DES-RISQUES.pdf

discussions[57]. Est-il avant tout un informaticien ou un consultant ? Met-il en place des mesures techniques ou se repose-t-il plutôt sur une communication interne ?

De fait, la technique a de moins en moins sa place dans l'action du RSSI. Plutôt que de faire du simple soutien à la direction des systèmes d'information, le RSSI agit à tous les niveaux pour faire appliquer des mesures de sécurité. Serge Saghroune, RSSI chez Accord, explique que c'est *« un métier qui se situe entre la voile en solitaire et la voile en équipe, il faut savoir prendre du recul, mais s'investir dès que cela est nécessaire. »*[58] Pour Joël Rivière, président de Lexsi, *« il y a longtemps que le RSSI n'a plus les mains dans le cambouis. »* On peut lire dans un document du CLUSIF que le RSSI assume une *« fonction transverse de manager »* puisqu'il *« rassemble de nombreux contributeurs (stratégie, communication, juridique, etc…) »*, il *« dialogue avec les Directions Métiers et la DSI »* et il *« participe à la relation Fournisseur »*[59].

Selon un expert en sécurité informatique travaillant pour le gouvernement, les experts en sécurité informatique peuvent parfois percevoir le RSSI comme *« ringard »*, car *« il existe une réelle différence de point de vue entre les techniciens et les organisationnels, chacun se pensant le "maillon fort" de la sécurité alors qu'une vraie "sécurité" combine les deux aspects. »*

2.2.2.1.3 Troisième tendance : le rattachement à la direction générale

Au fil du temps, le RSSI a été amené à se distinguer de la DSI pour prendre un rôle plus solitaire au sein de l'entreprise. La question du rattachement du RSSI dans la hiérarchie de l'entreprise anime de manière récurrente les cercles de réflexion sur la sécurité informatique. Souvent, le RSSI est intégré à la direction des systèmes d'information quand l'entreprise est de taille modeste ou lorsque l'architecture informatique de l'entreprise est en construction. Le RSSI peut alors donner son avis et avoir un impact direct sur la sécurité des outils informatiques de l'entreprise.

Pourtant, les experts en sécurité conseillent de plus en plus le rattachement du RSSI à la direction générale[60]. En effet, au fur et à mesure que le RSSI se fait communiquant et manager, il peut bénéficier de l'étiquette « DG » qui lui confère un plus grand poids et une plus grande lisibilité dans toute l'entreprise. Lorsque le RSSI est présent au plus haut niveau de l'entreprise, le signal envoyé est fort : la direction veut intégrer la sécurité au travail de l'entreprise et les décisions prises seront suivies d'actions[61].

---

[57] Security Vibes, « L'ère du RSSI non technicien », 18 Novembre 2010. Accessible ici : http://www.securityvibes.fr/conformite-organisation/lere-du-rssi-non-technicien/

[58] Le Journal du Net, Interview de Serge Saghroune, 9 décembre 2003. Accessible ici : http://emploi.journaldunet.com/magazine/1482/

[59] ARMAE-Clusif, publication collaborative « RM et RSSI : deux métiers s'unissent pour la gestion des risques liés au Système d'Information », Juin 2006. Accessible ici : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-RM-RSSI-GESTION-DES-RISQUES.pdf

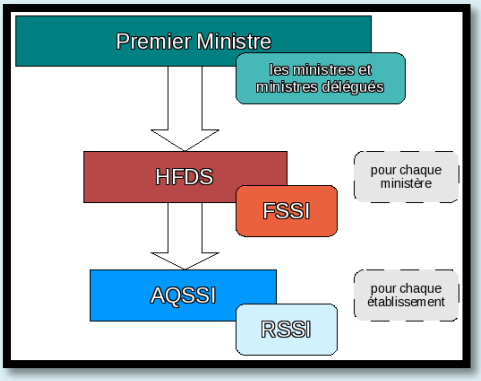
[60] Global Security Mag, « RSSI, du doctor no au monsieur oui mais », trimestriel juillet-août-septembre 2012, page 32.

[61] Présentation CLUSIF/CLUSIR, « Quelle organisation pour prendre en compte le risque informatique », 2005.

Focus : Comment travaillent les RSSI en administration ?

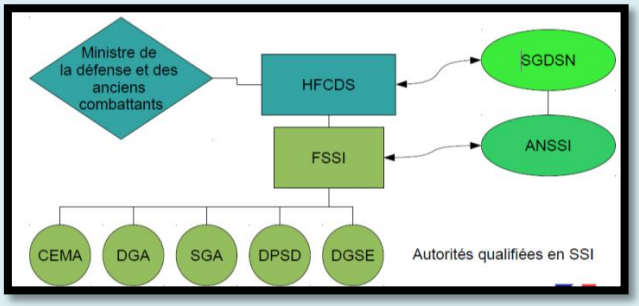
Dans les administrations, la sécurité de l'information n'est pas assurée par un RSSI en électron libre. Au contraire, elle répond à **une chaîne hiérarchique** bien précise[62].

- Le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) pilote au niveau national la SSI ;
- Un Haut Fonctionnaire de Défense et de Sécurité applique cette politique au sein de chaque ministère ;
- Le Fonctionnaire de la sécurité des systèmes d'information (FSSI) applique spécifiquement le volet SSI de la politique définie par le SGDSN ;
- Les autorités qualifiées pour la SSI (AQSSI) définissent la PSSI adaptée aux spécificités de l'organisme ;
- Les RSSI assistent les AQSSI dans la mise en œuvre de la SSI, en particulier d'un point de vue technique.



Source : https://www.cru.fr/ssi/securite/chaine_fonctionnelle_et_organisation_interministerielle

Pour sa part, l'ANSSI est rattachée 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.



La SSI du ministère de la Défense - *Source : http://www.arcsi.fr/doc/Cyberdefense-20100316.pdf*

[62] Journée des CRSSI du CNRS, Présentation PowerPoint, 17 octobre 2007. Accessible ici : https://www.pleiade.education.fr/portal/gear/generic/SelectPageContent?itemDesc=contenu&contentid=7019538

2.2.2.2 Les mutations de l'environnement professionnel de la SI

Si le métier de RSSI devient de moins en moins technique au fil des années, ce n'est pas le cas de la sécurité informatique dans son ensemble. Pour pallier au manque de technique du côté des RSSI, les entreprises sont tentées de faire appel à des experts en sécurité venus de l'extérieur ou de recruter des spécialistes techniques en sécurité.

2.2.2.2.1 La spécialisation et experts techniques au sein des entreprises

Typiquement, le RSSI peut surveiller des projets relativement techniques de la DSI, mettre en place une politique de sécurité des systèmes d'information (PSSI) et effectuer une sensibilisation interne. On lit de plus en plus fréquemment que le RSSI peut avoir une fonction de manager, et prendre la tête d'une équipe, en particulier dans de grands groupes ou dans des sociétés NTIC[63]. Lorsqu'un budget important est alloué à la sécurité informatique, l'entreprise recrutera des informaticiens ayant une spécialité dans la sécurité informatique pour assister le RSSI dans la mise en place de mesures techniques de sécurité. L'aspect managérial du métier de RSSI n'en est alors que renforcé.

La pluridisciplinarisation des métiers de la sécurité des systèmes d'information prend deux formes. D'abord avec le recrutement de RSSI venus de la gestion des risques et de la sécurité plutôt que des métiers de l'informatique. En effet un certain nombre de directeurs de la sécurité et de *risk managers* dans des entreprises sont issus du monde militaire. Or, ces métiers et celui de RSSI peuvent se recouper dans leur approche gestion de crise/sécurité. Il reste malgré tout impensable pour un RSSI de n'avoir aucune connaissance en sécurité informatique. On soulignera simplement que certains parcours à l'origine non-ingénieurs peuvent peu à peu amener au métier de RSSI.

Deuxièmement, un juriste peut apporter beaucoup à la sécurité d'un système d'information étant donné la complexité des menaces et des crises auxquelles un RSSI fait face. La dématérialisation des échanges et des données, l'encadrement des usages, la protection des données sont autant d'éléments qui font peu à peu du juriste une pièce maîtresse dans le processus de sécurité de l'entreprise. Au sein d'une équipe de sécurité, le juriste peut s'assurer du respect des règles relatives à la protection des données et systèmes de stockage ; prévenir le risque de failles dans la sécurité informatique ; aider à résoudre les crises en cas de problème de sécurité informatique ; et accompagner l'entreprise dans sa sortie de crise. C'est particulièrement la question de la vie privée et les nouvelles lois dans ce domaine qui obligent les plus grosse structures à recourir à des juristes. Alors que le RSSI peut être perçu comme un *« fossoyeur de la vie privée »*[64] en entreprise, le juriste peut venir rétablir l'équilibre en explicitant au RSSI les règles en matière de collecte des données, de traçabilité des informations ou de cybersurveillance. Dans le futur, le métier de juriste appliqué à la

[63] Formation RSSI de HSC, plaquette de présentation. Accessible ici : http://www.clusif.fr/fr/production/formations-ssi/formation.asp?f=294&c=0&t=a&region=0&categorie=0

