Internet : du rêve du partage généralisé à la nécessaire sécurité

Par Philippe Truillet

"*La méfiance et la prudence sont les parents de la sécurité*"
Benjamin Franklin

Concomitamment aux facilités qu'offrent les moyens technologiques récents, la question de la cybercriminalité se pose dans de nouvelles dimensions et des termes qui, par bien des aspects, peuvent paraître très inquiétants. De simples logiciels aisément accessibles sur Internet permettent à des néophytes de paralyser des sites *Web* (par exemple par le biais d'attaques par déni de service (DDoS[1]) avec l'outil librement téléchargeable *LOIC*[2]) ; de "casser" des mots de passe ou des clés de cryptage *WiFi* (avec des logiciels tels que *John The Ripper*[3] *ou Aircrack-ng*[4]), facilitant ainsi l'intrusion et l'accès à des données sensibles, ou encore de capturer et modifier à la volée des données transitant sur le réseau par la technique dite du *network spoofer*.[5]

Ces attaques via les supports numériques ne concernent pas seulement l'usage de la "force brute" (cassage de mots de passe ou de clés *WiFi* par exemple) mais reposent de manière beaucoup plus importante sur l'ingénierie sociale. En effet, elles suivent le plus souvent une stratégie "globale" mêlant à la fois technique et ciblage d'information : en témoignent les nombreuses affaires récentes révélées (comme l'intrusion sur le site de l'Élysée en 2012 via le réseau social *Facebook*,[6] ou très récemment l'attaque de *TV5 Monde*[7]).

L'émergence des réseaux sociaux facilitant le ciblage des utilisateurs, personne n'est plus à l'abri : particuliers, laboratoires de recherche et développement, grandes entreprises mais aussi et surtout les PME et ETI, pour des motifs divers : appât du gain, vol de données sensibles – brevets, grilles de tarification, etc. De plus, l'utilisation des traces laissées sur le réseau : données stockées sur le "*cloud*", photos géo-localisées, numéros de téléphone, mèls, documents divers (voir à ce sujet l'excellent rapport déclassifié de la NSA, 2013), permet d'abolir les frontières physiques et celles qui séparent usages privé et professionnel – ceci avec l'approbation implicite ou involontaire des usagers transformant notre planète en "village global" hautement interconnecté.

---

[1] Déni de Service Distribué (DDoS) : *cf.* https://www.securiteinfo.com/attaques/hacking/ddos.shtml.
[2] Low Orbit Ion Cannon. *Cf.* http://sourceforge.net/projects/loic.
[3] *Cf.* http://www.openwall.com/john.
[4] *Cf.* http://www.aircrack-ng.org.
[5] *Cf.* http://sourceforge.net/projects/netspoof.
[6] Source : *L'Expansion*, 20 novembre 2012. *Cf.* http://lexpansion.lexpress.fr/high-tech/cyberguerre-comment-les-americains-ont-pirate-l-elysee_361225.html&action_object_map=%7B%2210151464678.
[7] *Cf.* http://www.undernews.fr/hacking-hacktivisme/tv5-monde-spear-phishing-un-simple-mail-aura-suffit.html.

Quelles sont les menaces, réelles ou supposées ? Quelles sont les techniques utilisées ? Qui sont les acteurs et les cibles ? Quelle riposte technique et juridique peut-on proposer pour s'en prémunir ? Telles sont les questions abordées dans cet article.

Réseaux, Internet et attaques

En matière de réseaux (Tanenbaum, 2011), le nom qui vient immédiatement à l'esprit est *Internet*, le "réseau des réseaux". Internet s'est en effet imposé au fil des années comme un standard incontournable, présent sur quasiment tous les réseaux physiques, permettant l'acheminement d'informations par commutation de paquets.[8]

Dans son principe fondateur, Internet a été conçu pour faciliter les communications entre chercheurs. ARPANET,[9] considéré comme son ancêtre, naît en effet "officiellement" en 1969 avec une première communication entre l'université de Californie à Los Angeles (UCLA[10]) et le Stanford Research Institute (SRI[11]) : *cf.* figure 1 ci-dessous. Les usages de ce réseau balbutiant sont imaginés dès 1970 par Doug Engelbart[12] (inventeur, entre autres, de la souris, et précurseur des systèmes hypertextes) :

> There will emerge a new "marketplace", representing fantastic wealth in commodities of knowledge, service, information, processing, storage, etc. In the number and range of transactions, and in the speed and flexibility with which they are negotiated, this new market will have a vitality and dynamism as much greater than today's as today's is greater than the village market.[13]

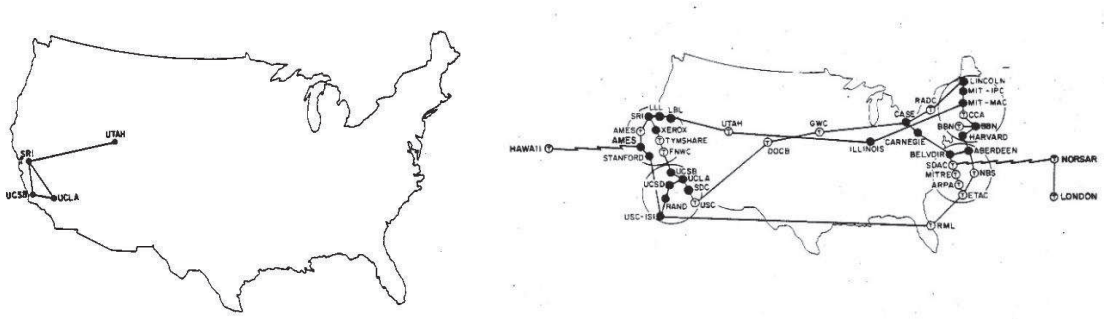


Figure 1 : Évolution du réseau ARPANET entre décembre 1969 et septembre 1973
(Source : http://som.csudh.edu/cis/lpress/history/arpamaps/)

---

[8] Mode d'acheminement de messages dans un réseau de télécommunication, où les messages sont préalablement découpés en paquets munis d'une adresse ; dans les nœuds du réseau, ces paquets sont reçus, mis en mémoire et retransmis sur la ou les voies de transmission appropriées ; à l'arrivée, le message est reconstitué à partir des paquets reçus. *Cf.* http://www.marche-public.fr/Terminologie/Entrees/commutation-de-paquets.htm.

[9] Advanced Research Projects Agency Network : *cf.* http://en.wikipedia.org/wiki/ARPANET.

[10] *Cf.* http://www.ucla.edu.

[11] *Cf.* http://www.sri.com.

[12] *Cf.* http://www.dougengelbart.org/firsts/internet.html.

[13] "*Un nouveau marché va émerger, représentant une richesse fantastique en termes de produits de la connaissance, de services, d'information, de traitement, de stockage, etc. Ce nouveau marché, en nombre et possibilités de transactions, en vitesse et flexibilité avec lesquelles elles seront négociées, aura une vitalité et un dynamisme beaucoup plus grands qu'aujourd'hui, tout comme le marché d'aujourd'hui n'a plus aucune commune mesure avec les marchés de village*".

