Cyber-conflits, quelques clés de compréhension

Philippe WOLF, *chargé de mission auprès du Directeur Général*
et Luc VALLÉE, *ingénieur au Centre opérationnel en Sécurité des Systèmes d'Information* (COSSI),
Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)

L'objectif de cet article est de fournir quelques clés de compréhension des cyber-conflits [1] en replaçant la lutte contre la cybercriminalité dans un contexte plus large. Pour mesurer l'ampleur de cette forme de criminalité relativement jeune [2], l'étude de quelques cas réels observés est instructive. Ces incidents, dont certains font l'objet d'enquêtes criminelles confiées aux services spécialisés, sont blanchis, si nécessaire, pour servir d'archétypes à des modes opératoires en perpétuelle mutation. Ceci illustre déjà la difficulté particulière de la quantification en matière de cybercriminalité et de l'établissement de statistiques fiables. Pour élargir l'interprétation, des définitions précisent les concepts principaux en essayant de dégager quelques caractéristiques propres au cyberespace. Les difficultés singulières de traitement liées à des ambiguïtés propres à l'espace numérique sont soulignées à travers quatre situations qui ont été fortement médiatisées. Cette partie fait appel à des considérations plus techniques [3]. La lutte contre la cybercriminalité s'inscrit dans une politique globale de défense et de sécurité des systèmes d'information. Pour la décrire, les missions principales de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), service à compétence nationale rattaché au Secrétariat général de la défense et de la sécurité nationale, sont présentées dans le cadre rénové de la cyber-stratégie nationale.

L'étude de quelques cas réels observés est instructive

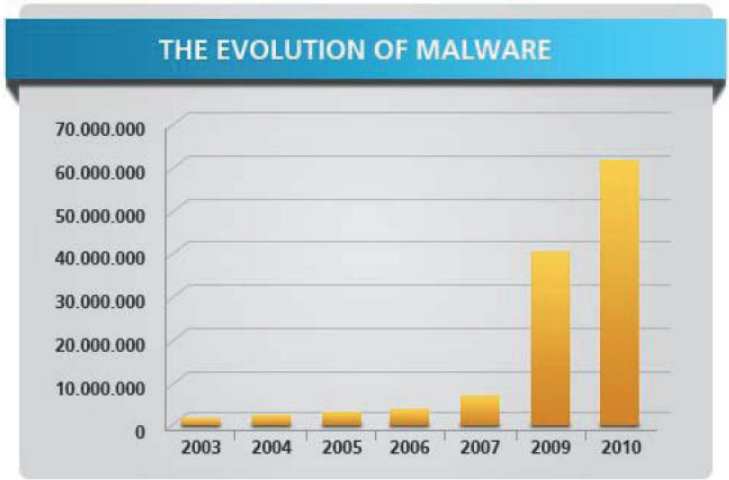
Beaucoup de travaux essaient de quantifier la progression constatée des cyber-conflits.

Un premier comptage concerne soit la **prolifération des outils malveillants** (les armes du cyber-attaquant) soit l'augmentation des failles [4] exploitables. Ainsi, un rapport récent [5] parmi d'autres, dénombre, en 2010, 60 millions de logiciels ou codes malveillants [6] en circulation, pour seulement 92 000 en 2005 (*voir figure* 1). La moitié de ces codes auraient été développés durant la dernière année. Cette progression, qui suit une loi exponentielle croissante, devra bien s'infléchir, mais cela ne semble pas devoir être encore le cas pour les prochaines années. Il s'agit là de chiffres dont l'objectif est parfois de faire peur pour stimuler le marché des produits de sécurité d'autant plus qu'ils proviennent d'une entreprise qui fournit des services de sécurité informatique. La possibilité de créer facilement des variantes à partir de certains codes malveillants, c'est-à-dire, pour l'attaquant, de les personnaliser, biaise ce dénombrement. Le CERTA [7] a diffusé 395 avis de vulnérabilité sur le premier semestre 2011, dont seulement 4 alertes. Là aussi, il faut bien distinguer la portée d'une vulnérabilité, qui n'est pas la même quand elle touche 90 % des machines individuelles ou un logiciel de niche.

Un deuxième comptage, beaucoup plus délicat, concerne les **attaques elles-mêmes** [8]. La victime, surtout quand cela touche son image, a des réticences compréhensibles à les déclarer. Il faudrait aussi distinguer les tentatives qui ont réussies ou ont été détectées, de celles, plus « professionnelles », si discrètes qu'elles passent inaperçues, d'où l'importance de l'amélioration permanente des fonctions de détection. Le plus intéressant réside dans les évolutions des proportions des différentes catégories recensées [9] (*voir figure* 2).

• • • (1) Terme générique employé ici pour caractériser tout type d'attaque dans le cyberespace.
(2) On situe souvent le premier cyber-incident en 1978 où Kevin Mitnick, figure historique du « hacking », pirate son premier réseau. La première propagation d'un ver informatique sur l'internet est l'œuvre de Robert T. Morris Jr. en 1988.
(3) Philippe WOLF, « Ambiguïtés et cyber-conflits », Colloque IMODEV « Cybercriminalité, cybermenaces et cyberfraudes », Paris, 20 et 21 juin 2011.
(4) Faille : vulnérabilité dans un système informatique permettant à un attaquant de porter atteinte à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.
(5) "The Cyber-Crime Black-Market: Uncovered", http://press.pandasecurity.com/press-room/reports/
(6) Un logiciel ou code malveillant (en anglais, malware) est un logiciel développé dans le but de nuire à un système informatique. Les virus et les vers sont les deux exemples de logiciels malveillants les plus connus, mais il en existe beaucoup d'autres.
(7) Centre d'expertise gouvernementale de réponse et de traitement des attaques informatiques (au sein de l'ANSSI), http://www.certa.ssi.gouv.fr/
(8) "Security threat report 2011", http://www.sophos.com/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreport2011wpna.pdf
(9) "2010/2011 Computer Crime and Security Survey", http://analytics.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html

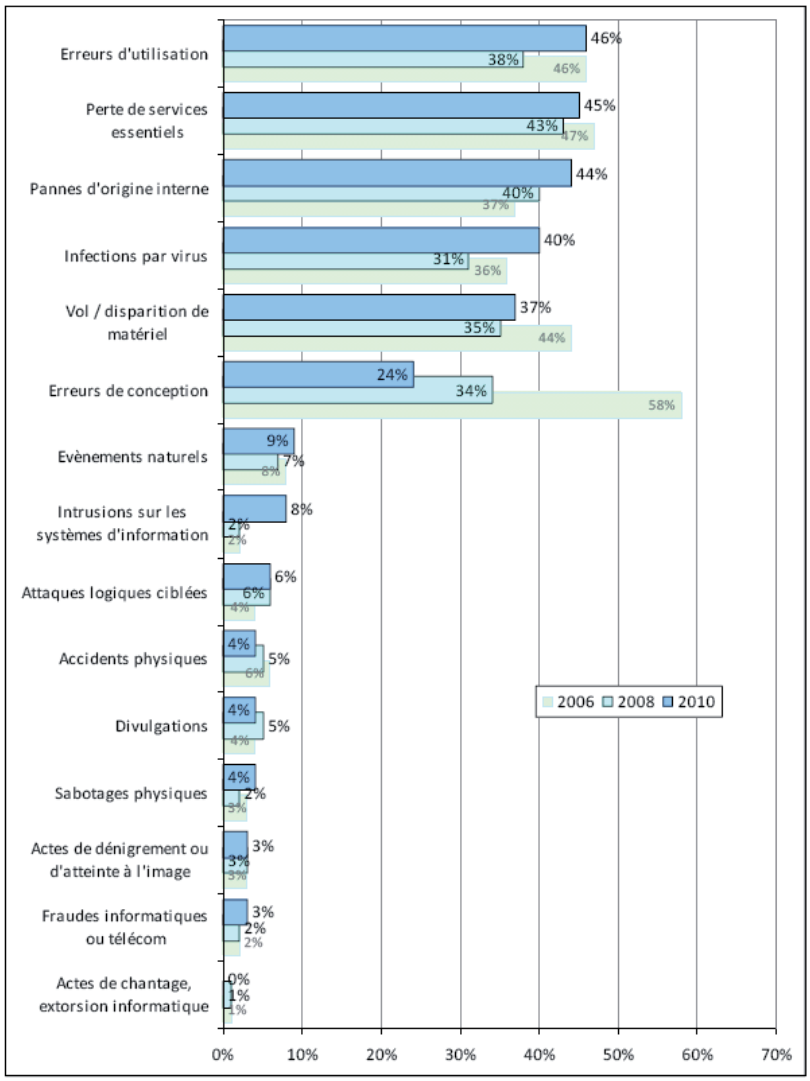
Figure 1. Évolution du nombre de codes malveillants.



Source : "The Cyber-Crime Black-Market: Uncovered", Panda Security Press

Figure 2. Typologie des incidents de sécurité.

Au cours de l'année passée, à quel type d'incidents de sécurité votre entreprise a-t-elle été soumise ?



Source : « Menaces informatiques et pratiques de sécurité en France », CLUSIF

Une analyse qualitative de quelques cas réels (*voir ci-après*) montre la difficulté de l'établissement de métriques partagées. Une approche globale, qui essaie de caractériser les chemins d'attaques empruntés par l'agresseur et les probables erreurs commises par le défenseur, est aujourd'hui privilégiée par les enquêtes menées par des organismes professionnels [10]. La qualité de l'investigation dépend aussi fortement d'un certain nombre de bonnes conduites qui sont rappelées ici.