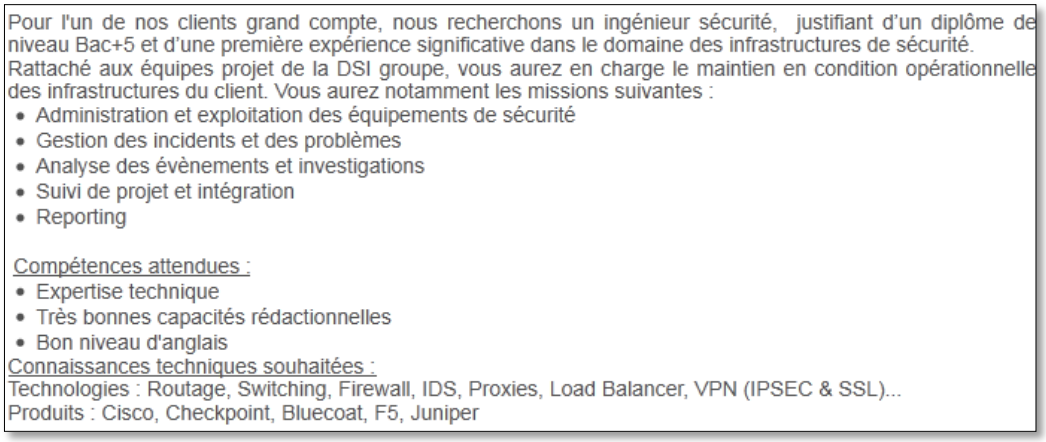
[64] Global Security Mag, « Le RSSI, fossoyeur de la vie privée ? », octobre 2011. Accessible ici : http://www.globalsecuritymag.fr/Les-Ambassadeurs-de-la-Securite-le,20110928,26000.html

sécurité des systèmes d'information sera particulièrement tributaire de l'évolution du droit en matière de protection des données et de cybersécurité.[65]

2.2.2.2.2 L'externalisation de la fonction de RSSI

L'externalisation, autre tendance importante, consiste à faire appel à un RSSI d'une compagnie tierce. Plusieurs motifs peuvent pousser une entreprise à externaliser[66]. C'est d'abord et avant tout sa taille et son budget qui peuvent l'y contraindre. Les petites et moyennes entreprises font souvent reposer une partie des tâches classiques du RSSI sur les bras d'un directeur financier. Autre raison qui tient plus à l'organisation interne des entreprises : il peut être parfois difficile de créer une position de RSSI là où la culture de l'entreprise répartissait ce rôle entre le *risk manager* et les techniciens de la DSI[67].

Il peut également être nécessaire pour l'entreprise de faire momentanément appel à un RSSI en cas de cyberattaque. Quels avantages peut-elle en retirer ? Principalement une optimisation des coûts puisque les tâches d'un RSSI peuvent être ponctuelles, en particulier dans une PME (réunions de sensibilisation, avis sur un projet) et peuvent ne pas requérir une personne à temps-plein sur le long terme.



Pour l'un de nos clients grand compte, nous recherchons un ingénieur sécurité, justifiant d'un diplôme de niveau Bac+5 et d'une première expérience significative dans le domaine des infrastructures de sécurité.
Rattaché aux équipes projet de la DSI groupe, vous aurez en charge le maintien en condition opérationnelle des infrastructures du client. Vous aurez notamment les missions suivantes :

- Administration et exploitation des équipements de sécurité
- Gestion des incidents et des problèmes
- Analyse des évènements et investigations
- Suivi de projet et intégration
- Reporting

Compétences attendues :

- Expertise technique
- Très bonnes capacités rédactionnelles
- Bon niveau d'anglais

Connaissances techniques souhaitées :
Technologies : Routage, Switching, Firewall, IDS, Proxies, Load Balancer, VPN (IPSEC & SSL)...
Produits : Cisco, Checkpoint, Bluecoat, F5, Juniper

Figure 16. Un exemple d'externalisation : le recrutement par la SSII Openminded Consulting d'un RSSI pour un de ses clients « grand compte »[68]

Pourtant, les RSSI freelance évoquent de manière récurrente la difficulté à convaincre des petites structures des bénéfices qu'elles pourraient avoir à recruter à temps partiel un RSSI venu de

---

[65] « Juriste, un juge de paix pour l'entreprise », Global Security Mag, N° 20, juillet-août-septembre 2012.

[66] Ysosecure, « L'externalisation de la fonction RSSI en PME PMI », date inconnue. Accessible ici : http://www.ysosecure.com/securite-information/externalisation-fonction-rssi.html

[67] ARMAE-Clusif, voir note 3.

[68] http://www.lesjeudis.com/recherche-offre-emploi/OPENMINDED-CONSULTING/Ingnieur-scurit_JHS63Z784LCG5RJW3MD/?IPath=QHKCV&APath=2.21.0.0.0

l'extérieur. Souvent, les chefs d'entreprise qui n'ont pas connu de problème de sécurité de l'information ne voient pas l'apport qu'un RSSI pourrait représenter : *« tant que l'informatique fonctionne, tout va bien et il ne voit pas pourquoi il lui faudrait payer quelqu'un pour veiller sur un système qui fonctionne, et qui est déjà géré par un DSI. »*[69]

Le recours à une société de service en ingénierie informatique (SSII) est plus fréquent que l'emploi de RSSI freelance. La plupart du temps, les services offerts par une SSII ne concernent pas la sécurité des systèmes d'information mais plutôt le développement logiciel, l'architecture, ou le conseil. Mais l'expertise, l'agilité et la main-d'œuvre flexible dont disposent les SSII leur permettent de proposer des services de SSI particulièrement poussés (pentest, forensics, etc.) sur une durée courte. Ainsi, on assiste dans certains cas à une mutualisation des prestations d'un seul RSSI que se « partagent » plusieurs PME. Le directeur commercial d'Intrinsec, une entreprise qui propose des services de RSSI en temps partagé, explique l'intérêt du RSSI mutualisé : *« Ce que nous proposons, c'est de mettre à disposition une personne qui va accompagner l'entreprise dans la durée. Le contrat est de plus totalement flexible puisque l'entreprise décide elle-même des jours de présence mensuelle. Elle peut par exemple solliciter plus le RSSI au début d'une mission, comme dans le cadre d'un projet de PCA, puis plusieurs mois ensuite. »*[70]

2.2.2.2.3 La création de normes professionnelles de sécurité informatique

La normalisation est un élément de structuration important pour les métiers de la sécurité informatique. Comme dans de nombreux autres domaines professionnels, le développement des métiers de la sécurité de l'information s'est accompagné de la création de nombreuses normes qui viennent certifier les capacités d'un professionnel auprès d'autres personnes. On compte parmi les normes les plus importantes le CISSP ou l'ISO 27001.

Le site de l'ISC², l'organisme en charge de la délivrance de la norme *Certified Information Systems Security Professional* (CISSP) explique ainsi que *« dans un monde regorgeant de menaces sur la sécurité, le besoin en professionnels de l'information qualifiés n'a jamais été ainsi important. »* Et si l'expérience a son importance, *« les employeurs ont besoin d'une mesure quantifiable et vérifiable pour savoir que l'on dispose de l'expertise requise »*[71]. Il faut pouvoir prouver 5 ans d'expérience dans la sécurité informatique pour être éligible à la certification. Celle-ci s'obtient au moyen d'un test qui contrôle les connaissances dans une dizaine de domaines tel que la sécurité applicative les plans de continuité d'activité et de restauration en cas de désastre ou la cryptographie. Plusieurs dizaines de milliers des professionnels sont certifiés CISSP partout dans le monde.

Le standard de sécurité de l'information ISO 27001 a permis le développement de normes professionnelles sur sa base comme la certification *Lead Auditor* ou *Lead Implementer*. La première

---

[69] Security Vibes, interview de Patrick Boulet, 3 novembre 2009. Accessible ici: http://www.securityvibes.fr/carriere/patrick-boulet-je-ne-crois-pas-au-rssi-a-distance/

[70] Journal du Net, « Assurer la sécurité et faire des économies avec un RSSI à temps partagé », 4 juillet 2008. Accessible ici : http://www.journaldunet.com/solutions/securite/analyse/assurer-la-securite-et-faire-des-economies-avec-un-rssi-a-temps-partage.shtml

[71] Site officiel de l'ISC². Accessible ici : www.isc2.org/credentials/default.aspx

certification est destinée aux professionnels qui souhaitent prouver leur capacité à auditer des systèmes de gestion de la sécurité de l'information (SMSI) tandis que la deuxième correspond aux professionnels qui mettent sur pied de tels systèmes. Pour obtenir une de ces certifications, il faut assister à quelques dizaines d'heures de cours et passer un examen plus simple que celui de CISSP. La détention de ces certifications peut parfois conditionner la réponse aux appels d'offres émis par des entreprises demandeuses de main-d'œuvre en sécurité de l'information.

La création de ces normes et leur diffusion participe pleinement à la structuration des ressources humaines de la sécurité informatique. L'AFNOR, organisme qui est en charge de la normalisation ISO en France, explique ainsi qu' *« une norme permet de définir un langage commun entre les acteurs économiques-producteurs, utilisateurs et consommateurs, de clarifier, d'harmoniser les pratiques et de définir le niveau de qualité, de sécurité, de compatibilité, de moindre impact environnemental des produits, services et pratiques. Elles facilitent les échanges commerciaux, tant nationaux qu'internationaux, et contribuent à mieux structurer l'économie et à faciliter la vie quotidienne de chacun. »*[72]

Nous avons vu que les métiers de la sécurité de l'information avec au premier chef celui de RSSI sont relativement récents et mutent rapidement sous l'effet de cybermenaces changeantes. Ces métiers répondent à un besoin essentiel et récurent : les entreprises sont de plus en plus nombreuses à se soucier de leur sécurité informatique. Pour répondre cette demande en main-d'œuvre qualifiée, une filière s'est mise en place pour assurer la formation et le recrutement des RSSI et autres métiers de la sécurité informatique.