Rapidement, toutefois, il s'avère nécessaire de refondre les protocoles de communication entre machines hôtes. Ce n'est plus le réseau qui doit assurer la cohérence de ses communications, mais les ordinateurs du réseau eux-mêmes via l'utilisation d'un protocole standard commun à tous, indépendamment du matériel. Il va en découler la définition de "couches réseau" qui constituent des piles de protocoles. Chaque "couche" a la charge d'objectifs spécifiques (par exemple, transférer les données physiquement des données d'un point à un autre, router ces données, vérifier les transferts, etc.). Ceci a l'avantage de pouvoir définir une vision abstraite (donc une généralisation) du comportement du réseau à différents niveaux : du niveau physique à l'applicatif. La normalisation des interfaces de service libère de plus l'utilisateur du besoin de connaître les protocoles utilisés. Ceci permet de prédire et contrôler les conséquences des changements effectués dans un réseau qui s'effectuent ainsi de manière transparente pour les couches supérieures (par exemple, suite au changement de site d'un serveur, du changement de la technologie du réseau, etc.).

C'est au travers d'autres projets qui voient le jour en parallèle, notamment en France avec le projet *Cyclades*[14] de Louis Pouzin (IRIA) en 1971, qu'est définie la première spécification du protocole de communication TCP/IP[15] (Transport Control Protocol/ Internet Protocol : DARPA, 1981) utilisé par Internet en 1974.

Comprendre cette structuration du réseau permet d'appréhender les forces et les faiblesses de celui-ci et de comprendre d'où proviennent et comment sont construites les attaques informatiques. En effet, ces attaques s'appuient la plupart du temps spécifiquement sur une ou plusieurs de ces couches définies plus haut : des techniques de l'*ARP spoofing* ou *ARP Poisoning*[16] (usurpation d'adresse ethernet) à bas niveau, ou la technique de *l'injection SQL*[17] ou attaques de type *XSS* (*cross-site scripting*[18]) à plus haut niveau.

Il est à noter que même si certains protocoles définis utilisent un mécanisme de cryptage (c'est-à-dire que les informations envoyées d'un processus à un autre sont cryptées pendant le transfert), toutes les couches ne le sont pas (*cf.* figure 2, page suivante).

On arrive donc tout de même à identifier, par une analyse du trafic réseau, un certain nombre d'informations potentiellement utiles pour une attaque, voire (plus grave) à pouvoir exploiter une faille liée au système de cryptage (comme la faille *Heartbleed*[19] détectée en 2014, concernant le protocole de cryptage *OpenSSL*[20]). Enfin, dans tous les cas, rien ne garantit que les processus émetteur et récepteur ne sont pas compromis.[21]

---

[14] *Cf.* https://interstices.info/encart.jsp?id=c_16645&encart=8&size=640,600.

[15] Specification of Internet Transmission Control Program, décembre 1974, *Cf.* http://tools.ietf.org/html/rfc675.

[16] *Cf.* http://fr.wikipedia.org/wiki/ARP_poisoning.

[17] *Cf.* http://fr.wikipedia.org/wiki/Injection_SQL.

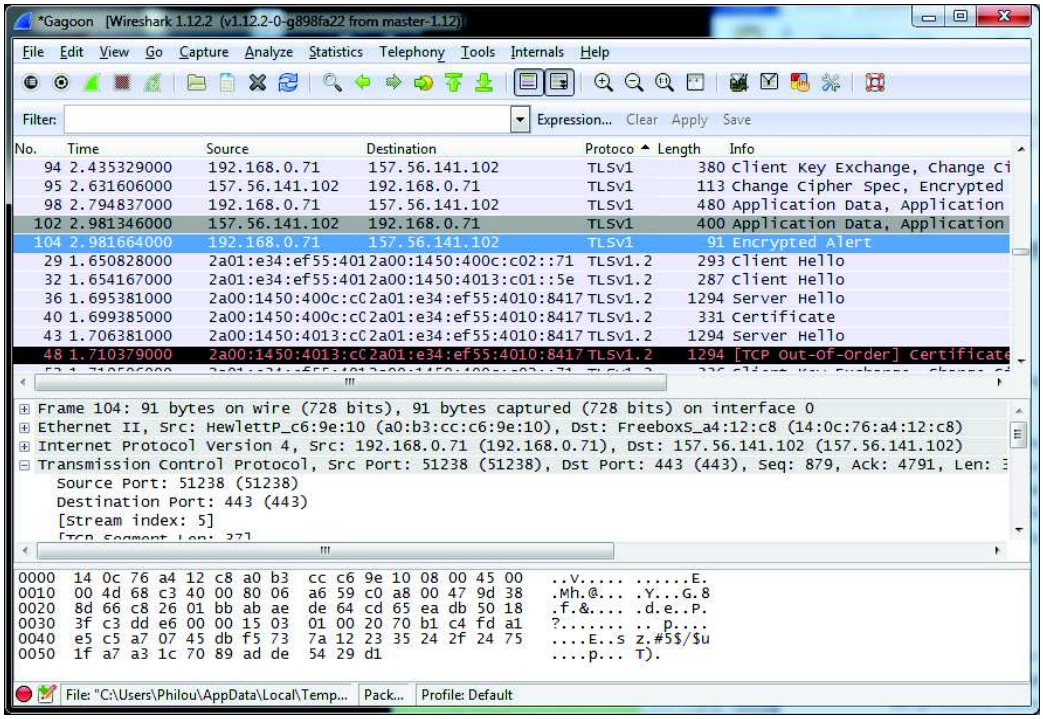
[18] *Cf.* http://fr.wikipedia.org/wiki/Cross-site_scripting.

[19] *Cf.* http://www.heartbleed.fr et http://www.01net.com/editorial/618076/tout-savoir-sur-l-enorme-faille-heartbleed-en-7-questions/.

[20] *Cf.* https://www.openssl.org/.

[21] *Cf.* http://www.undernews.fr/malwares-virus-antivirus/la-nouvelle-version-du-trojan-citadel-sen-prend-aux-gestionnaires-de-mots-de-passe-securises.html.

Figure 2 : Exemple de trafic réseau utilisant un protocole crypté. On peut repérer les adresses sources et destination, les versions des protocoles utilisés. Capture de trafic effectuée avec le logiciel *Wireshark*[22]



Les attaques informatiques reposent donc pour une part non négligeable sur des "failles" du système, que ce soit au niveau du signal transmis,[23] du matériel électronique,[24][25] du code informatique utilisé voire des protocoles eux-mêmes. Par exemple, dans le protocole FTP[26] (*File Transfer Protocol* – protocole de transfert de fichiers), les *logins* et mots de passe transitent en clair sur le réseau : quiconque a accès à l'écoute du réseau peut capturer ces informations. Malgré cela, ce protocole reste encore très répandu en 2015.