Filoutage contre les usagers de l'administration

L'administration électronique est une nouvelle cible pour les escrocs. Des campagnes successives de filoutage [11] ont cherché à tromper les usagers de la télédéclaration et du télépaiement des impôts. Ces campagnes influent défavorablement sur l'administration électronique. Les filoutages contre les usagers français concernaient jusqu'alors les banques, puis les fournisseurs d'accès à l'Internet. En 2008, un seul cas de filoutage contre le Trésor public avait été signalé à l'ANSSI. Les fraudeurs incitaient l'usager naïf à demander un remboursement d'impôt sur le site contrefait. L'automne 2009 a vu un déferlement de vagues de filoutage. Elles se succèdent sans relâche en 2010 et 2011. Les premiers courriels étaient rédigés en français approximatif. Les progrès dans la rédaction sont constants. Le scénario part d'un courriel en HTML (format de données des pages web) utilisant une fausse adresse du ministère, avec une Marianne en en-tête. Ce courriel indique à sa victime que le fisc lui rembourse presque 200 euros (le montant augmente régulièrement) et qu'elle doit faire vite. Le prétendu formulaire est accessible par un lien hypertexte dont l'adresse réelle est masquée.

Ces courriels rassemblent des ingrédients de l'ingénierie sociale, que l'on retrouve dans les canulars (*hoaxes*) : apparences de références sérieuses (Marianne, organisme, signature numérisée), élément affectif (argent), urgence prétendue. Le site vers lequel pointe le lien demande à la victime les références et le code de sa carte bancaire. La charte graphique du portail des impôts est d'autant mieux imitée que les éléments graphiques sont directement pris sur ce dernier.

L'action technique contre ces pourriels [12] est difficile. Les serveurs d'émission ou de relais de ces messages sont souvent des machines compromises, des ordinateurs appartenant à des *botnets* [13], situés partout à travers le monde. La multiplicité des adresses IP de ces ordinateurs rend inefficace la tentative de gérer une liste noire d'adresses d'émission de courriels à proscrire en entrée des réseaux. Seuls les liens dans les courriels peuvent donner un indice, au risque de rejeter des courriels légitimes. La vigilance de l'utilisateur reste la meilleure arme.

La lutte passe par la fermeture la plus rapide possible des sites de filoutage, mais ces derniers sont généralement situés à l'étranger. Celle-ci doit s'accompagner de la préservation des indices, de manière à ce que les enquêteurs des services spécialisés puissent remonter aux commanditaires de ces attaques.

Que faut-il compter ici ? Si l'on s'intéresse aux victimes directes de l'escroquerie potentielle, les échelles de grandeurs sont très différentes entre : le nombre de courriels émis (difficile à déterminer tant que le *botnet* n'est pas démantelé) ; le nombre limité aux adresses de contribuables seulement (mais qui ne signalent pas systématiquement) ; le nombre d'adresses différentes ; aux contribuables différents, chacun pouvant être destinataire sur plusieurs adresses ; les contribuables qui sont tombés dans le piège ; ceux qui de plus en ont fait part aux services compétents ; le nombre de vagues, chacune comptée globalement, pourvu qu'on sache les distinguer... Il existe également des victimes indirectes : les courriels frauduleux vers toutes les adresses électroniques, valides ou invalides, encombrent inutilement les réseaux et les systèmes de messagerie ; les ordinateurs à partir desquels les courriels sont émis sont infectés, donc leurs possesseurs sont victimes d'intrusions dans un système de traitement automatique des données ; le faux site des impôts est lui-même un parasite sur un site légitime, donc victime supplémentaire d'une intrusion ; l'administration est victime, à chaque vague, au moins de la contrefaçon des éléments graphiques de son portail et d'une atteinte à son image.

Attaques en déni de service distribué contre une administration

Le service informatique d'une administration a d'abord identifié et bloqué quelques adresses qui envoyaient de très nombreuses requêtes sur un serveur web. Cette action ayant été insuffisante, l'ANSSI a été appelée à la

(10) « Menaces informatiques et pratiques de sécurité en France, Club de la Sécurité de l'Information Français, Édition 2010 », http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2010.pdf

(11) Le filoutage, ou phishing, est une technique utilisée par des personnes malveillantes dans le but d'obtenir des informations confidentielles sur leurs victimes puis de s'en servir. Pour ce faire les fraudeurs contactent leurs victimes sous différents prétextes en usurpant l'identité d'un tiers dans lequel la victime pourrait avoir confiance (une banque, un site de commerce...), http://www.securite-informatique.gouv.fr/gp_article44.html

(12) Un pourriel est un courriel non sollicité par son destinataire et source d'une gêne manifeste, http://www.securite-informatique.gouv.fr/gp_article99.html

(13) Réseaux de machines zombies (botnet) : un botnet, contraction de robot et network, est un réseau de machines compromises à la disposition d'un individu malveillant (le maître). Ce réseau est structuré de façon à permettre à son propriétaire de transmettre des ordres à tout ou partie des machines du botnet et de les actionner à sa guise.

rescousse. L'analyse des journaux de connexion a mis en évidence la multiplicité des adresses et a permis de les cartographier. L'attaque était menée depuis un *botnet* réparti sur les cinq continents. Si un seul serveur web était visé, tous les services informatiques partageant la même connexion réseau étaient touchés : les autres serveurs web et la messagerie en particulier. Le CERTA a pu contacter le fournisseur d'accès dont il connaissait la capacité à remédier à certaines attaques de ce type. Il a permis l'établissement d'une relation juridique et technique pour revenir à une situation plus saine : le blocage de tout le trafic web dans un premier temps, pour remettre en état les autres services Internet. Ensuite, l'analyse des journaux ayant montré que l'essentiel des machines attaquantes étaient à l'étranger, le service web a été limité aux internautes situés en France (dont l'outre-mer). Enfin, une fois l'attaque terminée, le service a été complètement réouvert. En parallèle, l'affaire a fait l'objet d'un dépôt de plainte.

Comment établir des statistiques ici ? L'attaque visait techniquement un serveur web. Était-il la cible réelle ou un moyen d'atteindre la cible par ricochet, voire plusieurs cibles ? Combien de méfaits, se traduisant par une intention de nuire et un moyen de réalisation, cache cette opération ? Comme dans le cas précédent, les ordinateurs du *botnet* attaquant conduisent à autant de victimes d'intrusion informatiques. Dans certains cas, le *botnet* utilise des ordinateurs compromis pour son infrastructure : relais, canaux de commande, serveurs de résolution de noms (DNS). Les possesseurs de ces ordinateurs s'ajoutent à la liste des victimes. L'hébergeur, ses autres clients, les fournisseurs d'accès (côté serveur victime) subissent également un préjudice, plus ou moins sensible.

La question de la taille du *botnet* et de l'identification des ordinateurs qui le composent n'est pas évidente à résoudre. Les agressions applicatives utilisent des protocoles qui nécessitent que l'ordinateur attaquant présente son adresse réseau (IP), mais d'autres attaques, plus frustes, utilisent des protocoles pour lesquels l'adresse d'émission peut être fausse. Ainsi, un ordinateur du *botnet* peut envoyer vers le serveur victime des milliers de messages parasites avec autant d'adresses différentes. L'analyse des messages reçus par la cible de l'attaque ne permet pas de dénombrer et d'identifier les ordinateurs sources des parasites.

Attaque ciblée contre une entreprise

Les attaquants atteignent leur cible de la façon suivante [14] (*voir figure* 3) :

1) compromission d'un ou de plusieurs sites Internet publics, afin de les utiliser comme vecteurs d'infection des postes informatiques de l'entreprise ciblée. Les sites Internet publics sont sélectionnés parmi ceux qui sont régulièrement consultés par le personnel de cette entreprise (notamment le site Internet institutionnel de la cible). Les attaquants compromettent les sites en exploitant par exemple des vulnérabilités de logiciels utilisés pour gérer leur contenu [15]. Pour cela, les attaquants modifient les pages des sites afin de provoquer la navigation vers un script malveillant, provenant d'un serveur tiers, au moyen d'un lien illégitime [16]. Ce script exploite les vulnérabilités des navigateurs Internet usuels et de leurs modules d'extensions. Ces vulnérabilités sont généralement exploitées dans le mois suivant leur publication ou parfois beaucoup plus vite en quelques heures ;
2) compromission des postes informatiques des personnes ayant consulté le ou les sites Internet publics piégés lors de la première étape (par exemple, avec vol de mot de passe), grâce à un code malveillant spécifiquement conçu ;
3) accès aux réseaux internes de l'entreprise depuis les postes informatiques compromis ;
4) exfiltration de données sensibles copiées depuis les réseaux internes atteints.

Comment quantifier ce type d'attaques ? Cette agression globale se traduit par l'intrusion dans plusieurs ordinateurs de la victime, mais parfois aussi, par exploitation de leurs actions sur les postes piégés, sur des serveurs web d'autres organismes. Outre ces intrusions, chaque récupération de données est un préjudice pour la victime et se double parfois d'une qualification pénale : collecte déloyale de données, atteinte au secret patrimonial... Les employés peuvent être des victimes indirectes si des données sur leurs postes de travail leur sont personnelles et ont été copiées. Il en est de même des partenaires de l'entreprise victime : fournisseurs, sous-traitants, conseils, etc.