2.2.3
Formations, recrutement et carrières dans la sécurité de l'information

2.2.3.1 La démultiplication de formations plus ou moins techniques

On pouvait entendre il y a quatre ans Bernard Foray, RSSI de Casino Information Technology, dire qu'*« il n'y a pas de cycle d'études ni de diplôme de RSSI. »*[73] De nombreux professionnels continuent d'estimer que le métier de RSSI est trop neuf et hybride pour faire l'objet de formations spécifiques. Pourtant, au fur et à mesure qu'il se normalise, se répand et se situe en entreprise, des formations dédiées spécifiquement au métier de RSSI apparaissent. Ainsi, la plupart de celles qui existent aujourd'hui en France n'existaient pas encore il y a dix ans.

De nombreuses formations existent aujourd'hui en France dans le domaine de la sécurité informatique. Elles ne suivent pas toutes le même programme et ont un niveau de connaissance

[72] Site officiel de l'AFNOR. Accessible ici : http://www.afnor.org/metiers/normalisation/forum-aux-questions-faq/10-questions-normalisation

[73] 01Net, « Comment devenir un bon RSSI », 22 mai 2008. Accessible ici : http://pro.01net.com/editorial/384386/comment-devenir-un-bon-rssi/

technique plus ou moins avancée. La plupart d'entre elles, en revanche, prétendent que le métier de RSSI fait partie des débouchés possibles.

Les formations entièrement dédiées à la sécurité informatique en France sont toutes des formations de master proposées à des étudiants ayant déjà de solides connaissances en informatique. Elles durent donc un ou deux ans. Les universités et écoles qui mettent en place ces formations considèrent que la sécurité informatique n'est pas une fin en soi mais plutôt une spécialisation de l'informatique. L'idée de formations entièrement dédiées à la cybersécurité fait cependant son apparition à l'étranger, avec par exemple le Maryland Cybersecurity Center sur lequel nous reviendrons plus tard.

Quelques formations françaises en sécurité informatique :

- Telecom Bretagne Mastère « Cybersécurité » en partenariat avec Supélec
- Université de technologie de Troyes, master de sécurité des systèmes d'information
- Paris 12, Master 2 Sécurité des systèmes d'information
- Université de Rouen, Master informatique, Sécurité des systèmes d'information
- Université de Limoges, master Cryptis
- Université de Lorraine, Master Informatique : Sécurité des Systèmes d'information et de communication
- Université de Grenoble, Master 2 Sécurité, Cryptologie et Codage de l'Information
- Université de Bordeaux, master double cryptologie et sécurité informatique
- Université de Rennes, master sécurité des systèmes d'information
- Blois - Licence professionnelle – Sécurité des systèmes d'information
- ParisTech- MS Architecture et sécurité des systèmes d'information

On constate qu'il n'existe pas d'uniformité entre ces formations, le critère de distinction principal étant le niveau de technicité de l'enseignement. Certains ont un aspect relativement managérial tandis que d'autres font lourdement appel aux mathématiques (cryptologie). Voici deux exemples de masters dont le degré de technicité varie fortement :

Supelec	**Université de Lorraine**
- Maîtriser les **méthodes organisationnelles** (méthode EBIOS, normes ISO 17799 et ISO 27001…) et techniques (authentification, certification, pare-feu…) permettant de protéger les ressources d'un système d'information - Appréhender dans sa **globalité**, les problèmes liés à la sécurité des systèmes d'information en	- Maîtriser **des techniques de sécurité informatique** : comprendre et mettre en oeuvre des méthodes et des outils de sécurité des systèmes, des réseaux et des services, connaître le fonctionnement des principaux protocoles de communication, savoir gérer la défense des systèmes et les **outils techniques de sécurité** (PKI, smartcards, systèmes biométriques,

vue de gérer les risques associés (Risk Management) - Mettre en perspective **l'environnement technique, économique et juridique** dans lequel doit être créée la politique de sécurité du système d'information	firewall, IDS, VPN, etc.) - Explorer des **domaines fondamentaux et théoriques** qui constituent une ouverture sur la recherche... - S'approprier les méthodologies de gestion de la sécurité afin de pouvoir effectuer l'identification, l'évaluation des risques en matière de sécurité informatique, […] la mise en oeuvre et le suivi des solutions de sécurité (EBIOS, Mehari, normes ISO 27…) - Enfin, des cours de communication et de droit informatique

Les formations courtes

On relève également l'existence de plusieurs dizaines de formations dans la sécurité de l'information sur des sujets spécifiques ou pour apprendre les bases en la matière. Ces formations, que proposent des entreprises de sécurité de l'information, durent la plupart du temps moins d'une semaine. Certaines sont spécifiquement destinées à former les participants aux tests de certifications professionnelles (ISO 27001 ou CISSP). Ces formations ne donnent pas lieu à la remise d'un diplôme mais on peut faire valoir sa participation sur un CV. Le CLUSIF répertorie ces formations pour la France[74]. En voici quelques exemples :

- LEXSI : Ethical Hacking – Attaques, Failles et Protection du SI (5 jours, 4950€)
- DEVOTEAM : Introduction à la méthode MEHARI (3 jours, 1680€)
- HSC : Formation RSSI (5 jours, 2950€)
- AUDITWARE : Préparation à la certification CISM (35 heures, 2390€)

2.2.3.2 Comment sont recrutés les professionnels de la sécurité de l'information ?

S'agissant du recrutement dans les métiers de la sécurité informatique, on relève une distinction récurrente dans les annonces de recrutement entre le métier de RSSI en entreprise/administration d'une part, et celui d'expert technique plutôt recruté dans une SSII, un cabinet de conseil ou plus rarement au sein d'une équipe de SSI dans une grande entreprise d'autre part.

[74] Site officiel du CLUSIF. Accessible ici : http://www.clusif.asso.fr/fr/production/formations-ssi/

Les annonces de recrutement de RSSI font plutôt appel à des généralistes capables de s'insérer correctement dans la hiérarchie de l'organisation et de dialoguer avec les métiers. Le RSSI est alors un touche-à-tout, un bon communiquant, et ses capacités techniques ne sont pas forcément poussées, même si les recruteurs avisés apprécient que le RSSI ait fait ses preuves dans le passé en participant à la mise en place de systèmes sécurisés.

Deux offres de postes de RSSI où les aspects de communication et de management ont leur importance :

Une offre d'emploi de RSSI « dans un éditeur indépendant français de solutions monétiques et de services connexes » (07.9.2012)

Le Responsable de la sécurité des systèmes d'information (SSI) est en charge de la protection des systèmes d'informations en recourant à l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires pour conserver, rétablir, et garantir la sécurité du système d'information. Il intervient dans le domaine de la monétique et devra oeuvrer dans le cadre des normes PCI-DSS / PA-DSS ainsi que celles du GIE-CB.

Définir et mettre en œuvre une politique sécurité conforme aux besoins de l'activité, dans le domaine de la monétique
Choisir et mettre en œuvre les actions concernant :
o la sensibilisation des utilisateurs aux problèmes de sécurité
o la sécurité des réseaux
o la sécurité des systèmes
o la sécurité des télécommunications
o la sécurité des applications
o la sécurité physique.
o la mise en place de moyens de fonctionnement en mode dégradé (récupération sur erreur)
o la stratégie de sauvegarde des données.
o la mise en place d'un plan de continuité d'activité « disaster recovery ».

Une autre offre dans un cabinet de conseil en GRH :

Véritable garant de la sécurité du SI, vous intervenez sur toute la mise en place des éléments nécessaires à la protection des données de l'entreprise.

Au sein du département SI (60 personnes), et en collaboration directe avec le Responsable, vous:
- Définissez les politiques de sécurité adaptées à l'écosystème de l'entreprise.
- Contribuez à garantir la disponibilité du système d'information, préservez son intégrité et sa confidentialité et assurez la sécurité des transactions électroniques.
- Etes en charge de définir la politique générale de sécurité, vous suivez sa mise en œuvre.
- Etes également associé à tous les développements touchant aux systèmes d'information.

Grâce à une veille constante, vous proposez les évolutions nécessaires pour maintenir le meilleur niveau de sécurité possible. Vous devez aussi sensibiliser l'ensemble des collaborateurs de l'entreprise aux enjeux de la sécurité.

Le recrutement par des SSII ou des sociétés de conseil fait logiquement appel à des personnes ayant des compétences très spécifiques. Ils sont le plus souvent techniciens (pentester, forensic, etc…) mais sont également consultants (audit, assistance) et plus rarement juristes.

Chez Lexsi, pour un poste de pentester et auditeur

Vos missions types :

- Référent technique en interne comme auprès des clients
- Tests d'intrusion externes et internes (informatique et téléphonique (ToIP))
- Audits d'architecture
- Audits de configuration
- Formation et sensibilisation
- Possibilités d'ouverture vers des projets transverses (analyses de risques, rédaction de directives, référentiels de sécurité technique, accompagnement de RSSI...)

Vos compétences techniques et qualités personnelles :

Expert en tests d'intrusion, les techniques d'attaques n'ont aucun secret pour vous. Vous connaissez parfaitement la sécurité des systèmes Unix ou Windows et des réseaux IP, ainsi que celle des principales applications commerciales (serveurs Web, messagerie, bases de données, etc.).

Idéalement, vous êtes capable de développer vos codes d'exploitation et d'effectuer des analyses de reverse engineering.