Concernant les failles réputées les plus dangereuses, on peut bien évidemment citer les failles dites "*0-day*" (ANSSI, 2013) – les vulnérabilités inconnues d'un produit et/ ou ne possédant pas de correctif – qui constituent des risques majeurs et permanents pour les systèmes d'information. Ces failles peuvent se trouver dans n'importe quel code, qu'il s'agisse d'un logiciel classique, d'une application mobile, d'un composant *Web*, d'un service en ligne ou dans un logiciel embarqué. Certains individus et groupes cherchent ces failles pour les corriger, d'autres pour les exploiter. Parmi eux, il y a bien évidemment les "pirates" – *hackers*, *crackers*, etc. (voir ci-après la section intitulée "Les acteurs") – mais également les agences de sécurité et de renseignement comme la NSA (National Security Agency : https://www.nsa.gov). On trouvera aisément, dans la littérature (Engrebretson,

---

[22] *Cf.* https://www.wireshark.org.

[23] *Cf.* http://defensesystems.com/articles/2014/08/15/drones-can-hack-wifi-networks.aspx.

[24] *Cf.* http://arstechnica.com/information-technology/2013/12/inside-the-nsas-leaked-catalog-of-surveillance-magic.

[25] *Cf.* http://www.wired.com/2012/03/pwnie.

[26] Protocole FTP, RFC 959, octobre 1985 : *cf.* https://www.ietf.org/rfc/rfc959.txt.

2013 ; Erickson, 2008 ; Northcutt, 2001) et sur des sites Internet spécialisés, la présentation d'un certain nombre de ces techniques de *hacking*: scans réseaux, craquages de mots de passe, techniques d'intrusion classiques, expliquées pas à pas. Mais le principal vecteur d'attaque repose à la fois sur un ciblage humain et technologique permettant une réduction de la complexité d'accès et d'identification de failles possibles. Cette approche n'est pas nouvelle : le cassage du code ENIGMA par l'équipe d'Alan Turing durant la Seconde Guerre mondiale a été permis grâce à la cryptanalyse bien sûr, mais encore grâce à la capture de manuels de chiffrage et la faiblesse de certaines machines (Singh, 2001, pp.185-241).

En résumé, les attaques informatiques suivent toujours le même schéma général en cinq phases :

Phase 1 : prise d'informations sur le système à attaquer. C'est dans cette phase qu'intervient le ciblage du système à attaquer. En effet, la plupart des protocoles renvoient un certain nombre d'informations intéressantes sur le système cible (*cf.* figure 3, ci-dessous). La simple analyse de trafic réseau permet de remonter des informations sur le système, les versions installées, etc., et donc permet d'identifier des vulnérabilités si les mises à jours et correctifs n'ont pas été effectués. Ceci est évidemment souvent plus complexe, et de nombreuses techniques combinées sont utilisées avec de plus en plus fréquemment un ciblage des utilisateurs du système à l'aide des réseaux sociaux. Pour mémoire, la cyberattaque de l'Elysée en mai 2012 a débuté via le réseau social *Facebook*[27] tout comme l'attaque de la chaîne *TV5 Monde* sur un envoi de mèl.[28] Autre exemple de la variabilité des attaques et de l'opportunisme des assaillants : un test de pénétration réussi a été effectué en 2011 par Netragard chez un de ses clients à l'aide d'une une souris "modifiée"[29] [30] et d'une faille *0-day*.

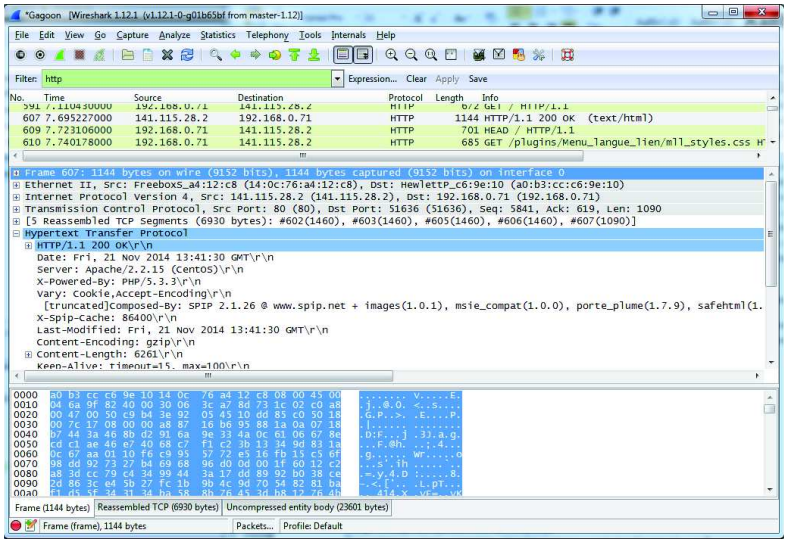


Figure 3 : Exemple de trafic réseau lors d'une réponse à une requête d'un serveur *Web* (http://www.irit.fr). On peut vérifier que le serveur *Web* est un serveur Apache version 2..2.15 et utilise une version du langage PHP 5.3.3 sous un OS CentOS ainsi que de nombreux plugins. (Capture de trafic effectuée avec le logiciel *Wireshark 1*).

[27] *Cf.* http://lexpansion.lexpress.fr/high-tech/nsa-les-americains-etaient-ils-a-l-origine-de-l-espionnage-de-l-elysee-en-2012_1340421.html.

[28] *Cf.* http://www.undernews.fr/hacking-hacktivisme/tv5-monde-spear-phishing-un-simple-mail-aura-suffit.html.

[29] *Cf.* http://www.theregister.co.uk/2011/06/27/mission_impossible_mouse_attack/.

[30] *Cf.* http://www.netragard.com/netragards-hacker-interface-device-hid.

Phase 2 : un gain d'accès. L'objectif est ensuite de s'introduire sur le système-cible, soit simplement quand le système n'est pas vraiment protégé (mots de passe d'"usine" non modifiés, ou très simples comme "*lemotdepassedeyoutube*"[31]), par cassage de mots de passe par force brute, ou encore par l'introduction de chevaux de Troie (*trojans*) ou de logiciels malveillants (*malwares*). Ces derniers sont transmis le plus souvent, par des pièces jointes dans des mèls ou via des téléchargements (exemple du *malware* introduit par le FBI via le réseau TOR[32]).

Phase 3 : une élévation de privilèges (qui inclut le plus souvent des fonctions d'administration), afin de prendre en main le système-cible. Ceci n'est possible qu'au travers de l'exploitation de failles de systèmes d'exploitation et peut se faire en local sur le système, ou à distance.

Phase 4 : un maintien de l'accès. Ce processus consiste à ouvrir des "portes dérobées" (*backdoors*) afin de revenir sur le système à n'importe quel moment. Ceci peut être utile lors d'attaques par "déni de service" ou d'envois de mèls de grande ampleur ("pourriels") nécessitant l'usage de milliers de machines zombies (on parle alors de "botnet" (Ollmann, 2009) : raccourci de robot + network). Il est à noter que certaines *backdoors* sont parfois installées par le fabricant lui-même (par exemple, sur *Samsung Galaxy*[33] ou le routeur *DLink*[34])

Enfin, une **Phase 5 : un nettoyage des traces**. Après l'attaque, il est intéressant d'effacer les traces de son passage afin d'éviter d'être identifié et, le cas échéant, de pouvoir recommencer une attaque similaire dans le futur.