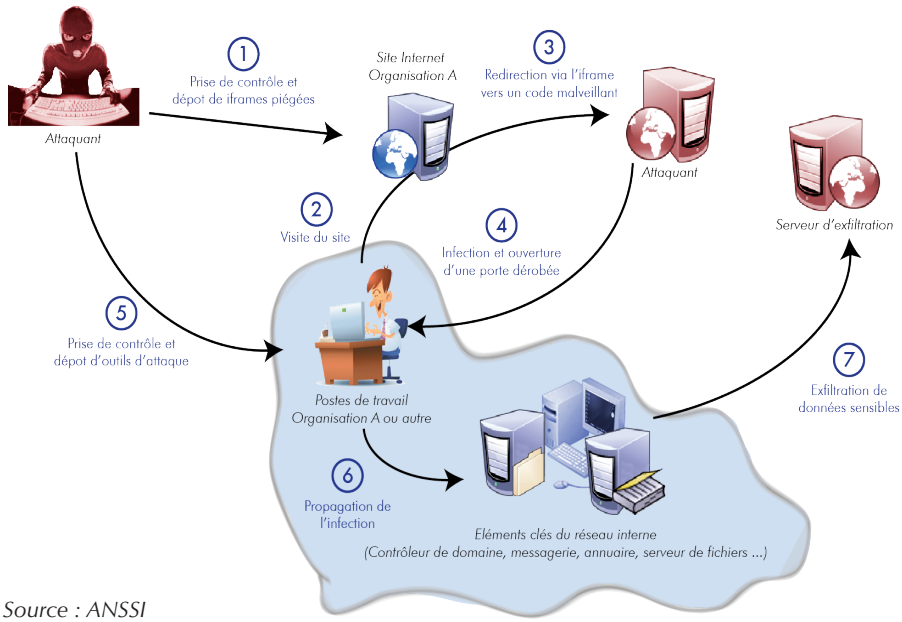
Conduite à tenir

Il ne s'agit pas de traiter ici le volet technique en détail, pour lequel un document est publié sur le site du CERTA [17], mais de s'attarder sur l'impact de la réaction à une agression sur les statistiques en criminalité.

En cas d'attaque suspectée (constat d'une intrusion ou tentative d'intrusion ; données modifiées, introduites ou supprimées ; entrave depuis l'intérieur ou l'extérieur du bon fonctionnement du système d'information),

(14) Pour une analyse technique plus fouillée, voir l'analyse d'attaques ciblant 72 entreprises et organisations dans 14 pays depuis 2006 : http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
(15) Un système de gestion de contenu (en anglais : *Content Management System* ou CMS) est une famille de logiciels destinés à la conception et à la mise à jour dynamique de site Web ou d'application multimédia.
(16) Dans des éléments HTML, par exemple de type IFRAME, ou des scripts Javascript plus ou moins obscurcis.
(17) Voir http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002.pdf

Figure 3. Scénario possible d'une attaque ciblée.



Source : ANSSI

le principe essentiel est de ne rien faire pouvant entraver le travail d'investigation (effacer ou altérer des traces) ou avertir l'attaquant. La déconnexion physique des réseaux extérieurs peut s'avérer nécessaire pour sauvegarder une activité ou des données éphémères.

Il est préférable de confier l'analyse de l'intrusion à des professionnels expérimentés. Attention aux effets néfastes découlant directement d'une mauvaise réaction après la découverte de l'intrusion. Une gestion saine de la découverte de l'incident améliorera l'analyse technique et non technique et permettra de mieux quantifier et qualifier les infractions commises.

Après compromission suspectée d'un système, il s'agit pour l'organisme ou l'entreprise de déposer plainte (infractions sanctionnées par les articles 323-1 et suivants du Code Pénal, d'atteinte à la propriété industrielle ou aux données personnelles), auprès du procureur de la République territorialement compétent, ou d'un service de police ou de gendarmerie.

Définitions, concepts

La capacité d'interprétation des cyber-conflits nécessite une approche partagée autour de définitions cohérentes, une compréhension des caractéristiques du cyberespace et une anticipation sur ses évolutions.

Cyberespace

Le cyberespace[18] est l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. On présente habituellement le système nerveux de nos sociétés modernes comme le cinquième domaine après la mer, l'air, la terre et l'espace. Les débats (ONU, OTAN, UE, etc.) sont vifs dans les tentatives internationales de régulation pour trouver l'analogie la plus pertinente avec les domaines classiques[19]. Nous opterons, pour notre part, plutôt pour l'espace, car les constituants « physiques » du cyberespace (ordinateurs en tous genres, tuyaux de communication, satellites, fréquences) ont toujours un propriétaire.

C'est une création purement humaine et un artefact. Le cyberespace est définitivement différent du monde physique naturel, car il obéit à des lois d'une autre nature. Les réseaux numériques n'ont pas de frontières, sont extensibles à l'infini et sont à la fois de nature très physique (machines, tuyauterie) et de nature abstraite et virtuelle. Le temps et l'espace y sont comprimés ; les attaquants potentiels sont parfois vos proches voisins. Les identités sont difficiles à discerner et les actions y sont incertaines. Les transitions y sont indécelables ; les faits précurseurs d'une attaque sont des événements très difficiles à percevoir.

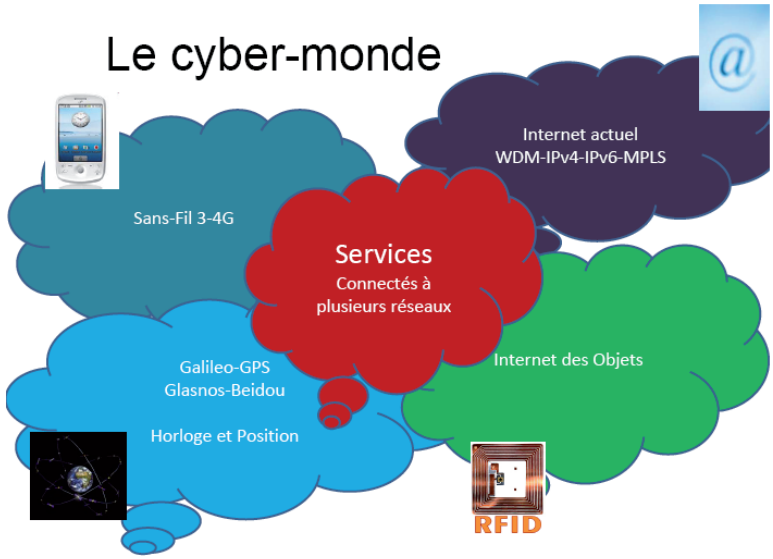
Le monde numérique n'est pas uniforme. Il agrège diverses sphères technologiques (*voir figure* 4) :

- la sphère de l'Internet, peu régulée, assez friable car reposant sur un squelette momifié. Elle est le champ privilégié des attaques informatiques, qui sont les vecteurs d'une nouvelle activité souterraine estimée de plus en plus lucrative. Sa refondation

(18) Pour une exégèse fouillée des représentations du cyberespace on lira avec profit le premier chapitre du livre : Daniel VENTRE, *Cyberespace et acteurs du cyberconflit,* Lavoisier, 2011.

(19) La notion intéressante de « Global Commons » poussée par certains à l'OTAN fait référence aux « jardins ouvriers » dans l'ancienne Angleterre.

Figure 4. Composantes du cyberespace.



Source : ANSSI

sur un socle sécurisé est régulièrement annoncée, mais cela mettra du temps et peut inquiéter aussi ;

- la sphère des technologies mobiles, très contrôlée par les opérateurs nationaux et globaux, plus fragile avec des limitations physiques et une bataille feutrée autour de la gestion future des fréquences qui resteront une ressource rare et stratégique ;
- la sphère de la géolocalisation, sous contrôle des quelques États en capacité de la déployer ;
- la sphère du nouvel Internet des objets, dont les enjeux de contrôle seront très importants. Ce sera vraisemblablement un futur champ d'attaques rendues possibles par une sécurisation faible prétextée par les coûts unitaires.

La convergence est amorcée entre ces diverses sphères, autour de services comme les réseaux intelligents (électriques et de transport), mais aussi dans le télétravail, la télémédecine, l'e-santé, l'e-administration, l'e-éducation, l'e-justice, la numérisation des contenus culturels… Au besoin en s'appuyant sur le développement d'infrastructures partagées ("cloud computing" ou « informatique nébuleuse », supercalculateurs, etc.). Cette convergence facilitera, à coup sûr, les modes d'action des cybercriminels car ils s'attaquent toujours aux maillons faibles d'un système.

Caractéristiques du cyberespace

Le cyberespace est fragile et le demeurera par le rythme effréné des mises sur le marché de produits logiciels dont la sécurité n'a pas été vérifiée et par la complexité intrinsèque des nouveaux développements. La cyber-fragilité se manifeste aussi sur deux autres points essentiels : l'existence de points singuliers de vulnérabilité et le potentiel de défaillances en cascade (effet domino). Elle se révèle d'une manière particulière dans le cadre des systèmes automatisés de contrôle des processus industriels, qui se sont ouverts sans réflexion préalable à l'informatique de masse et connectés aux réseaux ouverts. Une autre fragilité est constituée par nos machines numériques. Les chargements réguliers de mises à jour ou « patchs correctifs », bien que nécessaires, transforment petit à petit nos machines en un monceau de rustines. Il n'y aura probablement pas d'inflexion future notable sur ce point. Nos achats compulsifs se complaisent d'un rythme effréné de renouvellement, et l'innovation, parfois factice, « ringardise » toute consolidation.