Chez iDNA, on recrute un ingénieur-consultant sur la sécurité des réseaux

Assurer la mise en œuvre et l'exploitation d'équipements réseau et Sécurité ;
Assurer le contrôle des événements de sécurité ;
Assurer le support Niveau 2 et 3 des équipements de sécurité ou réseaux LAN, MAN et WAN;
Définir les architectures techniques ;
Piloter la mise en œuvre et le maintien en conditions opérationnelles de réseaux sécurisé;
Assurer la veille technologique des solutions de sécurité et réseaux / Télécoms;
Participer à l'amélioration de la robustesse des éléments du SI ;
Rédiger / mettre à jour la documentation d'exploitation et les schémas d'architectures ;

2.2.3.3 Carrières : des professionnels souvent jeunes, dynamiques et mobiles

Il est difficile de dégager une carrière-type dans la sécurité informatique ou même en tant que RSSI, tant ces métiers sont neufs et encore en pleine formation. La profession tente de s'organiser et de se faire connaître en France, mais elle n'est pas entièrement structurée. On retrouve cela dit un élément dans beaucoup de témoignages de RSSI et d'experts en sécurité : la jeunesse de la profession. Au sein même des métiers de la sécurité informatique, les personnes qui occupent des métiers techniques sont souvent plus jeunes que ceux occupant des positions managériales (RSSI). Dans les témoignages, les professionnels expliquent souvent que plus on avance dans sa carrière, moins on est amené à faire un travail technique[75]. Aussi ardu qu'il puisse être, le rôle de technicien en sécurité informatique semble être réservé à des jeunes diplômés.

On note également que les carrières dans la sécurité de l'information sont placées sous le signe de la mobilité. Les professionnels sont amenés à naviguer en permanence entre les entreprises et entre les métiers au cours de leur carrière. Dans le cas du RSSI, certains estiment qu'il peut s'agir d'un passage

[75] Blog *Le petit monde d'un pentester*, « La pénurie nous guette-t-elle ? », 10 juin 2010. Accessible ici : http://pentester.fr/blog/index.php?post/2010/06/10/La-p%C3%A9nurie-nous-guette-t-elle#comments

transitoire au cours d'une carrière dans le risque[76] ou dans l'informatique[77]. Au sein d'une SSII, rares sont ceux qui restent entièrement dans le technique tout au long de leur carrière. Au fur et à mesure, le consultant voit son statut évoluer et il peut espérer devenir manager après un certain temps. Il s'occupe alors de l'aspect administratif, commercial et gère ses équipes sans procéder lui-même à des opérations techniques[78].

Le club de la sécurité de l'information français (CLUSIF)

Un signe important de la prise de conscience des métiers de la sécurité de l'information d'une véritable structuration des ressources humaines dans ce domaine passe par la reconnaissance mutuelle des professionnels. La création de divers clubs et associations en France et à l'étranger témoigne ainsi de la croissance de la profession mais aussi d'une volonté de partage des connaissances, de l'uniformisation des formes de sécurisation informatique et d'une défense des intérêts communs.

Assez logiquement, les clubs professionnels dans le domaine de la sécurité informatique ne concernent pour l'instant que les métiers assez répandus et clairement constitués comme celui de RSSI. En France, le CLUSIF (Club de la sécurité de l'information français) se présente comme "un club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité" qui "agit pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques." Le CLUSIF organise des séminaires, publie des recommandations relatives à la sécurité de l'information et s'organise pour cela en "groupes" et "espaces" de travail. Un des trois espaces est dédié au métier de RSSI, espace au sein duquel les intéressés réfléchissent à tous les aspects de la profession depuis 2004. La longue liste des sociétés membre du CLUSIF indique l'impact que peut avoir un tel club pour la création d'un esprit de corporation.

[76] Security Vibes, « De RSSI à Risk Manager…ou pas », 14 avril 2010. Accessible ici : http://www.securityvibes.fr/carriere/de-rssi-a-risk-manager-ou-pas/

[77] ZDNet, « Mourad Sélimi, RSSI du Tribunal de Paris », 11 avril 2011. Accessible ici : http://www.zdnet.fr/actualites/mourad-selimi-rssi-du-tribunal-de-paris-mon-job-est-aussi-bien-axe-sur-la-prevention-des-intrusions-que-la-perennisation-du-si-39759660.htm

[78] Blog *Le petit monde d'un pentester*, « Je suis étudiant, je veux faire du pentest ». Accessible ici : http://pentester.fr/blog/index.php?post/2010/05/26/je-suis-etudiant-je-veux-faire-du-pentest

2.3 Fonctions régaliennes : comment passer d'un recrutement de crise à la construction d'une filière forte de la cybersécurité ?

« Le ministre de la Défense, Jean-Yves Le Drian, a annoncé[79] ce vendredi la création de 200 emplois près de Rennes, principalement dans le secteur de la « cyber-défense », destinée à parer d'éventuelles attaques informatiques.

Jean-Yves Le Drian a fait cette annonce lors d'un déplacement sur le site de la Direction générale de l'armement (DGA) à Bruz (Ille-et-Vilaine), qui accueillera ces nouveaux emplois d'ici à 2015.

Le site, principal centre d'expertise français consacré à la maîtrise de l'information, à la guerre électronique et aux systèmes de missiles, emploie actuellement 1 200 personnes. »

La sécurité informatique passe par une hygiène basique, depuis les ordinateurs des particuliers jusqu'aux systèmes informatique militaires et politiques. Depuis l'apparition et la diffusion d'Internet dans les années 1990, le monde cybernétique vient de manière grandissante provoquer les intérêts et prérogatives des Etats. Ainsi, les aspects politiques, macroéconomiques et militaires de la cybersécurité ne cessent de croître. Appliquée aux fonctions régaliennes de l'Etat, la sécurité informatique répond à des priorités et des modes de fonctionnement différents de ceux appliqués en entreprise et en administration. Pour répondre aux besoins spécifiques de la cybersécurité et de la cyberdéfense, une filière des ressources humaines distincte de celle décrite dans la première partie est en train de se former. Avec des menaces plus graves pour la cybersécurité, et un besoin en main-d'œuvre qui ne trouve pour l'instant pas de réponse satisfaisante, la question de la construction d'une filière forte de la cybersécurité se retrouve au centre des préoccupations de décideurs politiques et militaires.

Quel est l'état des choses actuel ? Quels efforts sont menés en France et à l'étranger ? Et comment passer d'un recrutement de crise à la construction d'une filière forte de la cybersécurité ? Après avoir dressé un rapide panorama de la gravité des menaces cyber, nous verrons en quoi celles-ci appellent à la constitution d'agences et d'équipes aux compétences techniques très poussées.

2.3.1 Des cybermenaces qui appellent à la création d'une filière forte d'experts en cybersécurité

S'il existe une continuité très claire entre les menaces qui affectent les particuliers, les entreprises et les administrations d'un côté et l'Etat de l'autre, l'actualité des dernières années en matière de cybersécurité laisse penser que les menaces ont évolué à un tel point de dangerosité qu'elles

[79] Agence France Presse, « Le Drian annonce 200 emplois en Bretagne dans la "cyber-défense" », 7 septembre 2012.

viennent directement affecter les intérêts des Etats. Bien évidemment, les menaces que nous avons décrites dans la première partie et touchant les entreprises peuvent intéresser les gouvernements et les armées. Des menaces militaires et politiques récentes incitent les gouvernements à former des agences pour lutter spécifiquement contre ces menaces.

2.3.1.1 APT, SCADAs, cyberguerre : la cybersécurité contrainte d'accélérer

Une énergie particulière a été consacrée dans les dernières années au développement de cyberarmes extrêmement puissantes afin d'atteindre des buts fixés par des acteurs d'importance politique, économique ou militaire. Aujourd'hui, les outils d'attaque les plus dangereux sont conçus pour s'en prendre à des victimes spécifiques. Ces outils sont inconnus des éditeurs d'antivirus avant qu'ils aient été découverts après avoir fait effet (principe du *zero-day*). Le terme anglais d'*Advanced Persistent Threat* (APT) recouvre en partie ces nouvelles menaces. Un expert de l'entreprise Sourcefire décrit les APT comme des *« attaques complexes, ciblées et persistantes visant à exfiltrer d'un réseau informatique des informations précises sur un individu, un groupe d'individus ou une organisation »*[80]. A l'instar du virus Stuxnet largement couvert dans les médias récemment[81], des équipes d'experts en sécurité informatique peuvent exploiter les vulnérabilités des systèmes d'information des infrastructures critiques (SCADAs). Ces failles dans les réseaux électriques, de transports, d'eau et autres commencent seulement à être connues du grand public malgré leur gravité. La gravité et la complexité de ces menaces ainsi que leur domaine critique d'application exigent le recrutement d'experts en cybersécurité chevronnés, formés à ce type de problématiques.

2.3.1.2 Des menaces cyber à des fins politiques ou idéologiques qui visent à détruire

Mais plus que la nature des menaces, c'est leur aspect politique, économique et militaire qui les font rentrer dans le champ d'action des Etats. La particularité des menaces cyber en 2012 ne réside pas tant dans leur sophistication que dans l'usage qu'on en fait. Dans le domaine économique d'abord, le pillage de données peut prendre une telle ampleur qu'il affecte en profondeur l'économie d'un pays et le sentiment de sécurité que peuvent avoir les consommateurs et entreprises. Les *Advanced Persistent Threat* n'ont d'ailleurs pas qu'un aspect économique quand elles s'attaquent à des industries de la défense et de l'aérospatial. Les menaces cyber sont également appropriées par des acteurs en conflit pour des raisons politiques ou militaires. Ainsi, de manière plus grave, elles peuvent avoir pour but la destruction pure et simple plutôt que le profit économique, comme l'ont démontré les virus Flame et Stuxnet utilisés contre les centrales iraniennes. Quand les menaces cyber ont de telles capacités de destruction, elles rentrent dans le domaine d'intérêt des armées, qui ont toutes les raisons de s'y intéresser de près. Les Etats mènent des efforts tant du côté de la lutte informatique défensive (LID) que de la lutte informatique offensive (LIO). Le rapport Bockel a très

[80] Experts-IT, « Cyber-Espionnage / Advance Persistent Threats (APT) : Science-Fiction ou réalité ?? ». Accessible ici : http://experts-it.fr/2011/06/03/cyber-espionnage-advance-persistent-threats-apt-science-fiction-ou-realite%C2%A0/

[81] New York Times, « Obama Order Sped Up Wave of cyberattacks Against Iran », 1 juin 2012. Accessible ici: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

récemment évoqué l'opportunité d'une doctrine publique française en matière de LIO, accompagné d'un effort de recrutement important.