Ce schéma général peut bien évidemment s'appliquer à toutes sortes d'attaques n'impliquant que des accès réseau ou impliquant un autre vecteur de pénétration tiers comme des clés USB[35] (cas du ciblage des infrastructures logicielles et matérielles pour les virus *Stuxnet*[36] en 2010 et *Flame*[37] en 2012). L'imagination des attaquants, la multiplication des matériels, logiciels, systèmes d'exploitation peuvent laisser à penser que le combat est presque perdu d'avance. Il convient donc d'analyser les pratiques de sécurité.

D'après le dernier rapport du CLUSIF (2014), intitulé *Menaces informatiques et pratiques de sécurité en France*, qui concerne les menaces pesant sur les entreprises de plus de 200 salariés, les hôpitaux publics et les particuliers, "[l]*'informatique est perçue comme stratégique par une très large majorité des entreprises* […], *77% d'entre elles jugent lourde de conséquences une indisponibilité de moins de 24 h de leurs outils informatiques (avec un maximum de 95% pour le secteur de la Banque-Assurance*" (p. 21). Du côté du nombre d'incidents d'origine malveillante dans les entreprises, les infections

---

[31] *Cf.* http://www.arretsurimages.net/breves/2015-04-11/Lemotdepassedeyoutube-TV5Monde-admet-une-bourde-id18809.

[32] *Cf.* http://www.theguardian.com/technology/2014/nov/14/government-hackers-tor-malware-attacks-onionduke-miniduke.

[33] *Cf.* http://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor.

[34] *Cf.* https://nakedsecurity.sophos.com/2013/12/03/d-link-patches-joels-backdoor-security-hole-in-its-soho-routers.

[35] *Cf.* http://blogs.mcafee.com/mcafee-labs/hooking-mac?utm_medium=spredfast&utm_source=twitter&utm_campaign=Labs#sf5821441.

[36] *Cf.* http://www.monde-diplomatique.fr/2011/03/RIVIERE/20197.

[37] *Cf.* http://www.zdnet.fr/actualites/flame-un-virus-developpe-en-israel-pour-attaquer-l-iran-39772215.htm.

dues à des virus restent en pole position (en moyenne, les entreprises connaissent 15,4 incidents de sécurité de ce type par an), suivi par les attaques logiques ciblées (10,5) et les vols (7,1). De cette étude, on peut enfin constater une évolution majeure de l'usage des systèmes informatiques vers une *externalisation des ressources informatiques utilisées* (via le *cloud* ou l'accès à des logiciels externes – réseaux sociaux, etc. – qui, pour certains, sont assez peu réputés pour le respect de la vie privée[38]) – mais aussi de *l'externalisation des matériels permettant l'accès à ces ressources* via des tablettes ou smartphones utilisant majoritairement des réseaux sans fils (*WiFi*, 3G, 4G, …). Ce sont deux nouveaux *vecteurs d'attaque* à prendre absolument en compte pour une protection maximale des données.

Les "nouvelles" menaces

L'ANSSI, dans son Guide n°650, *Menaces sur les systèmes informatiques* (2006), expose quinze menaces générales qui peuvent porter atteinte à la sécurité des systèmes d'information (p.13), dont certaines concernent plus spécifiquement l'externalisation des ressources et du matériel :

- **l'écoute ou l'interception de signaux**, rendue plus facile par l'usage de transmission sans fil, notamment via des *hotspots WiFi*, 3/ 4G, ou liaison radio ;
- **le vol du matériel**, qui devient problématique si les données ne sont pas cryptées ;
- **le piégeage de logiciel** par virus, *malware*, exploitation d'un défaut, *rootkits* (logiciel furtif permettant de pérenniser un accès à distance), *trojans* (chevaux de Troie), *RAT*[39] (*Remote Access Trojan*), facilité par le nomadisme et la multiplicité des matériels ;
- **l'utilisation illicite de matériels**, notamment grâce à des *backdoors* (trappes) ouvertes par des logiciels ou laissé intentionnellement par le constructeur matériel (exemple avec les smartphones *Galaxy* de Samsung[40] ou routeurs *DLink*[41]) ou tout simplement par la négligence des utilisateurs. On peut ainsi trouver des moteurs de recherche spécialisés dans la recherche de périphériques (ouverts) connectés à Internet comme *Shodan*[42] ou *Insecam*.[43]

En outre, ces attaques sont facilitées ces dernières années par au moins quatre autres éléments :

- **la multiplication du nombre d'objets connectés à Internet**, dont les smartphones, montres connectées, drones, ou tout autre type de capteurs faciles à dissimuler et permettant l'acquisition de données de manière cachée ;

---

[38] *Cf.* http://www.france24.com/fr/20140806-vie-privee-internautes-attaquent-facebook-justice-autriche-max-schrems.
[39] *Cf.* http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan.
[40] *Cf.* http://www.journaldugeek.com/2014/03/14/backdoor-samsung-galaxy/.
[41] *Cf.* https://nakedsecurity.sophos.com/2013/12/03/d-link-patches-joels-backdoor-security-hole-in-its-soho-routers.
[42] *Cf.* https://www.shodan.io.
[43] *Cf.* http://insecam.com.

- **l'apparition de nouveaux matériels électroniques** open-source à bas coût, comme le *Teensy*,[44] *Arduino*,[45] *Raspberry pi*,[46] *Intel Edison*,[47] etc. (*cf.* figure 5) pour les plus répandus, qui ont des capacités de stockage de plus en plus importantes, et d'émulation de clics souris, appuis clavier, etc. permettant une multiplicité d'attaques.

De plus, cette tendance de fond est largement favorisée par des sites de financement participatif (*crowdfunding*), comme *Kickstarter*[48] ou *Indiegogo*,[49] permettant de faire émerger et financer des projets personnels innovants.

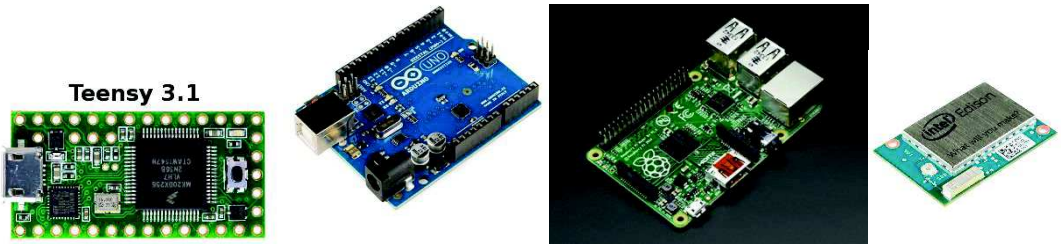


Figure 4 : Plaques *Teensy*, *Arduino*, *et Raspberry Pi* et *Intel Edison.*

- **des langages informatiques** "**simples**" multi-plateformes, accessibles à des quasi-novices (le langage *Python*,[50] par exemple), et assez puissants pour effectuer des attaques, qui bien que naïves, sont souvent suffisantes pour faire quelques dégâts ;
- **les communautés** sur Internet permettant un échange de codes, technique qui facilite les attaques. Il peut paraître étrange de trouver sans problème les codes-sources (par exemple sur des sites comme *http://sourceforge.net*, *https://github.com, http://code.google.com*,), des tutoriaux[51] ou des outils[52] permettant une attaque de systèmes d'information.