Le cyberespace n'est pas assez diversifié. La parcellisation du futur Internet autour d'écosystèmes numériques contrôlés par quelques géants [20], dont aucun n'est européen aujourd'hui, a démarré. Le coût d'accès aux technologies numériques devient prohibitif. La cyber-diversité est trop absente de nos systèmes. Rien n'indique une évolution notable tant les sommes en jeu sont considérables. Mais si l'on se place du point de vue des cyber-conflits, Internet comme interconnexion de 20 000 réseaux ne présente plus la même homogénéité et se « balkanise » en zones qui seront le reflet d'un affrontement très clair entre plusieurs modèles de société ayant chacune leurs valeurs portées dans leurs modèles de protection des systèmes d'information. On distinguera, entre autres, le modèle libéral nord-américain (la liberté fonde la démocratie), le modèle chinois (l'organisation fonde la démocratie) et le modèle européen, où la protection du faible est plus prise en charge par l'État (la dignité fonde la démocratie) [21].

(20) « Le web est complètement mort », http://www.wired.com/magazine/2010/08/ff_webrip/all/1
(21) James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty", 4 janvier 2004, http://www.yalelawjournal.org/images/pdfs/246.pdf

La loi exponentielle de Moore (1965), qui affirme que la complexité des semi-conducteurs double tous les dix-huit mois à coût constant, est morte en 2010[22]. Les développements logiciels ou micro-logiciels suivent eux la loi de Hofstadter qui déclare que : « *Ça prend toujours plus de temps qu'on croit, même en prenant en compte la loi de Hofstadter*[23] ». Ainsi, les vulnérabilités de machines de plus en plus complexes avec des impératifs de rapidité de mise sur le marché vont croître dans une proportion plus que linéaire.

Parmi les 1 000 exaoctets[24] de volume annuel de l'information numérique, la proportion des informations souveraines à protéger est bien évidemment infinitésimale en volume, mais reste déterminante en termes de capacité d'influence, de développement économique et parfois même de survie pour les activités vitales de la Nation. Il faut donc repenser en profondeur la protection des informations – « secret » accessible, correct et réservé – qu'il soit personnel, industriel ou étatique. La protection des données personnelles a beau être encadrée par la loi en Europe, force est de constater le succès des réseaux sociaux, qui capturent ou falsifient notre intimité et diffusent notre affectif « à l'insu de notre plein gré ». Le droit à l'oubli numérique, que certains aimeraient ériger en nouveau droit de l'homme, se heurte à la « réalité du virtuel ». Détruire une information numérique est un oxymore. Les capacités de stockage annoncées, les outils de fouille immatérielle et d'inspection profonde de plus en plus performants et les nouvelles formes de traitement de l'« informatique nébuleuse » immortaliseront le patrimoine informationnel – modulo l'entropie des supports de stockage et de la pérennité de leurs gestionnaires – et deviendront aussi les outils privilégiés des pillages technologiques.

Cybersécurité

Le document de stratégie nationale[25] publié en février 2011 clarifie le terme de cybersécurité. C'est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. Trois dimensions la conditionnent. La cybersécurité fait appel, premièrement, à des techniques de protection des systèmes d'information connues depuis une vingtaine d'années sous le terme de Sécurité des systèmes d'information[26] (SSI). Elle s'appuie, deuxièmement, sur la lutte contre la cybercriminalité et, troisièmement, sur la mise en place d'une cyberdéfense. La cyberdéfense est l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information qu'il juge essentiels.

Cryptologie

Une autre caractéristique essentielle du cyberespace est l'importance centrale de la cryptologie, qui est la science englobant la cryptographie et la cryptanalyse. **La cryptographie** est la discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification ne passe inaperçue et/ou d'empêcher leur utilisation non autorisée. **La cryptanalyse** est le processus de déchiffrement de données protégées au moyen de cryptographie sans être en possession des clés de chiffrement.

La cryptographie est la seule technique efficace disponible pour protéger une information numérique en confidentialité et en intégrité. Elle réalise une réduction d'entropie sur les données à protéger grâce à de multiples clés qu'il s'agit de gérer comme les seuls secrets permettant de confiner le système d'information. La gestion de ces clés est un art difficile et de souveraineté, nécessitant une organisation rigoureuse qui se satisfait mal d'une externalisation trop poussée ou d'un recours à des solutions toutes faites. La cryptographie irrigue l'ensemble des architectures et dispositifs aptes à assurer la cybersécurité. La maîtrise de la cryptographie reste encore au cœur des problèmes de gouvernance d'Internet[27].

(22) Les lois empiriques de Moore ont trait à l'évolution de la puissance des ordinateurs et à la complexité du matériel informatique. C'est Gordon Moore lui-même qui annonce en 2010 que l'industrie approche de plus en plus des limites physiques de la micro-électronique. Les innovations futures de l'empilement en trois dimensions, des nanotechnologies et peut-être un jour du calcul quantique ou ADN, pourraient permettre de dépasser la pseudo-stagnation actuelle.

(23) Ou « Loi de glissement de planning » est une loi empirique concernant la difficulté de la planification particulièrement dans la gestion des développements logiciels. Cette loi auto-référentielle a été énoncée par Douglas Hofstadter dans son œuvre phare, « Gödel, Escher, Bach, les brins d'une guirlande éternelle ».

(24) L'octet, composé de huit éléments binaires, est une unité de mesure en informatique mesurant la quantité de données. Un exaoctet c'est 10^{18} octets (un milliard de milliards d'octets).

(25) *Défense et sécurité des systèmes d'information* - Stratégie de la France, voir http://www.ssi.gouv.fr/site_article318.html

(26) Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des attaques de quelques natures qu'elles soient.

(27) Citons, par exemple, DNSSEC (Domain Name System Security Extensions) qui a pour but de combler les failles de sécurité spécifiques au service du système de noms de domaines DNS indispensable au fonctionnement de l'Internet, voir http://www.afnic.fr/afnic/r_d/dnssec

Dans le cadre des enquêtes criminelles, elle est parfois un obstacle à franchir. Mais ce sont les mathématiques qui dictent leurs lois. Un exemple permet de l'illustrer. L'auteur ou le complice de l'infraction doit, à la demande des autorités judiciaires ou administratives, remettre la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement[28]. Il lui est possible, à partir de tout document chiffré, de fournir une fausse clé, aussi vraisemblable que la vraie clé de chiffrement, et pouvant correspondre à un document clair quelconque[29].

Cybercriminalité

La cybercriminalité est constituée des actes contrevenant aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible. Elle regroupe :

1. les crimes et délits traditionnels facilités par l'usage des nouvelles technologies : blanchiment d'argent sale, pédophilie, grand banditisme, terrorisme, etc. ;
2. les crimes et délits nouveaux directement liés à l'usage des Technologies de l'Information et de la Communication[30] : falsification de cartes bancaires, usurpation d'identité, taggage ou défacement de sites officiels, attaque de sites en déni de service, vol de données, vol de ressources informatiques, « *phishing* » ou hameçonnage, « *botnets* », « *carding* » (vente illégale de numéros de cartes bancaires), etc. ;
3. le détournement rapide des nouvelles technologies à des fins criminelles et terroristes : usage des téléphones portables pour déclencher les bombes artisanales, GPS de plus en plus accessible et couplé à des moyens de communication pour guider des engins explosifs, drones commerciaux, internet des objets, etc.

Une typologie des attaquants n'est pas l'objet de cet article. Un document publié par l'ANSSI et révisé en 2006[31] propose une classification forcément évolutive ainsi qu'une tentative de compréhension de leurs motivations souvent incertaines. Il distingue le hacker ou passionné, le cracker ou casseur, le fraudeur, l'employé malveillant, le militant, l'espion et le terroriste[32]. Les analyses resteront délicates dans ce domaine étant donné la diversité des acteurs. L'espionnage étatique ou industriel a une influence grandissante. Le renseignement jouera un rôle essentiel dans une meilleure compréhension des interactions entre des équipes œuvrant dans l'ombre et ayant une grande capacité d'adaptation aux environnements.

Prospective

Une vision prospective est nécessaire quand il s'agit de dimensionner les futures réponses à des cyber-agressions qui s'intensifient et se diversifient. Quels qu'en soient les motifs, idéologiques, d'espionnage et/ou financiers, les attaques se multiplient et sont le fait d'équipes de plus en plus organisées et déterminées pas toujours visibles si elles sont formées de bons, professionnels. La cybersociété aurait-elle ainsi connu sa parenthèse enchantée[34] de 15 ans entre 1995, apparition de l'Internet grand public et de l'e-commerce et 2010, année de la création du Cyber-Command aux USA ? Certaines analyses[35] situent la rupture du cyber-activisme vers des actions plus radicales en 2005[36]. De nouvelles menaces vont se développer : recyclage de sabotages physiques mieux ciblés ; attaques des couches basses dans les réseaux même si la surface d'attaque est moindre que dans les couches hautes ; utilisation des techniques du très haut débit avec un effet boomerang pour saturer des ressources ; sophistication des rançongiciels[37] ; banalisation de certaines techniques d'agression électromagnétique intentionnelle.