2.3.1.3 L'asymétrie de la cyberguerre

Il y a en matière de cyberguerre une asymétrie complète entre la capacité de petites équipes de hackers à causer des destructions importantes et le besoin en experts du côté de la cybersécurité des structures et des données. Face à de petites équipes de hackers et d'experts informatiques, les Etats doivent mettre en place des chaînes de commandement et des structures de sécurité informatique de grande ampleur afin que les points critiques qui ont besoin d'être défendus le soient à chaque niveau. Prenons l'exemple des Etats-Unis : les responsables de la cybersécurité informatique du pays tirent la sonnette d'alarme sur leur manque de « cybersoldats », mais c'est pourtant de ce pays qui a pu produire Stuxnet avec seulement une poignée d'experts informatiques. Si les cybermenaces prolifèrent à une grande vitesse, les moyens de la protection face à celles-ci sont bien plus difficiles à mettre en place.

2.3.2 Les métiers de la cybersécurité : des mathématiciens, ingénieurs et juristes au service de l'Etat

Y'a-t-il une réelle différence entre les métiers de la sécurité informatique tels que pratiqués dans les entreprises et administrations et ceux qui intéressent directement les agences de l'Etat ? Il y a lieu de rappeler encore une fois que le travail d'informaticiens travaillant dans une grande entreprise ou à l'Agence nationale de sécurité des systèmes d'information (ANSSI) connaît un certain nombre de similitudes. Mais nous allons ici nous intéresser à ce qui fait la différence entre ces métiers, les spécificités sur lesquelles repose le métier des experts en cybersécurité du gouvernement et en quoi cela affecte leur recrutement et leur formation.

Pour ce qui est de systématiser et décrire les métiers de la cybersécurité, deux difficultés demeurent. Il y a d'abord peu d'informations disponibles en source ouverte qui nous permettraient de dépeindre le travail au quotidien d'experts travaillant pour le ministère de la Défense ou pour d'autres organisations qui travaillent sous habilitation. Sur les 58 annonces de recrutement actuellement exposées sur le site de l'ANSSI, il n'y en a pas une qui évoque un poste sans habilitation « secret défense ». Même dans le domaine des entreprises de sécurité informatique, le secret peut être imposé par le gouvernement. Récemment, l'agence de recherche du ministère de la Défense américain lançait un programme d'automatisation de la lutte dans le cyberespace, Plan X[82]. Pour participer à la journée de lancement dédiée aux entreprises de sécurité informatique, il fallait être habilité « secret défense ».

[82] CCC Blog, « DARPA to Hold Proposers' Day Ahead of New Foundational Cyberwarfare Program », 22 août 2012. Accessible ici: http://www.cccblog.org/2012/08/22/darpa-to-hold-proposers-day-ahead-of-new-foundational-cyberwarfare-program/

La deuxième difficulté réside plus prosaïquement dans l'aspect embryonnaire des métiers de la cybersécurité et de la cyberdéfense. Il est difficile de dégager un profil-type de professionnel de la cybersécurité travaillant pour l'Etat. Ceux-ci sont peu nombreux et ont pour un grand nombre d'entre eux accédé à leur poste récemment.

Il est toutefois possible de déceler certaines tendances que nous décrirons ci-dessous.

2.3.2.1 Des professionnels aux compétences techniques particulièrement poussées

Les professionnels de la cybersécurité, qu'ils travaillent pour l'Etat ou pour une entreprise de sécurité informatique sont amenés à mener des recherches plus théoriques en matière de sécurité que les professionnels décrits dans la première partie. L'idée de la lutte informatique repose sur un dynamisme permanent dans le cyberespace qui interdit aux acteurs de se reposer sur leurs acquis. Un expert de l'OTAN décrit la lutte informatique de cette manière : *« La cyber-défense (ou LID - Lutte Informatique Défensive), qui correspond aux aspects dynamiques et temps réel de la sécurité informatique pour pouvoir détecter les attaques et se défendre, est basée sur de nombreux outils et produits de sécurité comme les systèmes de détection d'intrusion (IDS), les outils de scan de vulnérabilités, les antivirus ainsi que les systèmes de gestion et corrélation d'événements sécurité (SIEM : Security Information and Events Management). »*[83]

Naturellement, les compétences requises pour opérer dans ce contexte sont bien plus techniques que celles demandées à un RSSI en entreprise. Il ne s'agit plus de trouver des managers qui puissent *« collaborer avec les métiers »*[84] mais des ingénieurs ayant des connaissances fondamentales en mathématique et en informatique. Les annonces de recrutement dans des organisations de cybersécurité et de cyberdéfense reflètent bien ce besoin en compétences particulières. En voici quelques exemples :

Quelques annonces de l'ANSSI (extraits) :

Pour un ingénieur au bureau contrôles réglementaires : « Le titulaire doit être diplômé d'une école d'ingénieur. Il doit disposer d'un **bon niveau général** en systèmes de télécommunication, en systèmes informatiques. Il doit également posséder une bonne connaissance dans le domaine de la **sécurité des technologies de l'information, notamment en cryptologie**. De bonnes **connaissances des textes réglementaires** nationaux et internationaux dans les domaines du contrôle constitueront un atout. Le titulaire doit […] faire preuve de **discrétion sur les sujets sensibles** et avoir une bonne **pratique de l'anglais** courant, tant à l'oral qu'à l'écrit. »[85]

[83] Philippe Lagadec, "Visualisation et Analyse de Risque Dynamique pour la Cyber-Défense", date inconnue. Accessible ici : https://www.sstic.org/media/SSTIC2010/SSTIC-actes/CyberDefense/SSTIC2010-Article-CyberDefense-lagadec.pdf

[84] AMRAE-Clusif, publication collaborative « RM et RSSI : deux métiers s'unissent pour la gestion des risques liés au Système d'Information », page 35, Juin 2006. Accessible ici : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-RM-RSSI-GESTION-DES-RISQUES.pdf

[85] http://www.ssi.gouv.fr/IMG/pdf/FdP_ANSSI_SDE_PSS_BCR_ingenieur.pdf

Pour un spécialiste en sécurité des composants : « Le titulaire devra être diplômé d'un **doctorat en électronique** ou bien être diplômé d'une formation à connotation micro-électronique de niveau BAC+5 et justifier d'au moins 2 ans d'expérience pratique dans le domaine de la sécurité matérielle. Le titulaire possèdera de **solides connaissances en conception numérique** (FPGA, ASIC, …) et en **électronique analogique**. Une bonne connaissance des problématiques de sécurité dans le domaine des composants et des cartes à puces, ainsi qu'une **expérience dans la mise en oeuvre d'attaques matérielles** seraient appréciées. De **bonnes bases dans les domaines de la cryptographie, de l'optique et/ou de l'électromagnétisme** sont également souhaitables. »

Pour un ingénieur projet supervision de sécurité : Les candidats doivent être titulaires d'un diplôme d'ingénieur reconnu par la commission des titres d'ingénieur. Compétences mises en œuvre : **connaissance des principes de fonctionnement des solutions de supervision des informations et des événements de sécurité (SIEM)**; maîtrise des protocoles courants pour le fonctionnement des services ; connaissance du **fonctionnement des sondes de détection d'intrusions, de systèmes de filtrage d'attaques** (prévention d'intrusions, filtrage d'attaques en déni de service distribué, web application firewall…) et **d'outils de corrélation de journaux d'événements** ; bonne connaissance d'**un ou plusieurs langages de** programmation et de scripts (Python, Perl, C).

Une annonce de recrutement chez Cassidian

Vous intégrerez l'équipe Security Assurance et serez impliqué dans les activités d'expertise Pentest/Audit, Forensic et Réponse sur incident.
Vous travaillerez dans une équipe de référence, dynamique et volontaire et serez amené à intervenir sur la plupart des sujets de l'équipe.
Vous participerez à des missions variées (projets internes et projets clients) avec de forts enjeux stratégiques.
Vous travaillerez plus particulièrement sur les missions de réponse à incident et d'audits techniques.
Votre savoir-faire et votre tempérament vous amèneront à être responsable rapidement de certaines missions.

Vous analyserez des logiciels et des codes sources à la recherche de vulnérabilités.
Vous développerez des codes d'exploitation permettant de démontrer la présence de vulnérabilités.

Vous analyserez certains logiciels malveillants.
Vous automatiserez les analyses de certaines malveillances.
Vous participerez aux missions de réponse à incident en analysant les logiciels malveillants.
Vous développerez les outils pour supporter votre activité ainsi que ceux pour le reste de l'équipe.
Vous serez amené à formaliser votre expertise pour des formations internes et externes.

2.3.2.2 Militaires et juristes: la pluridisciplinarité en dehors du champ technique

Comme nous l'avons constaté, plus la cybersécurité se complexifie, plus elle fait appel à des spécialistes qui doivent dépasser la vision globale que pourrait avoir un RSSI. Dans cette course à la compétence spécifique, ce sont évidemment les ingénieurs et autres métiers scientifiques qui sont les premiers recherchés par les recruteurs. Mais la spécialisation concerne aussi des domaines non

techniques, donnant ainsi aux non-techniciens un rôle essentiel à jouer dans le domaine de la sécurité informatique.