Cependant, ces communautés ont aussi un intérêt pour la lutte contre les cyber-attaques. En effet, le fait de rendre publiques les informations permet souvent de s'en prémunir. La plupart des outils présents sur ces sites servent aussi à effectuer des audits ou tests de pénétration (*pentest*). On peut ainsi trouver des distributions logicielles[53] comme *Kali-Linux*[54] ou *DEFT*,[55] offrant un certain nombre d'outils de pénétration à fins de test.

---

[44] *Cf.* https://www.pjrc.com/teensy.
[45] *Cf.* http://www.arduino.cc.
[46] *Cf.* http://www.raspberrypi.org.
[47] *Cf.* http://www.intel.fr/content/www/fr/fr/do-it-yourself/edison.html.
[48] *Cf.* https://www.kickstarter.com.
[49] *Cf.* https://www.indiegogo.com.
[50] *Cf.* https://www.python.org.
[51] *Cf.* http://www.irongeek.com/i.php?page=security/programmable-hid-usb-keystroke-dongle.
[52] Metasploit : penetration testing software. *cf.* http://www.metasploit.com.
[53] *Cf.* http://www.onemansanthology.com/blog/top-5-linux-security-distros.
[54] *Cf.* http://www.kali.org.
[55] *Cf.* http://www.deftlinux.net.

Les chercheurs de *TrendMicro* (2014) ajoutent huit prédictions pour 2015 et au-delà sur les menaces en émergence, dont le fait (déjà avéré) que les attaques se feront de plus en plus au travers des téléphones portables[56] et que, selon eux, la croissance de l'activité cyber va se traduire par la multiplicité des tentatives et outils de *hacking*.

Ce panel de menaces est complété par la publication régulière de "Preuves de Concept" (PoC – *Proof of Concept*) par des chercheurs en sécurité, qui révèlent des faiblesses de notre environnement connecté. Ces "PoC" ont montré que la prise de contrôle physique sur les automobiles,[57] drones (Reed, 2011) ou les avions,[58] la désanonymisation des échanges effectués sur le réseau TOR (Chakravarty *et al*., 2014) ou l'attaque directe de la mémoire RAM afin de récupérer des clés de chiffrement sur des systèmes informatiques éteints (Halderman, 2008) sont possibles.

Les dangers peuvent donc provenir de partout (les réseaux sont réellement inter-connectés) et de tout le monde : du simple particulier sans connaissances techniques jusqu'au spécialiste informatique capable d'élaborer des attaques de grande ampleur afin de paralyser un ou plusieurs systèmes d'information.

Les acteurs

L'ANSSI[59] définit six types d'assaillants, pour lesquels l'avidité et l'appât du gain sont les principales motivations. Il y a tout d'abord les *agresseurs*, dont on distingue deux sous-catégories :

- les *hackers*, pirates souvent par jeu ou par défi, qui ne nuisent pas intentionnellement et possèdent un "code d'honneur" et de conduite ;
- les *crackers*, plus dangereux, car ils cherchent à nuire et montrer qu'ils sont les plus forts.

Il y a ensuite les *fraudeurs* qui bénéficient souvent d'une complicité, volontaire ou non, de leurs victimes. Parfois liés au grand banditisme, organisés ou non, ils peuvent attaquer une banque, falsifier des cartes de crédit ou se placer sur des réseaux de transferts de fonds. On trouve aussi parmi les fraudeurs les *employés malveillants*[60] (fraudeurs internes). Ils possèdent de bonnes compétences sur le plan technique, ils sont souvent informaticiens et sans antécédents judiciaires. Ils veulent se venger de leur employeur et cherchent à lui nuire en lui faisant perdre de l'argent.

---

[56] *Cf.* http://www.vice.com/fr/video/phreaked-out-les-mille-et-une-facons-de-hacker-un-telephone-412.

[57] Black Hat 2014 : un pirate peut-il prendre le contrôle à distance d'une voiture ? *Cf.* http://www.01net.com/editorial/624860/black-hat-2014-un-pirate-peut-il-prendre-le-controle-a-distance-d-une-voiture/.

[58] Hacking planes – UK researchers developing plans to stop "flight cyberjacking". *Cf.* http://www.theguardian.com/technology/2014/nov/04/hacking-planes-uk-researchers-developing-plans-to-stop-flight-cyberjacking/print.

[59] *Cf.* http://www.ssi.gouv.fr/IMG/pdf/Guide650-2006-09-12.pdf.

[60] *Cf.* http://www.lapresse.ca/actualites/justice-et-affaires-criminelles/affaires-criminelles/201411/27/01-4823001-la-cybercriminalite-augmente-mais-sa-detection-diminue.php.

Il y a ensuite les *militants* (ou "*hacktivistes*"[61]) qui sont motivés par une idéologie et qui disposent de compétences techniques très variables. Leurs objectifs peuvent être limités à la diffusion massive de messages ou s'étendre à des nuisances effectives des organismes en opposition avec leur idéologie. Il y a encore les *espions* qui participent à la guerre économique. Ils travaillent pour un État ou pour un concurrent. Ils savent garder le secret de leur réussite pour ne pas éveiller les soupçons et continuer leur travail dans l'ombre. Ils ont pour but de voler des informations ou de détruire des données stratégiques (vitales) pour l'organisme. Il y a enfin les "*cyberterroristes*", aidés dans leur tâche par l'interconnexion et l'ouverture croissante des réseaux : très motivés, ils veulent faire peur et faire parler d'eux. Les actions se veulent spectaculaires, influentes, destructrices, meurtrières.

On pourrait ajouter à cette liste un septième type d'assaillant : les *États* et *agences gouvernementales*, qui prennent une part de plus en plus importante dans des attaques ciblées, comme ce fut le cas des virus *StuxNet* et *Flame*, lancés afin de ralentir la montée en puissance nucléaire de l'Iran. On peut aussi citer plus récemment l'infection des utilisateurs du réseau TOR[62] par le FBI[63] permettant de tracer les utilisateurs de ce réseau anonyme, ou l'usage de l'outil d'espionnage *FinSpy*[64] de la société *Gamma*,[65] dont on soupçonne qu'elle l'a vendu à des États autoritaires comme le Bahrein.[66] Enfin, il y a aussi la "découverte" récente de *Regin*,[67] [68] logiciel furtif de collecte de données pour lequel les États-Unis et la Grande-Bretagne sont pointés du doigt. Les États font de plus en plus appel à des sociétés spécialisées.[69] [70] [71] Néanmoins, certaines de ces sociétés (parfois considérées comme "*mercenaires*") peuvent aussi se retrouver dans le viseur de ces États.[72]

Toutefois, comme le montrent certains rapports du CERT-CC (Milletary, 2005 ; Householder, 2002) ou du NRI (2013), bien que la sophistication des attaques augmente, la compétence technique globale des attaquants tend à diminuer. On peut expliquer ce phénomène par un accès plus aisé à la technologie, comme vu précédemment, mais aussi par le fait que les équipements informatiques sont extrêmement nombreux et utilisés par un nombre croissant d'utilisateurs.