(28) Voir http://www.ssi.gouv.fr/archive/fr/reglementation/art_29_40_lcen.pdf
(29) En faisant appel au procédé cryptographique parfait du « one time pad ».
(30) Pour une étude détaillée : « Les marchés noirs de la cybercriminalité », CEIS, juin 2011, voir http://www.aisg.info/public/fr/medias/docutheque/document/externe/2011/186_ceis.pdf
(31) « Menaces sur les systèmes informatiques », 12 septembre 2006, voir http://www.ssi.gouv.fr/IMG/pdf/Guide650-2006-09-12.pdf
(32) « Souvent appelés les cyber-terroristes, moins courants, les terroristes sont aidés dans leur tâche par l'interconnexion et l'ouverture croissantes des réseaux : très motivés, ils veulent faire peur et faire parler d'eux. Les actions se veulent spectaculaires, influentes, destructrices, meurtrières. Ce profil est pris de plus en plus au sérieux par les États depuis l'attentat du 11 septembre 2001. Ils considèrent qu'une cyber-attaque perpétrée par un terroriste pourrait gravement nuire aux infrastructures économiques et critiques d'un État devenu très dépendant de ses systèmes d'informations vitaux ».
(33) Philippe WOLF, « Les cyberconflits, où va la sécurité des systèmes d'information ? », Forum ATENA « Où va la cyber société ? Champ de mines ou bateau ivre ? », 8 juin 2011, Paris.
(34) La parenthèse enchantée, d'après Françoise Giroud, est une courte période dans l'histoire de l'humanité, située entre l'apparition de la pilule contraceptive et celle du virus du SIDA. Cette période marquée par la révolution sexuelle aura duré 15 ans en France entre la loi Neuwirth de 1967 et 1982.
(35) Séminaire « cyber-activisme », Fondation pour la Recherche Stratégique, 30 juin 2011, Paris.
(36) Voir http://media.ccc.de/browse/congress/2005/22C3-920-en-we_lost_the_war.html
(37) Un rançongiciel ou ransomware est un logiciel malveillant qui prend en otage des données personnelles.

Le domaine de l'**Internet des objets** sera vraisemblablement un futur champ d'attaques rendues possibles par une sécurisation faible prétextée par les coûts unitaires. Pour prendre un seul exemple, un projet est en cours d'expérimentation en France, relatif au contrôle à distance des capteurs cardiaques. Dans un premier temps, le patient se rapproche d'une borne à partir de laquelle un centre de maintenance (situé en Allemagne) relève les informations du capteur/actionneur et peut en adapter les paramètres de pilotage. Dans un second temps, une puce sous la peau est reliée sans fil à un centre médical de contrôle, ce qui rend possible la distribution automatique des soins et permet d'ajuster aux besoins la distribution de médicaments. Ces solutions rendent une certaine autonomie aux personnes dépendantes et diminuent aussi les inconvénients que représentent les injections manuelles. Elles préfigurent, avec la miniaturisation des capteurs, les systèmes de distribution automatique de médicaments qui seront prochainement commercialisés aux États-Unis. Qu'adviendrait-il en cas d'attaque informatique[38] sur un tel système ? Interviewé sur les risques liés aux cyber-menaces, un responsable l'a considéré comme « acceptable au vu des avancées technologiques apportées » !

Dans son livre « l'accident originel[39] » de 2005, Paul Virilio (urbaniste et essayiste français, né en 1932) analyse le trait distinctif qui oppose la civilisation contemporaine à celles qui l'ont précédée : la vitesse qui est celle de la lumière dans nos fibres optiques : « *Si l'interactivité est à l'information ce que la radioactivité est à l'énergie – une puissance de contamination et de désintégration –, alors l'accident intégral du temps accumule les déflagrations du socius et de son intelligibilité, rendant peu à peu opaque le monde entier. Après l'accident des substances, autrement dit de la matière, vient donc le temps de l'accident des connaissances : c'est cela, la soi-disant révolution de l'information, et c'est aussi cela, la cybernétique : l'arbitraire de l'anarchie dans le pouvoir des nations, les différents pouvoirs d'une communauté non seulement désœuvrée par* l'AUTOMATION, *mais encore désaxée par la soudaine* SYNCHRONISATION *des activités humaines* ».

Caractérisations

Quatre questions principales caractérisent les cyber-conflits : ambiguïté de la source (qui m'attaque ?), ambiguïté du dommage (lequel ?), ambiguïté du moyen (comment ?), ambiguïté de la finalité (pourquoi ?). Nous confrontons ces quatre ambiguïtés à la réalité technique d'aujourd'hui et aux développements annoncés ou souhaités pour les réduire.

L'analyse est ici d'abord technique. Elle s'appuie sur un constat du célèbre article du juriste Lawrence Lessig en 2000 intitulé « Code is law[40] ». « *Ce régulateur, c'est le code : le logiciel et le matériel qui font du cyberespace ce qu'il est. Ce code, ou cette architecture, définit la manière dont nous vivons le cyberespace. Il détermine s'il est facile ou non de protéger sa vie privée, ou de censurer la parole. Il détermine si l'accès à l'information est global ou sectorisé. Il a un impact sur qui peut voir quoi, ou sur ce qui est surveillé. Lorsqu'on commence à comprendre la nature de ce code, on se rend compte que, d'une myriade de manières, le code du cyberespace régule* ». Ce qui est affirmé ici, c'est que tout usager du cyberespace est dépendant de réalisations tierces imparfaites (logiciel, micro-logiciel, matériel) dont il est parfois la victime innocente. De même, il peut devenir le complice involontaire de méfaits par la non-maîtrise (voulue par le constructeur) des technologies qu'il utilise. Le cyber-agresseur exploite ces faiblesses intrinsèques.

Fil rouge : quatre cyber-conflits

Quatre exemples réels parmi mille et pouvant être qualifiés de cyber-conflits vont nous servir de fil rouge pour éclairer certaines ambiguïtés. Pour la commodité, ils sont numérotés de 1 à 4.

EXEMPLE 1 DDOS : le premier exemple est une attaque en déni de service distribuée (DDOS) contre l'Estonie, qui a mis en action des réseaux de machines compromises ou zombies appelés *botnets*. Le contrôle malveillant et à distance de ces machines par une ou plusieurs machines (dites de commandes) permet des actions agressives variées et dont la puissance peut être démultipliée : relais de pourriels, réalisation d'opérations d'hameçonnage ou de filoutage (ou *phishing*), diffusion de programmes malveillants (*malwares*), saturation de ressources, diffusion de rançongiciels, vol et diffusion d'informations, calculs distribués (cassage de mots de passe par exemple), diffusion de produits contrefaits *via* des sites mouvants (techniques de *fast-flux*[41]). On considère généralement qu'une machine personnelle sur dix serait infectée par au moins un code malveillant autorisant parfois son enrôlement pour des tâches non souhaitées comme la diffusion de pourriels ou des saturations de ressources. L'attaque est survenue suite au conflit provoqué par le projet de déplacement du Soldat de bronze planifié par le gouvernement estonien en avril 2007 et qui a abouti à des nuits d'émeutes, émanant d'une minorité de nationalistes russophones implantée dans le pays. Elle a bloqué les sites gouvernementaux, des sites de banques, de médias et de partis politiques. Le numéro des urgences (ambulances, incendies) est même resté indisponible pendant plus d'une heure.

(38) YanYan Wang, John D. Haynes, Carey Thaldorf, "Security risks for remote intelligent Pharmacy-on-a-Chip delivery systems", International Journal of Biomedical Engineering and Technology, Vol. 2, N° 2, 2009.
(39) Paul Virilio, L'accident originel, éditions Galilée, 2005.
(40) Voir http://www.framablog.org/index.php/post/2010/05/22/code-is-law-lessig pour une traduction française. Pour une étude collective plus fournie, voir http://codev2.cc/download+remix/Lessig-Codev2.pdf
(41) Elle utilise une caractéristique du protocole DNS (ou Domain Name system) permettant d'attribuer à un même nom de domaine de nombreuses adresses IP.

EXEMPLE 2 APT[42] : le deuxième exemple est une attaque ciblée contre une entreprise. Début 2011, le PDG de la société de sécurité informatique américaine HBG*ary* diffuse une liste de membres présumés du groupe d'activistes qui s'est fait connaître sous le nom d'A*nonymous* en défenseur de W*ikileaks*. Cette liste aurait été obtenue notamment par une analyse automatique de données recueillies sur les réseaux sociaux T*witter* et F*acebook* et quelques fils de discussions. Le 5 février, A*nonymous* pénètre leur site web, copie des milliers de documents de la société et diffuse sur le réseau poste à poste « torrent » les boîtes mails de ses dirigeants, dévoilant, entre autres, des documents confidentiels sur de nouvelles techniques d'autopsie des mémoires machines. Le compte T*witter* du directeur est lui-même usurpé. Les conséquences de cette attaque – démission du directeur, image de marque souillée, dévoilement de projets de déstabilisation – nous intéressent moins que les techniques employées.

Cela commence par une injection de code SQL[43] sur le site web de la société *hbgaryfederal.com* développé par une société tierce. La récupération d'identifiants puis de mots de passe des responsables de HBG*ary* autorisés à mettre à jour le site est facilitée par l'emploi de la fonction de hachage MD5[44] obsolète et par le fait que les mots de passe de deux des responsables sont faibles car seulement composés de 6 lettres et de 2 chiffres. L'un d'eux utilise d'ailleurs ce même mot de passe sur son compte T*witter* et son compte L*inkedIn*. C'est encore grâce à ce mot de passe que les agresseurs accèdent à travers le protocole non sûr SSH à un compte client d'une machine interne de la société sous Linux. Cette machine n'ayant pas été mise à jour depuis quatre mois, l'exploitation d'une vulnérabilité connue permet une élévation de privilège qui donne accès à la totalité du contenu de celle-ci. Utilisée comme machine de sauvegarde, elle dévoile des gigaoctets de données de recherche. Le patrimoine informationnel de la société est accessible et diffusable mais ce n'est pas tout.

Les deux mots de passe, toujours eux, donnent accès aux deux boîtes de courrier électronique de ces responsables hébergés sous G*oogle Apps*. Mais l'un de ces dirigeants a également des droits d'administration sur la boîte de messagerie interne de la société gérée elle proprement en termes de sécurité avec les certificats numériques adéquats. Se déroule alors une opération d'ingénierie sociale pour faire sauter les derniers verrous internes et accéder, entre autres, à la messagerie du directeur lui-même. De faux vrais messages sont échangés qui exploitent finement l'intimité révélée par l'intrusion initiale. Tout cela est très pédagogique, et pour la petite histoire, invérifiable, cette partie de l'opération aurait été menée par une adolescente de 16 ans.