2.3.2.2.1 Les juristes du cyber, un travail primordial dans la cyberdéfense et la lutte contre la cybercriminalité

C'est par exemple le cas des juristes, à propos desquels nous avons vu qu'ils prenaient une place grandissante en entreprise, en particulier au sein de celles travaillant avec les nouvelles technologies et le web. En effet, la cybersécurité a un impact direct sur les questions de vie privée, de propriété intellectuelle ou de surveillance et la législation sur ces sujets est en évolution permanente. Dans le cas spécifique des pouvoirs de l'Etat, les juristes auront un rôle de plus en plus important dans la lutte contre la cybercriminalité, qui constitue aujourd'hui la menace cyber la plus répandue.[86] Le site web officiel de la Gendarmerie nationale explique que celle-ci s'est *« engagée résolument ces dernières années, dans la lutte contre les nouvelles formes de criminalité, en rapport notamment avec l'utilisation de l'Internet. Cette nouvelle typologie de crimes et de délits a nécessité la mise en place aux niveaux central et territorial de formations et de moyens spécifiques. »* Parmi les unités de lutte, on compte par exemple le Département cybercriminalité du service technique de recherches judiciaires et de documentation (STRJD). Il existe également des formations à même de produire des juristes en cybercriminalité, parmi lesquelles on peut compter par exemple le Master « Cybercriminalité : Droit, Sécurité de l'information et Informatique légale » de l'Université de Montpellier ou le Master 2 Droit et stratégies de la sécurité de l'Université Panthéon-Assas.[87]

2.3.2.2.2 Quel rôle pour les politiques et les militaires dans la cybersécurité ?

Mais ce sont aussi dans les domaines de l'action politique et militaire que s'est étendue la cybersécurité. En France et ailleurs, des unités spécifiques du gouvernement et du ministère de la Défense sont maintenant dédiées à la cybersécurité. On y trouve des professionnels au parcours scientifique limité mais capables de comprendre les ressorts politiques du cyberespace et de les exploiter.

En France, le ministère de la Défense mène des efforts particuliers pour disposer des moyens humains nécessaires à la cybersécurité du pays. On peut à ce titre citer deux exemples récents. Une chaire de cyberdéfense a été inaugurée en juillet 2012 au sein des écoles de Saint-Cyr Coëtquidan. Celle-ci vise en outre à *« développer les enseignements dans le domaine de la cyberdéfense en formation initiale, pour les élèves officiers en scolarité aux ESCC, et en formation continue, à destination des décideurs publics et privés. »*[88] Un blogueur estime cela dit que cet effort est encore

---

[86] E-juristes.org, Nathalie Bismuth, « Les perspectives pénales de la LOPPSI 2 en matière de cybercriminalité », 10 février 2010. Accessible ici : http://www.e-juristes.org/les-perspectives-penales-de-la-loppsi-2-en-matiere-de-cybercriminalite/

[87] Montpellier : http://www.dynamiques-du-droit.cnrs.fr/spip.php?article593
Panthéon-Assas : http://www.u-paris2.fr/5610p-2009/0/fiche___formation/

[88] Site web du ministère de la Défense, « Inauguration d'une chaire de cyberdéfense », 17 juillet 2012. Accessible ici : http://www.defense.gouv.fr/terre/actu-terre/inauguration-d-une-chaire-de-cyberdefense

marqué d'une centralisation trop importante si l'on compare la chaire à une initiative du même genre aux Etats-Unis, le NCCoE[89]. Deuxième actualité intéressante, la création d'un groupe de réservistes spécialisés en cyberdéfense, dans le cadre de la réserve citoyenne, à la rentrée 2012. Coordonnée par l'OG Cyber et Luc-François Salvador (qui recevra pour cela une lettre de mission personnelle), cette réserve est constituée d'un *« noyau de volontaires accrédités par l'autorité militaire qui apportera sa contribution à la cyberdéfense française. Les réservistes établiront un réseau qui travaillera en étroite concertation avec les autorités nationales en charge du domaine. »*[90] A l'étranger, on connaît les efforts particuliers des armées américaines et israéliennes[91].

Enfin, des experts sur les questions de cybersécurité pourraient avoir leur rôle au sein de ministères des affaires étrangères tant les questions de communication internet et de réseaux sociaux se retrouvent au centre de l'actualité alors que le monde arabe est secoué par des révolutions qualifiées de « 2.0 »[92].

2.3.2.2.3 L'internationalisation au travers des conférences et organisations

On a pu remarquer au cours des dernières années plusieurs signes de la prise de conscience au niveau international du rôle crucial de la sécurité de l'information dans la sécurité et la défense des Etats. Cette prise de conscience s'accompagne d'une discussion transnationale entre les professionnels de la cybersécurité, que ce soit au travers de forums, de conférences, ou d'organisations internationales spécifiquement dédiées à la cybersécurité.

2.3.2.2.3.1 Les conférences internationales sur le thème de la cybersécurité

La tenue de conférences et forums à travers dans le monde sur la question de la cybersécurité et de la cyberdéfense constitue un signe visible de la structuration et du développement de ces métiers. Elles sont pour les professionnels l'occasion de se rencontrer et de discuter mais également de prendre conscience de l'importance que prend leur rôle aux yeux des Etats en même temps que se développent les ressources humaines de la cybersécurité.

Certaines conférences à l'aspect plutôt techniques font appel à un public en grande partie constitué d'ingénieurs en informatique. On assiste également à l'ouverture de ce genre de conférences à des publics différents, parfois issus du monde politique ou militaire.

En France, le Forum International de la Cybersécurité (FIC) qui tiendra sa cinquième édition en janvier 2013 à Lille, est « un rendez-vous majeur pour les acteurs de la sécurité du cyberespace

---

[89] Si Vis Pacem Para Bellum, « Chaire de cyberdéfense, NCCoE : deux centres d'excellence cyber, une différence fondamentale », 7 juillet 2012. Accessible ici : http://alliancegeostrategique.org/2012/07/07/chaire-de-cyberdefense-nccoe-deux-centres-dexcellence-cyber-une-difference-fondamentale/

[90] Site web du ministère de la Défense, « Des réservistes spécialisés en cyberdéfense », 13 septembre 2012. Accessible ici : http://www.defense.gouv.fr/actualites/articles/des-reservistes-specialises-en-cyberdefense

[91] Blog officiel de L'armée de défense d'Israël en français, « Tsahal en 2012, c'est aussi la guerre cybernétique ». Accessible ici : http://tsahal.fr/2012/04/29/tsahal-en-2012-cest-aussi-la-guerre-cybernetique/

[92] Le Monde, « Les révoltes arabes sont-elles des révolutions 2.0 ? », 21 février 2011. Accessible ici : http://www.lemonde.fr/afrique/article/2011/02/21/les-revoltes-arabes-sont-elles-des-revolutions-2-0_1483033_3212.html

compte tenu de son envergure internationale et de l'importance des différentes thématiques abordées. »[93] Bien que réservé aux professionnels, le FIC attire des métiers très différents mais tous directement intéressés par la cybersécurité : *« juristes, responsables de la sécurité des systèmes d'information ; Non spécialistes : directeurs sécurité, directeurs des ressources humaines, risk managers, secrétaires généraux, assureurs, services de police et de gendarmerie, magistrats, universitaires. »*

2.3.2.2.3.2 Les organes internationaux

Au-delà de ces conférences qui réunissent pendant quelques jours des acteurs phares de la cybersécurité, des organes se sont constitués à l'échelle internationale pour réunir durablement les organisations et professionnels de la cybersécurité. Ces organes permettent en premier lieu de mieux assurer la prévention des menaces cyber qui ne s'arrêtent pas aux frontières. Mais elles sont aussi un moyen majeur de discussion et de mobilité pour les professionnels de la cybersécurité.

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) est un de ces organes qui intéresse tout particulièrement les institutions françaises. Cette agence créée par la commission européenne est basée à Héraklion, en Grèce, et réunit des professionnels des 27 Etats-membres de l'Union Européenne[94]. D'après son site web, *« L'ENISA a pour mission d'assurer un niveau élevé de sécurité des réseaux et de l'information. Elle agit de différentes façons: en intervenant en tant qu'expert en matière de sécurité des réseaux et de l'information auprès des autorités nationales et des institutions européennes; en favorisant l'échange de meilleures pratiques; et en facilitant les contacts entre les institutions (nationales et européennes) et les entreprises. »*[95] Son travail consiste en grande partie à mener des études et publier des rapports sur l'état de la cybersécurité des réseaux et de l'information en Europe. Elle organise également des déplacements dans les CERT (*Computer Emergency Response Team*) nationaux ou des ateliers, comme celui qui réunira des experts européens et américains le 15 octobre 2012 à Amsterdam sur le thème la sécurité des systèmes de contrôle industriel. De manière plus générale, l'ENISA œuvre pour une fluidification des rapports public-privés dans le domaine de la sécurité de l'information.

2.3.3 Formations, recrutement et carrières dans la cybersécurité

2.3.3.1 Pas de main-d'œuvre compétente sans des bassins de formation

Nous avons vu que le ministre de la Défense avait annoncé la création de 200 postes dans la cybersécurité à la DGA en Bretagne. Plusieurs dizaines d'annonces sont présentes sur le site de l'ANSSI. Cassidian vient de former une unité entièrement dédiée à la cybersécurité pour laquelle elle recrute. Le risque le plus grave pour le moment ne réside pas dans l'inexistence d'un esprit de corps

[93] Site web officiel du FIC. Accessible ici : http://fic2013.com/?conference=forum-international-sur-la-cybercriminalite-2016

[94] On peut citer à titre d'exemple Constance Bommelaer, récemment nommée directrice du groupe d'experts de l'Agence. Réserviste dans la Marine française, elle a occupé des postes à Matignon ou au sein de l'Internet Society avant de rejoindre l'ENISA.