---

[61] Parmi ces hacktivistes, on trouve les *Anonymous* par exemple : http://wearelegionthedocumentary.com.

[62] *Cf.* https://www.torproject.org.

[63] Le FBI infecte les utilisateurs de TOR avec un malware : http://www.gizmodo.fr/2014/08/07/fbi-infecte-tor-malware.html.

[64] *Cf.* https://wikileaks.org/spyfiles4.

[65] *Cf.* https://www.gammagroup.com.

[66] *Cf.* http://www.numerama.com/magazine/23586-finspy-le-spyware-britannique-vendu-a-des-regimes-autoritaires.html.

[67] *Cf.* https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq.

[68] *Cf.* http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/regin-le-graal-de-l-espionnage-va-t-il-changer-le-monde-27-11-2014-1884818_506.php.

[69] Quarkslab, *cf.* http://www.quarkslab.com.

[70] iTrust, *cf.* https://www.itrust.fr.

[71] Vupen Security, *cf.* http://www.vupen.com.

[72] "Les mercenaires de la cyberguerre", *L'Expansion*, 22 novembre 2014 : http://lexpansion.lexpress.fr/high-tech/les-mercenaires-de-la-cyberguerre_1623549.html.

Les ripostes

Il est difficile d'exposer les "ripostes" ou les contre-mesures contre des attaques informatiques tant les réponses sont nombreuses et variées. Quelques initiatives, comme la formalisation d'un format d'échanges de messages pour la détection et l'intrusion,[73] ont vu le jour à l'initiative de l'*IETF* (*Internet Engineering Task Force*). Certains réclament l'usage généralisé de la technique du *DPI – Deep Packet Inspection* (Kumar, 2006 ; Becchi, 2007) – qui, bien que très controversé, notamment durant la révolution tunisienne de 2011 (Mihoub, 2011),[74] permet l'inspection et le filtrage de paquets échangés sur Internet.

Le réseau étant par essence ouvert et multiforme, il s'avère que les ripostes ne peuvent être universelles, mais adaptées au contexte technique et humain, et doivent donc nécessairement reposer sur l'analyse du terrain. La première chose à faire pour se protéger est d'identifier les faiblesses possibles de son système d'information et de son environnement. Dans ce cadre, la norme ISO 15408 définit des critères d'évaluation internationaux de la sécurité des systèmes d'information à usage général.[75] Ces critères permettent l'évaluation des fonctions de sécurité au travers de onze classes fonctionnelles et d'exigence de garantie. Ce référentiel permet de s'assurer que les fonctions de sécurité sont efficaces et correctement mises en œuvre et que tous les mécanismes de sécurité critiques ont été testés pour établir leur capacité à résister aux attaques directes et indirectes.

S'informer, se former et échanger

Il existe depuis longtemps des organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT (*Computer Emergency Response Teams*), créés en 1988 après la propagation d'un "ver Internet",[76] sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises ou aux administrations. En France, ce service est assuré aux administrations par le CERT-FR[77] (l'ancien CERTA, créé en 1999). Ce centre publie chaque semaine des bulletins d'actualité relatifs aux vulnérabilités détectées sur des systèmes d'exploitation, logiciels ou protocoles, et aux moyens de s'en prémunir le cas échéant.

L'usage de forums et sites spécialisés comme le FIRST[78] (*Forum of Incidence Response and Security Teams*) est aussi un moyen efficace et intéressant de faire de la veille technologique. D'autres sources d'information sont proposées par le CLUSIF[79] (Club de la Sécurité de l'Information Français) sur leur site *Web* ou plus récemment par le CECyF

---

[73] *Cf.* http://www.ietf.org/rfc/rfc4765.txt.
[74] *Cf.* http://nawaat.org/portail/tag/dpi.
[75] *Cf.* http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341.
[76] *Cf.* http://www.cert.ssi.gouv.fr/cert-fr/cert.html.
[77] *Cf.* http://www.cert.ssi.gouv.fr.
[78] *Cf.* http://www.first.org.
[79] *Cf.* https://www.clusif.asso.fr.

(Centre Expert contre la Cybercriminalité Français[80]). De nombreux sites d'actualité autour de la "sécurité" ou simplement "techniques", maintenus par des entreprises, comme *Nakedsecurity*,[81] *Wired*,[82] *TechCrunch*,[83] ou personnel (comme c'est le cas d'*Undernews*[84]) complètent le panel. Enfin, on peut signaler la récente initiative de *Google* avec son "*Project Zero*",[85] dont l'ambition est d'améliorer la sécurité d'Internet en identifiant des failles "*0-day*". De nombreux outils sont aussi développés afin de "loguer",[86] analyser et visualiser les attaques et permettre une compréhension plus fine des phénomènes. Parmi les plus connus, citons *Wireshark*,[87] visualiseur de trames réseaux reposant sur la librairie *Libpcap/ WinPcap*,[88] *XArp*,[89] détecteur d'attaques au niveau du protocole de bas-niveau ARP ou *zAnti*[90] de la société *Zimperium*, application mobile de détection et de pénétration. D'autres types d'outils ont émergé ces dernières années et concernent la visualisation de grandes quantités de données comme par exemple l'outil *Norse*[91] qui montre en temps réel les attaques DDoS au niveau mondial, ou *Logstagia*,[92] visualiseur de requêtes sur un serveur *Apache* (cf. figures 5 et 6, ci-après).

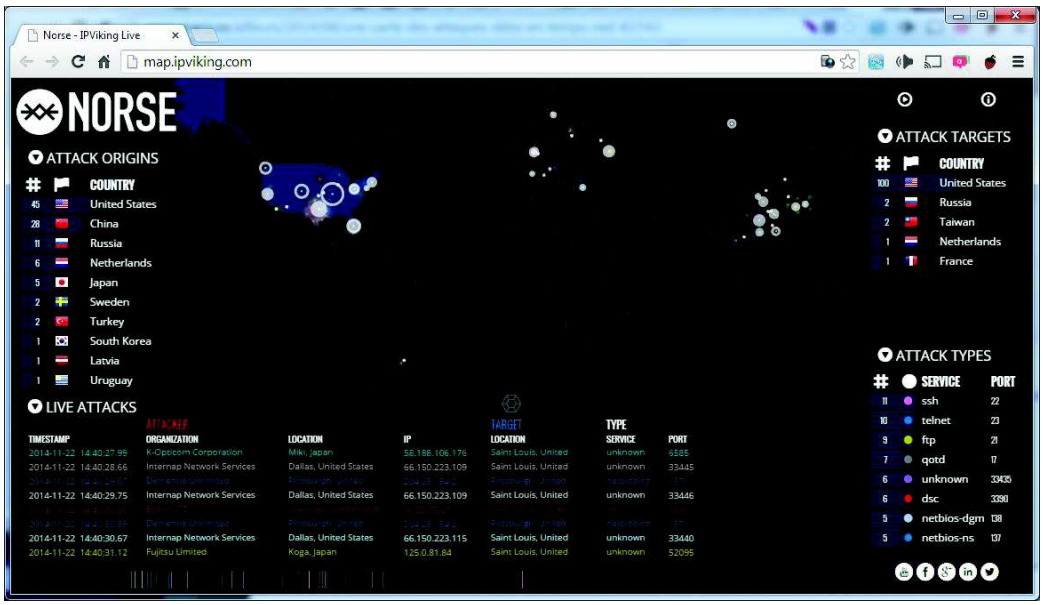
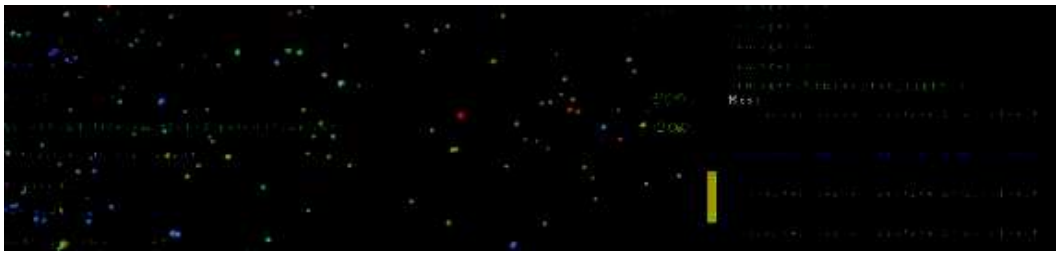