EXEMPLE 3 SCADA : le troisième exemple relève également de l'attaque ciblée. Tout a été dit ou presque sur S*tuxnet*[45], premier ver découvert qui identifie et reprogramme des systèmes industriels. J'en rappelle les principales caractéristiques : pas de techniques nouvelles, mais une combinaison unique créant un code complexe, une exploitation de quatre failles non corrigées dites 0-day, la subtilité du dommage attendu avec une analyse très renseignée des cibles, des modes de diffusions multiples même en « *air gap* » – grâce aux clés USB –, de l'usurpation de signatures après vol ou recel de clés privées, des auto-sauvegardes. Il visait les systèmes utilisant les logiciels SCADA WinCC/PCS 7 de Siemens.

EXEMPLE 4 HFT[46] : le quatrième exemple est plus complexe à comprendre et à qualifier. Il s'agit d'un mini-krach boursier qui s'est déroulé autour du D*ow Jones* le jeudi 6 mai 2010 à partir de 14h38 heure locale sur une dizaine de minutes. Il est bien difficile de trancher entre les diverses explications qui ont été proposées pour expliquer ce « *flash crash* »[47]. Elles tournent souvent autour de l'emballement des machines qui gèrent les transactions et en particulier le « H*igh* F*requency* T*rading* », qui a atteint 73 % du volume total des actions échangées en 2009 sur les marchés américains et constitue la moitié des échanges de produits dérivés. Les autorités cherchent toujours désespérément à contrôler ces risques[48].

Ambiguïté de la source (qui m'attaque ?)

Cette première question, si on la projette sur Internet qui interconnecte de manière globale des réseaux

(42) La société de sécurité américaine Mandiant a trouvé une appellation marketing à ces attaques en recyclant un terme avancé par l'US Air Force en 2006 : Advanced Persistent Threat (APT) en citant l'opération « Buckshot Yankee » visant les réseaux militaires classifiés des USA en 2008, l'opération Aurora visant Google en 2009.

(43) L'injection de code est une technique consistant à détourner l'utilisation normale d'un programme pour exécuter un code ou une commande arbitraire. SQL (sigle de Structured Query Language) est un langage informatique normalisé qui sert à effectuer des opérations sur des bases de données.

(44) On nomme fonction de hachage une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Le Référentiel Général de Sécurité interdit l'emploi de la fonction MD5.

(45) Voir, parmi beaucoup d'autres, http://arstechnica.com/tech-policy/news/2010/11/clues-suggest-stuxnet-virus-was-built-for-subtle-nuclear-sabotage.ars

(46) Les transactions à haute fréquence (en anglais High-Frequency Trading), réfèrent à l'exécution à grande vitesse de transactions financières faites par des algorithmes informatiques.

(47) Voir, par exemple, www.nanex.net/20100506/FlashCrashAnalysis_Intro.html

(48) Entretien avec Jean-Pierre Jouyet, *Le Monde*, dimanche 13 et lundi 14 juin.

souvent hétérogènes[49], pourrait trouver une réponse simple dans la suite TCP/IP qui est l'ensemble des protocoles utilisés pour le transfert des données. Les datagrammes IP qui sont les principales unités d'information sur Internet comprennent une adresse IP source (adresse IP de la machine émettrice qui permet au destinataire de répondre) et une adresse IP destination (adresse du destinataire). Le routage IP assure l'acheminement d'un datagramme IP à travers un réseau en empruntant le chemin potentiellement le plus court. Il est assuré par des machines appelées routeurs, reliées et reliant au moins deux réseaux. Il suffit donc, en principe, de remonter ce chemin de proche en proche pour retrouver l'origine d'une agression. Mais les cailloux blancs du Petit Poucet fonctionnent mal dans le cyberespace. De plus le facteur humain joue à plein dans ces difficiles problèmes d'attribution aussi bien du côté de l'agresseur qui concentre sa ruse sur l'effacement de ses traces ou l'usurpation d'autrui que du côté de l'agressé victime d'ingénierie sociale ou de négligences souvent involontaires ou non conscientes.

Pour protéger les systèmes d'information, il est de bonne pratique d'ériger des barrières successives, selon les principes de la défense en profondeur[50], sous forme de passerelles avec ruptures protocolaires, de zones démilitarisées et parfois même de fausses pistes ou chausse-trappes[51]. Il est alors fait usage, entre autres, de serveurs mandataires (proxy en anglais) qui sont des serveurs informatiques ayant pour fonction de relayer des requêtes entre un poste client et un serveur. Ils assurent notamment des fonctions de sécurisation du réseau local, de filtrage et d'anonymisation, mais aussi de journalisation. L'utilité des serveurs mandataires est importante, notamment dans le cadre de la protection des systèmes d'information.

Une autre illustration de cet usage de machines à rebonds successifs est le réseau Tor[52] utilisant une technique de routage par oignon mise au point initialement par le « N*aval* R*esearch* L*aboratory* » des États-Unis. Pour « anonymiser » un parcours sur Internet, « *le logiciel construit incrémentalement un circuit de connexions chiffrées passant par des relais sur le réseau. Le circuit passe d'un bond à l'autre, et chaque relais sur le chemin ne connaît que le relais qui lui a transmis la connexion, et celui à qui il doit la remettre. Aucun relais individuel ne connaît le chemin complet qu'emprunte une donnée. Le client négocie des clés de chiffrement pour chaque bond du circuit, pour permettre à ce que chaque relais ne puisse pas tracer les connexions qui passent par lui.* […] *Tor utilise le même circuit pour toutes les connexions effectuées dans les 10 minutes. Les requêtes effectuées ensuite génèrent un nouveau circuit, pour empêcher de faire le lien entre vos anciennes actions et les nouvelles* »[53]. La machine cible ne peut connaître, en théorie, que la machine de sortie du réseau. Bien évidemment, la sécurité de ce réseau est remise en cause régulièrement, car la confiance dans les nœuds du réseau ne peut être uniforme.

On considère généralement, avec ou sans utilisation de techniques d'anonymisation[54], qu'après deux ou trois rebonds, la remontée de la trace devient extrêmement délicate. L'usage de machines hébergées dans des « paradis numériques » rend la reconstitution des parcours quasi impossible.

Si l'on se place du point de vue de l'attaquant, les choses sont plus simples. Il s'agit d'usurper l'identité d'un internaute pour maquiller l'origine de l'attaque. Le plus simple consiste à utiliser un hotspot wifi ou à usurper une connexion sans fil accessible (densité très forte en ville). Le canal radio est une composante critique des réseaux mobiles qui permettent aujourd'hui, à travers les ordiphones, la quasi-totalité des actions informatiques. Il est vulnérable au brouillage et à l'interception. La bonne recommandation de 2002[55] tient plus que jamais : « *l'utilisation du protocole sécurisé* IPSEC *reste la manière la plus sûre de sécuriser son réseau sans fil, ce qui n'interdit pas de mettre en place le chiffrement disponible sur le lien radio* ». Elle n'est pratiquement jamais appliquée (et souvent impraticable sur les points d'accès).

EXEMPLE 2 APT: La police espagnole a arrêté début juin 2011 trois agresseurs informatiques considérés comme les responsables pour l'Espagne de l'organisation internationale A*nonymous*. D'après le chef de la Brigade d'investigation technologique de la police espagnole, c'étaient « *des experts informatiques* » capables de « *crypter* » leurs échanges. Deux d'entre eux « *n'avaient pas de connexion internet chez eux* » pour ne pas éveiller les soupçons et accédaient au web en passant par les connexions wifi des voisins. Rien ne prouve leur implication dans l'attaque HBG*ary*, mais l'autopsie de leurs machines permettra peut-être d'en savoir plus.

Ce problème d'attribution d'une attaque rejoint celui de l'authentification future de l'internaute dans un monde où la moitié de l'humanité n'a pas encore d'identité. Il suscite articles et débats, malgré « la dernière liberté du dernier mètre ». Ainsi le PDG de *Google*, Éric Schmidt, a estimé, le 4 août 2010, que l'anonymat sur Internet était voué à disparaître et serait remplacé par une « *transparence totale* ». Quelques jours

(49) Louis Pouzin, inventeur français du datagramme, parle de balkanisation.
(50) Mémento sur le concept de la défense en profondeur appliqué aux SI, www.circulaires.gouv.fr/pdf/2009/04/cir_2014.pdf
(51) La technique des leurres informatiques prend le nom de honeypot, ou pot de miel. Il s'agit d'ordinateurs ou de programmes volontairement vulnérables destinés à attirer et à piéger les attaquants.
(52) Un autre exemple est constitué par le réseau Freenet.
(53) Voir https://www.torproject.org/index.html.fr
(54) Voir le dossier « Anonymat sur Internet : risque ou nécessité ? », *Magazine MISC*, n°54, mars/avril 2011.
(55) Voir http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002.pdf

plus tard, un haut dignitaire du régime chinois, Wang Chen, annonce la mise en place le plus vite possible d'« *un système d'identification réelle sur Internet* ». Un autre Schmidt prénommé Howard, le nouveau responsable de la sécurisation d'Internet à la Maison-Blanche, a proposé le déploiement d'un système « *d'identification volontaire et vérifiée* ». Celui-ci serait basé sur la possession d'une carte à puce capable d'identifier l'empreinte digitale de l'internaute. Celui-ci devrait ainsi montrer patte blanche, via un lecteur relié à son ordinateur, à chaque fois qu'il se connecterait à Internet. La biométrie n'est pas d'une grande utilité dans ce contexte[56], sans compter les nombreux problèmes de respect de la vie privée posés par le recueil et le stockage massif de données de ce type.