[95] Site web officiel de l'ENISA. Accessible ici : http://www.enisa.europa.eu/media/enisa-en-francais/

ou d'associations de professionnels de la cybersécurité. Il s'agit plutôt d'un problème bien plus large de structuration et de systématisation complète des formations qui peuvent produire une main-d'œuvre qualifiée pour répondre à la demande qui émane actuellement de l'Etat et des entreprises de sécurité informatique. Les formations et ingénieurs en sécurité des systèmes d'information existent déjà en France et ailleurs mais deux problèmes subsistent. Certains estiment d'abord que trop peu d'étudiants sortent de ces formations chaque année. Même si assez d'étudiants en sécurité informatique sont formés pour combler en théorie les postes proposés par les agences gouvernementales et les entreprises de sécurité informatique, les recruteurs peuvent se plaindre du manque de talent dû à la faible compétition entre les candidats. Comme le démontrent les annonces de recrutement précédemment citées, les postes peuvent être extrêmement exigeants. Une compétition saine entre un grand nombre de candidats a plus de chance de mener au recrutement de personnes compétentes que le cas inverse.

Deuxièmement, on peut estimer que les formations actuelles en cybersécurité ne prennent pas en compte la spécificité de la cybersécurité de l'Etat. Elles ne forment pas les ingénieurs avec le sens de l'Etat et n'intègrent pas la cybersécurité dans un cadre politique et militaire. La création d'une chaire de cybersécurité à l'ESM Saint-Cyr montre bien qu'il faut multiplier les tentatives de rapprochement entre la cybersécurité et le monde militaire.

Le Maryland Cybersecurity Center

Une récente initiative de l'Université du Maryland constitue un exemple intéressant de tentative de rapprochement des univers de la sécurité informatique et de la sécurité nationale au sein d'une même institution académique. En 2010, cette université a ouvert un nouveau centre, le Maryland Cybersecurity Center, ou MC2. Rattaché à l'université, il sert de plateforme pour de nombreuses utilisations visant à rapprocher gouvernement, entreprises et universités autour de conférences et de formations dédiées à la cybersécurité dans son aspect défense/sécurité. La création de ce centre pourrait avoir un impact significatif pour le futur de la cybersécurité aux Etats-Unis.

C'est d'abord le cas grâce à sa position virtuelle et physique idéale, entre différentes institutions intéressées par la cybersécurité. Le MC2 bénéficie en outre de partenariats avec Northrop Grumman et Lockheed Martin, géants américains de l'armement, mais aussi avec Google ou Sourcefire. Le centre tient une série de conférences avec Google à chaque semestre ou sont invités experts d'horizons différents à discuter de questions de cybersécurité et de cyberdéfense. Deuxième élément qui fait l'originalité du MC2, il propose non seulement des masters en cybersécurité mais également des formations de niveau *undergraduate* aux étudiants. En d'autres termes, les étudiants de l'université du Maryland peuvent choisir dès leur première année d'étude, soit à l'âge de 18 ans, de commencer à étudier les questions de sécurité informatique. Northrop Grumman sponsorise ainsi le programme Advanced Cybersecurity Experience for Students (ACES), qui *"immerge les étudiants*

undergraduate dans tous les aspects du domaine de la cybersécurité afin de répondre à une besoin croissant de la nation et de l'Etat du Maryland en main-d'œuvre"[96].

Cette carte où le MC2 se trouve au centre indique où se situent les innombrables agences gouvernementales et entreprises de la région qui font toute la politique de cybersécurité des Etats-Unis.

Source : Présentation du MC2 par son directeur, Michael Hicks. Accessible sur : http://www.gamesec-conf.org/2011/files/01_HICKS__GameSec2011_11142011.pdf

Comme à bien d'autres égards, les Etats-Unis ont une longueur d'avance sur d'autres pays en matière de main-d'œuvre pour la sécurité informatique. Mais partout dans les pays développés, les gouvernements prennent conscience du besoin croissant en expertise informatique. Face à l'impossibilité de recruter en masse parmi des hackers rares et peu enclins à travailler pour des agences de sécurité, ces gouvernements sont tentés de mettre en place des programmes de formations massifs selon la même idée que le MC2.

2.3.3.2 Généralisation des formations en informatique et en sécurité informatique – le développement d'une « hygiène » de la cybersécurité

Du point de vue de la cybersécurité nationale, l'Etat a également intérêt à avoir une plus grande part de sa population qui soit formée à la sécurité informatique. Même si tous les ingénieurs ne sont pas

[96] Communiqué du MC2, "Unique Program To Educate Next Generation of U.S. Cybersecuity Leaders", date inconnue. Accessible ici: http://www.cyber.umd.edu/news/news_story.php?id=6556

destinés à occuper des positions dans des organisations de sécurité informatique, la diffusion d'une culture de la sécurité pourrait conduire à cette « hygiène » qui manque et à la conception de systèmes d'informations qui prennent en compte la sécurité à la racine.

L'Estonie a récemment décidé de proposer à ses élèves de classes élémentaires des cours de programmation informatique. Ces cours ne seront pas obligatoires et universels dès le début mais pourraient le devenir à terme. Le blog UbuntuLife explique en quoi ce projet devrait permettre de fournir la main-d'œuvre manquante aux compagnies high-tech du pays dans dix ou vingt ans.[97] La solution adoptée par l'Estonie ne permet pas de répondre immédiatement aux crises diverses induites par l'insécurité informatique et dont le pays a d'ailleurs fait les frais en 2007[98]. De même, si l'on est forcé de reconnaître que certaines professions ou industries pourraient bénéficier d'une plus grande connaissance de la programmation ou sécurité informatique, certains doutent que l'ensemble de la population puisse en avoir besoin[99]. Mais sur le long terme, c'est-à-dire à un horizon de quinze ou vingt ans, on peut parier que cela contribuera à la résolution de la question de la main-d'œuvre en sécurité informatique. Plus généralement, enseigner des bases en sécurité informatique à la population permet une sensibilisation extrêmement efficace qui pourrait résoudre la plupart des problèmes de sécurité dont le maillon faible reste le facteur humain manquant de vigilance.

2.3.3.3 Un recrutement aléatoire et difficile

Si les formations manquent en matière de cybersécurité, c'est le volume de la main-d'œuvre qui en subit directement les conséquences. Dès lors, le décalage entre l'offre et la demande rend le recrutement difficile. Les conséquences de ce recrutement de crise, particulièrement visible aux Etats-Unis, ont été soulignées par les médias.

Un article du magazine américain The Atlantic Wire explique comment les agences de sécurité et de renseignement américaines sont contraintes de recruter à des conférences et évènements qui attirent les hackers et autres experts informatiques. Le journal prend l'exemple de la visite de Keith Alexander, directeur de la NSA, à la conférence DefCon qui réunit chaque année des hackers, journalistes et experts de sécurité informatique à Las Vegas. Devant un parterre de hackers, Alexander louait leur travail *: « dans cette pièce, celle-ci même, se trouve le talent dont notre nation a besoin pour sécuriser son cyberespace. »* Le manque de main-d'œuvre en matière de cybersécurité aux Etats-Unis comme ailleurs est bien connu[100] [101]. En arpentant les hackatons et autres conférences qui réunissent des passionnés de sécurité informatique, le gouvernement veut aller chercher la main-

---

[97] UbuntuLife, "Computer programming will soon reach all Estonian schoolchildren", 4 septembre 2012. Accessible ici: http://ubuntulife.net/computer-programming-for-all-estonian-schoolchildren/

[98] 01Net, "L'Estonie dénonce les cyber-attaques de terroristes russes", 11 juin 2007. Accessible ici : http://www.01net.com/editorial/350759/lestonie-denonce-les-cyber-attaques-terroristes-russes/

[99] Jeff Atwood, "Please don't learn to code", 15 mai 2012. Accessible ici: http://www.codinghorror.com/blog/2012/05/please-dont-learn-to-code.html

[100] NextGov, « Cyber Command struggles to define its place on a shifting battlefield », 16 août 2012. Accessible ici: http://www.nextgov.com/cybersecurity/2012/08/hacker-wars/57438/

[101] The Guardian, "US urged to recruit master hackers to wage cyber war on America's foes", 10 juillet 2012. Accessible ici: http://www.guardian.co.uk/technology/2012/jul/10/us-master-hackers-al-qaida

d'œuvre dans le seul endroit où elle est pour le moment susceptible d'avoir le niveau technique particulièrement élevé pour mener une lutte informatique.

Pourtant, ces opérations de recrutement menées dans l'urgence laissent penser que les Etats-Unis naviguent à vue dans un domaine pourtant crucial pour les fonctions critiques et régaliennes de l'Etat, des infrastructures et des entreprises du pays. Les formations universitaires de SSI n'étant visiblement pas capable de fournir assez de main-d'œuvre aux agences de cybersécurité, toujours plus nombreuses, le gouvernement est contraint de procéder à des recrutements relativement aléatoires.

2.3.3.3.1 Quelles sont les barrières au recrutement ?

Un rapport de la société de services en ingénierie informatique Booz Allen Hamilton sur le recrutement fédéral aux Etats-Unis d'experts en cybersécurité publié en 2009 jetait la lumière sur les barrières au recrutement.[102] Elles sont encore très nombreuses. Il peut d'abord s'agir de **la lenteur du processus de recrutement**, en particulier dans des agences gouvernementales où une habilitation est requise. Le recrutement en cybersécurité est bel et bien urgent, et la longueur du processus de gestion des candidatures peut souffrir de la comparaison avec des petites sociétés informatiques très dynamiques. Les ingénieurs informatiques ont besoin d'être démarchés dès leur sortie d'école et seront peu enclins à patienter plusieurs mois pour voir si leur candidature aboutit.