Figure 5 : Capture d'écran de l'outil *Norse* (http://map.ipviking.com)

---

[80] *Cf.* http://www.cecyf.fr.
[81] *Cf.* https://nakedsecurity.sophos.com.
[82] *Cf.* http://www.wired.com.
[83] *Cf.* http://techcrunch.com/.
[84] *Cf.* http://www.undernews.fr.
[85] *Cf.* http://googleprojectzero.blogspot.fr.
[86] *Cf.* https://www.prelude-ids.org.
[87] *Cf.* https://www.wireshark.org.
[88] *Cf.* http://www.winpcap.org.
[89] *Cf.* http://www.xarp.net.
[90] *Cf.* https://www.zimperium.com/zanti-mobile-penetration-testing.
[91] *Cf.* http://map.ipviking.com.
[92] *Cf.* https://code.google.com/p/logstalgia.

Figure 6 : capture d'écran de l'outil Logstalgia (https://code.google.com/p/logstalgia)



Ces outils de visualisation de grandes masses de données sont intéressants à plus d'un titre : ils permettent de comprendre et d'identifier des phénomènes de plus en plus complexes, voire quasiment invisibles. De nombreux travaux de recherche (par exemple, Hurter, 2010) en interaction homme-machine sont d'ailleurs menés autour de cette thématique dite d'*InfoVis*[93] pour appréhender et comprendre ces phénomènes.

Enfin, de nombreuses conférences (ou *workshops*) sont organisées chaque année, comme les conférences américaines *BlackHat*[94] et *DEFCON*,[95] ou la conférence *FIC*[96] en France, qui proposent outre la présentation de travaux récents, des cours (*tutorials*) ou concours de pénétration de systèmes informatiques (*pentests*) comme la compétition organisée par la société Hewlett-Packard, *Pwn20wn*.[97]

La *veille technologique* reste donc un élément essentiel de la riposte face aux dernières avancées technologiques souvent prélude à de nouveaux types d'attaque.

Tester et (se) former

Enfin, le deuxième volet de la riposte concerne les tests de sécurité informatique. Identifier les failles, effectuer des audits ou essayer d'attaquer son propre système informatique (et donc développer et tester ses applications) sont des tâches absolument nécessaires. Là encore, de nombreux outils sont disponibles : les *outils d'audit* en ligne ou téléchargeables, comme *Detekt*,[98] qui permettent de scanner son ordinateur à la recherche de *spyware*. Des *outils de rétro-ingénierie* (*reverse engineering*) – désassembleurs, décompilateurs, débogueurs – permettent d'analyser des programmes afin d'en déterminer le fonctionnement et détecter des failles inhérentes au code informatique en lui-même.

Des *outils de pénétration* peuvent être déployés sur des distributions (dites de *pentesting*) comme *Kali-Linux*[99] ou *DEFT*.[100] Enfin, des *librairies informatiques* (comme la librairie *Scapy*[101] pour le langage *Python*) permettent l'analyse et le test d'intrusion.

---

[93] Conférences IEEE Vis : *cf.* http://ieeevis.org.
[94] *Cf.* http://www.blackhat.com/us-14/.
[95] *Cf.* https://www.defcon.org.
[96] *Cf.* http://www.forum-fic.com.
[97] *Cf.* http://www.pwn2own.com.
[98] *Cf.* https://resistsurveillance.org.
[99] *Cf.* http://www.kali.org.
[100] *Cf.* http://www.deftlinux.net.
[101] *Cf.* http://www.secdev.org/projects/scapy.

Cependant, comme le rappellent quelques chercheurs, le "*principal danger pour l'ordinateur se situe entre l'écran et le fauteuil*" : il est à chercher du côté du facteur humain. Sans être caricatural, l'utilisateur est souvent un composant essentiel de la réussite des attaques informatiques. Il n'est pas rare que la presse révèle certaines anecdotes cocasses à ce sujet[102] (*cf.* figure 7).

Figure 7 : Reportage de la CBS autour la sécurité du Super Bowl avec les *logins/ passwords* de l'accès *WiFi* affichés en clair. Source : ZDNet, http://www.zdnet.com/super-bowl-wi-fi-password-credentials-broadcast-in-pre-game-security-gaffe-7000025865.

C'est un point important à souligner : la formation des publics, du simple particulier au professionnel, est primordiale en ce qui concerne la sécurité informatique. Comprendre les enjeux de la sécurité, comprendre les modes de fonctionnement, permet de rester vigilant afin de garantir la sécurité la plus globale possible ! En effet, une trop grande confiance reste trop souvent le point de départ du piratage (Truillet, 2013). Le point primordial est d'être en capacité de déterminer ce qu'il faut protéger, et contre qui. Les attaques semblent inévitables. Il faut être capable d'identifier quelques scénarii d'attaques réalistes au vu de ses propres vulnérabilités, et par conséquent mettre en place des parades nécessaires (parfois simples) à la protection de ses informations.

Conclusion

Comme on vient de le voir, Internet et les réseaux en général fournissent un "*nouveau terrain de jeu*" pour les États, activistes, pirates et malfrats, etc. La professionnalisation criminelle est facilitée par l'"outil", qui facilite en retour l'opportunisme. Ces dernières années ont vu une explosion technologique des moyens informatiques disponibles.

---

[102] "Super Bowl Wi-Fi password credentials broadcast in pre-game security gaffe", ZDNet, 2 février 2014 : http://www.zdnet.com/super-bowl-wi-fi-password-credentials-broadcast-in-pre-game-security-gaffe-7000025865.

On le constate tous les jours, le domaine de la sécurité informatique est en pleine ébullition : les particuliers, les entreprises et les États ont pris conscience que l'informatique est devenue hautement stratégique pour nos sociétés. Malheureusement, si une majorité de personnes savent se servir plus ou moins bien de l'outil numérique (traitement de texte, tableurs, etc.), peu en comprennent – par manque de formation – le fonctionnement.