Le meilleur système d'authentification reste la carte à puce avec saisie de code porteur et lecteur non transparent. Les cartes récentes résistent aujourd'hui à des attaques sophistiquées par canaux auxiliaires[57]. Mais les agresseurs ne se soumettent pas à ces dispositifs d'authentification quand ils ne cherchent pas à les casser[58].

La lente bascule vers le nouvel espace d'adressage IPV6[59] promet une meilleure identification des « internautes » et fait disparaître la translation d'adresse qui obligeait de fait à une rupture entre enclaves. Mais l'impératif de sécurisation oblige à recréer ces ruptures pour masquer les architectures des réseaux internes. Les experts répètent qu' : « *il faut filtrer, filtrer et encore filtrer* ». Les coprocesseurs de sécurité peuvent être utiles pour marquer individuellement les machines informatiques. Mais cela s'avère insuffisant devant des attaques nouvelles sur les ressources matérielles annexes comme les cartes réseau ou de type « *man in the middle* » dans les phases critiques de démarrage. Les techniques de virtualisation dans les systèmes d'exploitation sont duales : comme souvent, très efficaces en matière de protection, mais aussi exploitables par les attaquants pour effacer ou falsifier des traces.

L'informatique nébuleuse ou *Cloud Computing* revisite le concept initial client-serveur de l'Internet. Profitant des capacités du très haut débit et de « fermes de serveurs » de plus en plus gigantesques, son concept consiste à déporter sur des serveurs distants des traitements informatiques traditionnellement localisés sur des serveurs locaux ou sur le poste client de l'utilisateur. Ce n'est pas seulement la recherche d'un effet d'aubaine, lié à la crise, de recyclage des surplus américains, mais une rupture profonde par rapport aux pratiques informatiques traditionnelles. Les stockages de données et les calculs sont délocalisés dans le nuage. Le temps et l'espace y sont éclatés. Retrouver la source d'une attaque peut s'y avérer redoutable d'autant plus que les « géants du web » se battent aujourd'hui autour de solutions propriétaires dont l'interopérabilité n'est pas garantie.

Ambiguïté du dommage (lequel ?)

Un trait distinctif qui oppose la civilisation contemporaine à celles qui l'ont précédée est la vitesse du cyberespace qui est celle de la lumière dans les fibres optiques[60]. Les cyber-conflits se jouent à cette vitesse. Des réponses doivent être apportées dans les cinq minutes mais cela dépasse le cadre de cet exposé. Comprendre et décortiquer une cyber-attaque prend du temps. Cela mobilise parfois quelques années-homme. Il s'agit en particulier de comprendre les dommages que l'agresseur s'ingéniera à rendre imperceptibles. Il s'agit aussi d'écarter les estimations financières simplistes[61] qui font florès et qui trouvent souvent leurs sources dans des intérêts commerciaux trop visibles.

Le cyberespace est d'abord un réseau physique formé de machines, de câbles, de fréquences dont les propriétaires sont multiples. Il ne s'agit pas d'un « *no man's land* » comme l'espace maritime. Les dommages peuvent donc y être physiques, comme le sabotage de nœuds de communication[62], mais sa résilience raccourcit les délais de remise en route. D'autres agressions physiques comme les agressions électromagnétiques intentionnelles sont plus difficiles à caractériser[63].

EXEMPLE 3 SCADA a mis en lumière qu'un programme malveillant pouvait cibler *in fine* le fonctionnement

• • • (56) Philippe Wolf, « De l'authentification biométrique », http://www.dgdr.cnrs.fr/fsd/securite-systemes/revues-pdf/num46.pdf

(57) Une carte à puce est un coffre à clés. Pour essayer de récupérer un morceau de ces clés (quelques bits suffisent parfois à affaiblir irrémédiablement le dispositif), l'analyse de canaux d'information (consommation, émissions électromagnétiques, chaleur) permet quand un certain nombre de précautions n'ont pas été prises (comme l'équilibrage des calculs quels que soient les bits de clés) de deviner la valeur d'un des composants.

(58) À l'exemple du vol des ferments RSA SecureID ayant compromis ce dispositif en mars 2011 et rendant possible des attaques ciblées (Lockheed Martin, Citibank).

(59) La taille de l'espace d'adressage (2^128=3,4×10^38) offre plus de 667 millions de milliards d'adresses par millimètre carré de surface terrestre de quoi identifier le monde réel.

(60) Paul Virilio, L'accident originel, éditions Galilée, 2005.

(61) « Chiffres en folie: le coût des cyberattaques », 11 juillet 2011, voir http://owni.fr/2011/07/11/chiffres-en-folie-le-cout-des-cyberattaques/

(62) Le 28 mars 2011, une Géorgienne âgée de 75 ans, en voulant récupérer du cuivre, a sectionné une fibre optique qui a provoqué la coupure de l'accès Internet pour l'Arménie pendant près de 5 heures.

(63) Voir, par exemple, Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid, http://www.futurescience.com/emp/ferc_Meta-R-323.pdf

physique de machines industrielles. *Stuxnet* est programmé pour agir sur des convertisseurs de fréquences qui permettent de générer des fréquences appropriées à certains moteurs bien spécifiques, tournant à vitesse élevée comme ceux des centrifugeuses destinées à l'enrichissement de l'uranium[64].

Mais le cyberespace, au-delà des systèmes, des biens et des personnes, c'est également un artefact produisant une société virtuelle où l'information et la communication modèlent le monde réel. Les dommages logiques et sémantiques dans cette sphère sont plus profonds : pillage de patrimoine informationnel, désinformation, déstabilisation, rumeurs. Toutes les techniques de manipulation[65] y sont applicables avec une puissance calculatoire inégalée.

EXEMPLE 4 HFT : le dommage immédiat était très visible : l'indice S&P du *NYSE* perd 10 % en quelques minutes ; plusieurs actions chutent à un penny (0,01 $) : Accenture, *Procter & Gamble*, une action grimpe à 100 000 $. Le dommage est tellement inexplicable (emballement des machines ?) que la SEC décide d'« effacer » 25 mn de transactions, une première !

Deux caractéristiques exploitables du numérique vont nourrir l'ambigüité du dommage : le piégeage et la stéganographie.

Dans un article célèbre publié il y a déjà 25 ans (*Reflections on Trusting Trust*[66]), Ken Thompson conclut ainsi sa démonstration de piégeage par porte dérobée de la structure d'un logiciel d'ordinateur : « *La morale est évidente. Vous ne pouvez pas faire confiance à du logiciel que vous n'avez pas totalement créé par vous-même. En particulier, ne faites pas confiance à des sociétés employant des types comme moi* ». Les possibilités de piégeage combinant les couches physiques, syntaxiques et sémantiques sont infinies. L'usage d'un piège dormant est indétectable dans la plupart des cas.

Les quatre fonctions de protection de la vie privée[67] sont aussi utilisables pour dissimuler les dommages et brouiller les pistes : l'Anonymat (FPR_ANO) qui garantit qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité d'utilisateur ; la Possibilité d'agir sous un pseudonyme (FPR_PSE) qui garantit qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité d'utilisateur, mais peut quand même avoir à répondre de cette utilisation ; l'Impossibilité d'établir un lien (FPR_UNL) qui garantit qu'un utilisateur peut utiliser plusieurs fois des ressources ou des services sans que d'autres soient capables d'établir un lien entre ces utilisations ; la Non-observabilité (FPR_UNO) qui garantit qu'un utilisateur peut utiliser une ressource ou un service sans que d'autres, en particulier de tierces parties, soient capables d'observer que la ressource ou le service est en cours d'utilisation.

Le vol d'information numérique (patrimoine informationnel) n'est jamais qu'un clonage. Il ne touche pas à l'objet volé. La discrétion de l'exfiltration dépend du bon usage de techniques de nature stéganographique. Le chiffrement préalable des donnés volées est accompli par le code malveillant extracteur pour leurrer les filtres périphériques.

La stéganographie est la science de la communication invisible d'informations. Les techniques de stéganographie cherchent à dissimuler l'existence même des informations échangées par exploitation de la redondance d'information, par dissimulation d'information dans des fichiers informatiques, par exploitation de l'imprécision de la perception humaine visuelle ou auditive. Il s'agit de cacher, à l'aide d'une stégo-clef, une information numérique (texte, son, image, vidéo, etc.) ou stégo-message dans un support numérique ou stégo-conteneur sans en altérer la perception. L'objet résultant est le stégo-objet. Le propriétaire ou destinataire du stégo-objet est en mesure d'extraire le stégo-message à l'aide de la stégo-clef. Un article théorique[68] prenant comme modèle deux personnes souhaitant communiquer entre-elles en prison à partir d'une liaison numérique démontre que quelles que soient les agissements d'un gardien qui écoute et agit à sa guise sur le canal de transmission (il n'a pas le droit de couper le canal), le partage d'informations est possible de manière invisible.

Le dommage est souvent indirect.

EXEMPLE 3 SCADA : Le vol, chez des fournisseurs asiatiques qualifiés par *Microsoft*, de clés de signature a eu un effet indirect ou retard. Les techniques utilisées pour ce vol n'ont pas été décrites. Une fois le code *Stuxnet* signé, sa présence est devenue plus discrète, car il était considéré par les postes d'accueil comme un logiciel de confiance.