Autre barrière de première importance : **les salaires** dans le public sont souvent inférieurs et moins flexibles que ceux proposés dans des entreprises très compétitives en pleine expansion. Le rapport de Booz Allen Hamilton explique que les décalages de salaires freinent le recrutement dans le public et peuvent inciter les employés à quitter prématurément leur poste au profit d'une entreprise. Ce peut être d'autant plus alarmant si des organisations publiques sont contraintes d'externaliser la gestion de leur sécurité informatique vers ces mêmes entreprises qui attirent les étudiants les plus brillants. Sur la question des salaires, les auteurs du rapport insistent sur le marketing qui peut être fait pour attirer des personnes tentées par un poste dans une entreprise : *« Beaucoup de candidats mettent en avant leur désir de changer les choses et de travailler pour le pays. Quand l'aspect crucial de la cybersécurité est mis en avant, le gouvernement peut être plus attirant qu'une entreprise. »* Beaucoup de nouveaux employés restent travailler pour le gouvernement plutôt que de partir, *« parce que le travail est amusant (fun) ».* [103]

2.3.3.3.2 Une bourse scolaire contre un recrutement gouvernemental – un programme de recrutement original

Le Department of Homeland Security des Etats-Unis associé à d'autres agences gouvernementales entretient un programme de bourses visant à fournir une main-d'œuvre stable au gouvernement en

---

[102] Booze Allen Hamilton, *Strengthening the Federal Cybersecurity Workforce*, 22 juillet 2009. Accessible ici: http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf

[103] Ibid, page 11-12.

matière de cybersécurité, le Scholarship for Service, ou CyberCorps[104]. Les étudiants boursiers voient tous leurs frais d'université payés par le gouvernement, ainsi que leur logement et autres frais pour étudier la sécurité informatique dans une des quelques dizaines d'universités participantes. A sa sortie d'université, le plus souvent avec un Master, l'étudiant a l'obligation de travailler pour le gouvernement un nombre d'années équivalent à la durée de la bourse.

En 2010, 225 étudiants étaient inscrits au programme et 870 étudiants avaient bénéficié de la bourse depuis sa création en 2001[105]. Il se pourrait que le budget du SFS soit en augmentation importante depuis 2009, et que le nombre d'étudiants sortant chaque année du programme pour travailler pour le gouvernement s'accroisse. La National Security Agency et le Department of Defense sont les deux plus gros recruteurs des étudiants du CyberCorps. Le SFS apporte la garantie au gouvernement qu'un nombre connu et prévisible d'étudiants ayant des capacités avancées en sécurité informatique iront travailler pour ses agences. Le fait de faire entrer des étudiants dès la fin de leurs études au service du gouvernement peut les pousser à y faire carrière toute leur vie plutôt que d'être tentés d'aller travailler pour des SSII. Un officier américain expert en sécurité informatique présente le CyberCorps de la façon suivante : *« un adolescent de 130 kilos qui se nourrit de chips et de soda serait une aberration complète au sein du Corps des Marines. Mais équipé des bonnes compétences techniques, ce même adolescent pour être lors d'une cyberguerre l'équivalent de Chesty Puller [un officier mythique du Corps des Marines]. »*[106]

La situation n'est pas nécessairement la même en France. Un expert en cybersécurité[107] estime qu'en France, *« les agences gouvernementales restent un le pilier du développement "cybersécurité" du pays et la plupart des diplômés dans ces domaines et voulant continuer en sécurité passeront par les agences gouvernementales pour se faire une idée de la réalité de la chose. »* Il ajoute qu' *« aujourd'hui, ces agences recrutent tous les "bons" et on se retrouve aujourd'hui avec un réel manque de matière grise dans le privé. »*

Le rapport Bockel sur les effectifs de l'ANSSI

« La principale faiblesse de l'agence tient cependant à la modestie de ses effectifs et de ses moyens. Comme on l'a vu précédemment l'ANSSI a connu ces dernières années une augmentation significative de ses personnels, mais le nombre total de ses agents reste encore inférieur de moitié, voire d'un tiers, à celui des agences homologues de nos partenaires britanniques ou allemands.

Même si l'on ne peut pas négliger les difficultés à recruter un nombre aussi significatif de personnels spécialisés dans des délais aussi courts, il semble souhaitable que le prochain Livre blanc fixe des objectifs ambitieux. Pour votre rapporteur, cet objectif doit être de parvenir progressivement, sur

[104] Site officiel de SFs, https://www.sfs.opm.gov/.

[105] Cabinet Booz Allen Hamilton, "Cyber In-Security; Strengthening the Federal Cybersecurity Workforce", juillet 2009. Accessible ici: http://www.boozallen.com/media/file/CyberIn-Security_2009.pdf

[106] John R. Surdu et Gregory J. Conti, "Join the Cyber Corps; A proposal for a *Different* Military Service", 2002. Accessible ici: rumint.org/gregconti/publications/cyber_corps.doc

[107] Entretien accordé par un expert en cybersécurité travaillant dans la sécurité informatique pour le gouvernement.

plusieurs années, à un niveau similaire à celui des services équivalents de l'Allemagne et du Royaume-Uni. Il semble donc souhaitable d'élaborer, dans le cadre du nouveau Livre blanc, un plan pluriannuel permettant de poursuivre au même rythme, voire d'amplifier, l'augmentation des effectifs de l'ANSSI dans les prochaines années et de renforcer parallèlement l'effort d'investissement. Une croissance régulière des effectifs de l'ANSSI de l'ordre de 80 personnes supplémentaires par an lui permettrait ainsi d'atteindre 500 personnes à la fin de l'année 2015. Les volumes d'effectifs et d'investissements concernés sont au demeurant modestes. »

2.4 Conclusion

A l'aune de ce décalage entre une demande accrue d'experts en sécurité informatique et une offre trop embryonnaire, comment s'organisent et se structurent les ressources humaines de la cybersécurité ?

Il y a autant d'aspects dans la sécurité informatique qu'il y a d'états d'avancement et de structuration des ressources humaines de ce domaine.

Si l'on prend les aspects de la sécurité de l'information les plus anciens, on a une filière des ressources humaines particulièrement structurée et aboutie. Il s'agit des métiers de gestion du risque, de sécurité des systèmes d'information qui bien qu'en pleine évolution, existent pour certains d'entre eux depuis plusieurs décennies. Nous avons vu en quoi le métier de RSSI est aujourd'hui particulièrement bien établi dans toutes les structures qui font un usage intensif de l'informatique, qu'il s'agisse d'entreprises ou d'administrations. Il existe de nombreuses formations universitaires en France et à l'étranger qui forment aux métiers de sécurité de l'information, de même que des filières de recrutement pérennes et dynamiques. Les RSSI sont reconnus par les autres métiers de l'organigramme et une conscience professionnelle émerge avec la création de clubs et de conférences dédiés aux métiers de la sécurité de l'information.

Le constat n'est pas le même pour les professionnels de la cybersécurité et de la cyberdéfense, pour lesquels il est difficile d'identifier une filière structurée des ressources humaines. On constate que ces métiers sont bien plus techniques, spécialisés et demandeurs que ceux de la sécurité de l'information décrits précédemment. Qui plus est, la demande en main-d'œuvre répondant à ces critères exigeants est en train d'exploser sans que les formations puissent assurer une réponse adéquate à ces besoins. A ce titre, les efforts novateurs dans le domaine académique menés en France et ailleurs méritent d'être encouragés et généralisés. Seul un investissement important sur le long terme pourra permettre la formation en France d'ingénieurs, de mathématiciens mais aussi de juristes et militaires capables d'assurer la cyberdéfense du pays.

Enfin, cette étude a décrit différents ***axes de mobilité*** pour les professionnels de la cybersécurité. On constate d'abord que si celle-ci est un domaine qui touche au cœur même des prérogatives étatiques (défense, sécurité de la nation et des citoyens), elle appartient encore en grande partie à la société civile. Les acteurs économiques qui y prennent part sont innombrables et constituent la chaine cruciale de la cybersécurité du pays. Il s'agit des RSSI dans chaque entreprise, des sociétés de service

en ingénierie informatique, des éditeurs d'antivirus traditionnels ou de nouvelle génération et des entreprises de défense et de sécurité. Les ingénieurs et autres experts en sécurité informatique peuvent changer de structure un grand nombre de fois au cours de leur carrière et faire des allers et retours entre les services de l'Etat et ces entreprises.

Deuxième axe de mobilité important, l'internationalisation de l'action en matière de cybersécurité. Il s'agit de conférences, toujours plus nombreuses et qui font se côtoyer des professionnels de la sécurité informatique de cultures et de maturités différentes. La constitution de réseaux et organisations transnationaux dédiés à la sécurité informatique constitue une autre voie d'internationalisation. L'existence de meilleures formations académiques en cybersécurité ici qu'ailleurs peut constituer un aimant important à l'échelle internationale. Enfin, les Etats les plus soucieux de leur cybersécurité et disposant de moyens conséquents peuvent attirer des jeunes talents et des experts pour renforcer les moyens humains de leur cybersécurité.

Cette mobilité et ce dynamisme particulièrement aigu dans les ressources humaines de la cybersécurité sont une opportunité pour les pays qui sauront investir dans leurs moyens humains et jouer habilement sur cette intégration du public et du privé. Les passerelles qui unissent les entreprises directement concernées par la sécurité de l'information et les services de l'Etat dédiés à la sécurité et à la défense constituent un atout de première importance dans une cyberguerre où la rapidité de l'innovation technologique détermine qui perd et qui gagne.