Longtemps réservé à quelques spécialistes, ce domaine doit être pris en main par l'ensemble de la société : initier, former, éduquer à l'informatique et à la programmation dès le plus âge (toutes choses appelées de ses vœux par la Société Informatique de France[103] afin de promouvoir une véritable culture informatique dans notre pays) permettrait de diminuer les risques. Certains pays (nordiques et anglo-saxons) ont déjà amorcé cette "révolution" : il ne tient qu'à la volonté publique d'effectuer ce tournant.

Au vu de la complexité du phénomène "cyber", il est urgent de décloisonner les disciplines : un informaticien ne peut plus ignorer les textes de loi régissant l'usage des réseaux et les sanctions auxquelles il s'expose, pas plus qu'un juriste ne peut désormais ignorer le mode de fonctionnement "basique" des systèmes informatiques. Les systèmes d'information, et Internet en particulier, ouvrent de nouveaux champs de réflexion : abolition des frontières, inadaptation parfois des lois et décrets, etc. On ne peut répondre au défi ainsi posé que s'il est vu dans sa *globalité* technique et juridique, et non traité séparément par chacun des domaines concernés. Ceci passe, c'est du moins l'avis de l'auteur de ces lignes, par la formation d'équipes pluri- ou transdisciplinaires comme on peut en trouver dans les milieux de la recherche : chacun étant spécialiste de son domaine tout en étant capable de discuter et comprendre le point de vue de son collègue.

Bibliographie

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), *Menaces sur les systèmes informatiques*, guide n°650, 2006 : http://www.ssi.gouv.fr/img/pdf/guide650-2006-09-12.pdf.

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), *Vulnerabilities 0-Day : Prévention et bonnes pratiques* (http://www.ssi.gouv.fr/img/pdf/guide_vulnerabilites_0day.pdf), version 1.1, novembre 2013.

Becchi, M. & P. **Crowley**, "A hybrid automaton for practical deep packet inspection", *Proceedings of the 2007 ACM CoNEXT Conference*, article n°1: http://dl.acm.org/citation.cfm?id=1364656, 2007.

Chakravarty S., M. **Barbera**, G. **Portokalidis**, M. **Polychronakis** & A. **Keromytis**, "On the effectiveness of traffic analysis against anonymity networks using flow records, passive and active mesurement", *Springer Lecture Notes in Computer Science*, vol.8362, 2014, pp.247-257 : https://mice.cs.columbia.edu/gettechreport.php?techreportid=1545&format=pdf.

Clusif, (Club de Sécurité de l'Information Français), "Menaces informatiques et pratiques de sécurité en France", édition 2014 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/clusif-rapport-2014.pdf.

Darpa, "Transmission Control Protocol – Darpa Internet Program – Protocol Specification", septembre 1981 : https://www.ietf.org/rfc/rfc793.txt.

---

[103] *Cf.* http://www.societe-informatique-de-france.fr/wp-content/uploads/2014/11/Communique_SIF_7_11_2014.pdf.

ENGEBRETSON, P., *Les bases du hacking*, Montreuil, Pearson France, 2013.

ERICKSON, J., *Techniques de hacking*, Montreuil, Pearson France, 2008, 2e édition 2012.

HALDERMAN, J.A., S. **SCHOEN**, N. **HENINGER**, W. **CLARKSON**, W. **PAUL**, J. **CALANDRINO**, A. **FELDMAN**, J. **APPELBAUM** & E. **FELTEN**, "Lest We Remember : Cold Boot Attacks on Encryption Keys", Proceedings of the Usenix Security Symposium, 2008 : https://citp.princeton.edu/research/memory.

HOUSEHOLDER, A., K. **HOULE** & C. **DOUGHERTY**, "Computer Attack Trends Challenge Internet Security", Supplément au numéro d'avril 2002 (vol.35, Issue 4) de *Computer Magazine*, pp.5-7 : http://doi.ieeecomputersociety.org/10.1109/mc.2002.10028.

HURTER, Ch., *Caractérisation de visualisations et exploration interactive de grandes quantités de données multidimensionnelles*. Thèse de l'université de Toulouse-III, 2010 : https://tel.archives-ouvertes.fr/tel-00610623/document.

IETF, "Specification of Internet Transmission Control Program", 1974: http://tools.ietf.org/html/rfc675.

IETF, "The Intrusion Detection Message Exchange Format", 2007: http://www.ietf.org/rfc/rfc4765.txt.

KUMAR, S., S. **DHARMAPURIKAT**, F. **YU**, P. **CROWLEY** & J. **TURNER**, "Algorithms to Accelerate Multiple Regular Expressions Matching for Deep Packet Inspection", *Sigcomm '06 Conference Proceedings*, 2006, pp.239-250 : http://dl.acm.org/citation.cfm?id=1159952.

MIHOUB, S., "Le cyberactivisme à l'heure de la révolution tunisienne", *Arch. Antrop. Mediterraneo*, 2011 : https://hal.archives-ouvertes.fr/file/index/docid/678440/filename/cyberactivisme.smihoub.publia_.pdf.

MILLETARY, Jason, "Technical Trends in Phishing Attacks", US-CERT, 2005 : https://www.us-cert.gov/sites/default/files/publications/phishing_trends0511.pdf.

NORTHCUTT, S., J. **NOVAK** & D. **MCLACHLAN**, *Détection des intrusions réseaux*, Paris, Campus Press, 2001.

NRI SECURE TECHNOLOGIES, "Cyber Security Trends – Annual Review 2013" : http://www.nri-secure.co.jp/news/2013/pdf/cyber_security_trend_report_en.pdf.

NSA, "Untangling the Web", mai 2013 : http://stephenslighthouse.com/2013/05/13/nsa-nsa-untangling-the-web-a-guide-to-internet-research.

OLLMANN, G., "Botnet Communication Topologies – Understanding the Intricacies of Botnet Command-and-Control" (https://www.damballa.com/downloads/r_pubs/wp_botnet_communications_primer.pdf), 2009.

REED, TH., J. **GEIS** & S. **DIETRICH**, "SkyNET : A 3G-enabled Mobile Attack Drone and Stealth Botmaster", WOOT 2011, 5th Usenix Worshop on Offensive Technologies, San-Francisco, 2011.

SINGH, S., *Histoire des codes secrets, de l'Égypte des pharaons à l'ordinateur quantique*, Paris, J.C. Lattès, 2001.

TANENBAUM, A. & D. **WETHERALL**, *Réseaux*, 5e édition, Montreuil, Pearson-France, 2011.

TREND MICRO, "The Invisible Becomes Visible : Trend Micro Security Predictions for 2015 and Beyond", Trend Micro Report, 2014 : http://www.trendmicro.com/vinfo/us/security/predictions.

TRUILLET, Ph., "La confiance, moteur du piratage", in ForumEco, édition spéciale sur "Intelligence économique, réputation, influence : un réflexe", pp.36-37, juin 2013.

VORI, R.S., "Understanding IBM's System Network Architecture, or 'Through a Glass Darkly'" – A Tutorial", janvier 2003 : http://www.openmpe.com/cslproceed/HPIX88/2045v3.pdf.