Le dommage dépend aussi de la valeur intrinsèque des informations divulguées. La proportion des informations souveraines à protéger est infinitésimale en volume par rapport à l'ensemble des données qui circulent librement, mais reste déterminante en termes de capacité d'influence, de développement économique et parfois même de survie pour les activités vitales de la Nation. Les pertes peuvent être incalculables quand

(64) Voir analyse de *Symantec* qui pense que *Stuxnet* peut agir sur les convertisseurs de fréquences en induisant des variations cycliques très subtiles, susceptibles d'altérer la pureté du combustible enrichi.

(65) Jean-Luc Guilmot, « Décodage de 25 techniques de désinformation », juin 2008, http://www.vigli.org/PDF911/Decodage_de_25_techniques_de_desinformation.pdf

(66) Voir http://cm.bell-labs.com/who/ken/trust.html

(67) Voir chapitre 9 des critères communs http://www.ssi.gouv.fr/IMG/pdf/CCpart2v21-fr.pdf

(68) Nicholas J. Hopper, John Langford, Luis von Ahn, "Provably Secure Steganography", http://hunch.net/~jl/projects/steganography/stego_newest.pdf

elles touchent à un savoir-faire critique ou quand elles impactent même indirectement des vies humaines. Il faut donc repenser en profondeur la protection des informations – « secret » accessible, correct et réservé – qu'il soit personnel, industriel ou étatique ; prise en compte du temps[69]. Beaucoup a été dit et écrit sur la vraie valeur des télégrammes diplomatiques diffusés par *Wikileaks*. Le dommage est d'abord politique par la lente[70] mise en ligne des télégrammes dans une campagne médiatique très orchestrée.

Ambiguïté du moyen (comment ?)

La boîte à outils pour cyber-attaquants est vaste. Une tentative de classification distingue : les pièges (porte dérobée ou *trapdoor*, piège matériel, logiciel, syntaxique, sémantique), la prédation informationnelle (sources dites ouvertes – *data-mining* –, interceptions – SIGINT –), les codes malveillants – *malware* – (bombe logique, cheval de Troie[71] – trojan –, vers et virus) et d'autres techniques (ingénierie sociale, déni de service : *botnets*, brouilleurs, canaux auxiliaires, signaux parasites compromettants, agressions électromagnétiques intentionnelles, etc.). La caractérisation des armes employées lors d'une cyber-attaque est une tâche difficile et de longue haleine.

Le théorème dit du virus exposé en 1984 par Fred Cohen[72] affirme que la détection d'un virus informatique est indécidable par une analyse a priori ou une analyse dynamique. Ce théorème rend théoriquement impossible la détermination, à coup sûr, de la malveillance d'un programme informatique. On peut prendre ici l'exemple connu de tous du logiciel de téléphonie sans infrastructure *Skype*. Certains ont présenté cet outil comme le premier cryptovirus de masse car il dissimule, entre autres, l'annuaire sur les machines des réseaux desservis et traverse les gardes-barrières périphériques par une analyse protocolaire fine. Ce logiciel est protégé contre la rétro-conception par un usage immodéré de l'obscurcissement. On parle d'obfuscation de code. Cette caractéristique a fait la fortune de ses concepteurs. Pour les programmes malveillants, l'obfuscation de code fait partie des mécanismes de base, au même titre que la furtivité, l'auto-mutation ou le polymorphisme. Dans un livre chinois de 1999 intitulé en français « La Guerre hors limites »[73] les auteurs déclaraient « *Nous croyons qu'un beau matin les hommes découvriront avec surprise que des objets aimables et pacifiques ont acquis des propriétés offensives et meurtrières* ». Une des difficultés principales est l'ambivalence naturelle des fonctions de sécurité qui peuvent être mises à profit par des attaquants (un couteau de cuisine est lui aussi dual). Les anti-virus et autres filtres de sécurité deviendront eux-mêmes des cibles privilégiées et des vecteurs d'attaques étant donné les droits excessifs qu'on leur accorde.

La prolifération des cyber-armes et de leurs modes d'emploi sont inéluctables.

EXEMPLE 3 SCADA : un site russe propose déjà en ligne un « *toolkit* » à partir des fonctions élémentaires de *Stuxnet* pour réaliser de nouvelles armes.

EXEMPLE 2 APT illustre la notion de chemin d'attaques qui consiste, à l'image d'une opération commando, à rechercher les maillons faibles, à exploiter les failles qu'elles soient techniques ou humaines, à créer la confusion, à effacer les traces, à brouiller les pistes. La vaste boîte à outils va servir dans ce cas la stratégie dans le cadre des objectifs visés. Un document annuel d'une société américaine[74], analysant les fraudes informatiques financières aux États-Unis, propose une classification des événements élémentaires sous la forme de 630 événements menaçants (une grille à deux entrées : « nature de l'attaque » x « cible »). Un chemin d'attaque est une combinaison de ces événements élémentaires affectant aussi bien l'agresseur que l'agressé. Une analyse de l'ensemble des fraudes traitées judiciairement à travers cette grille d'analyse montre que seuls 55 de ces éléments menaçants ont été découverts. 90 % de l'espace des menaces n'a pas été mis en œuvre. Cela ne prouve pas un manque d'imagination des attaquants, mais illustre le fait que les failles sont largement communes et que les techniques éprouvées marchent toujours. Ce rapport montre également que, parmi les outils logiciels malveillants analysés, 43 % sont des combinaisons et du paramétrage d'éléments existant (large diffusion des briques élémentaires) et 18 % des réalisations *ad hoc*. De façon générale, les méthodes d'analyse de risques[75] fournissent des éléments de compréhension précieux pour reconstruire une cyber-agression.

• • • (69) Ainsi, le secret médical protège les données vingt-cinq ans après le décès de la personne ou cent vingt ans après sa naissance si la date du décès n'est pas connue.

(70) Le 11 juin seuls 14 604 télégrammes sur 251 287 ont été diffusés.

(71) Un cheval de Troie est un programme, installé le plus souvent à l'insu de l'utilisateur, qui permet à un attaquant de se connecter à l'ordinateur de sa victime. Un tel programme est en général composé d'un serveur (installé sur la machine de la victime), et d'un client qu'utilise l'attaquant pour prendre la main sur la machine. Voir http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-002/

(72) Voir http://all.net/books/virus/part5.html

(73) Liang Qiao (Auteur), Xiangsui Wang (Auteur), Michel Jan (Préface), Hervé Denès (Traduction), *La Guerre hors limites*, Rivages poche.

(74) 2011 Data Breach Investigations Report, http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

(75) Une méthode comme EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet de construire des scénarios redoutés, voir http://www.ssi.gouv.fr/site_article45.html

Une autre caractéristique des protocoles de l'Internet c'est de fonctionner selon un mécanisme puissant de poupée russe appelé l'encapsulation. Une attaque peut en profiter pour rejoindre des fonctions de stéganographie. Des techniques connues sous le nom de « *Deep Packet Inspection* » (DPI) cherchent à démêler l'écheveau. Le DPI mêle les fonctions d'un système de détection d'intrusion (IDS) et d'un système de prévention d'intrusion (IPS ou IDS actif) à celles d'un pare-feu traditionnel : cette combinaison permet de détecter certaines attaques que les IDS/ISP et le pare-feu ne peuvent révéler à eux seuls. Mais leur usage étant potentiellement intrusif, leur mise en œuvre nécessite des règles d'emploi bien précises.

La machine peut être d'une aide précieuse à l'investigation forensique[76] par un pré-traitement intelligent des traces ou logs laissés directement ou indirectement par l'agression. La structuration sémantique des « *logs* » et les fonctions d'analyse devront être améliorées. Il faut aussi journaliser pour détecter ce qu'on ne peut empêcher.

Enfin, l'ampleur d'une attaque est délicate à mesurer en temps réel dans le feu de l'action.

EXEMPLE 1 DDOS : Un responsable estonien a présenté récemment la liste reconstituée des machines attaquantes et leur origine. On trouve dans le Top10 : Égypte 6082, États-Unis 5231, Vietnam 1601, Turquie 988, Pérou 789, Pologne 620, Allemagne 587, Russie 527, Inde 521, Brésil 510. Même si l'attaque de type DDOS est avérée, la reconstitution fine du botnet est bien difficile : s'agit-il d'un test ? D'une première attaque ? D'une diversion ? Beaucoup de données fantaisistes circulent sur les tailles qu'atteindraient ces réseaux et sur les prix de leur vente par appartements. Certaines exagérations sont très vite colportées ; certains commentateurs ont parlé d'un million de machines. Pour l'anecdote, une contre-attaque prônée par certains comme une réponse acceptable relevant du droit à la légitime défense aurait atteint en priorité l'Égypte et aussi la Turquie, membre de l'OTAN.

Le détournement de moyens sera, à n'en pas douter, une arme du futur. *EXEMPLE 4 HFT* : parmi les moyens utilisés, on trouve le « *Quote Stuffing* ou *Stub quote* » ou « bourrage » de cotations, qui consiste à utilisation de faux ordres de vente ou d'achat d'actions pour « pourrir » les données des concurrents. Ils sont généralement annulés après quelques millisecondes et c'est totalement légal. Ces techniques peuvent être qualifiées d'une forme nouvelle de Déni de Service : le Déni de Service Financier (FDoS)[77].

Des asymétries fortes existent entre l'attaquant et le défenseur. L'attaquant choisit le meilleur endroit, la meilleure chronologie et les moyens d'attaque appropriés. Le défenseur doit défendre partout, tout le temps et contre toutes les attaques. L'attaquant est agile et les cycles de décisions de petits groupes sont courts. Le défenseur doit mobiliser des organisations souvent lourdes. Son principal avantage est la connaissance et le contrôle de son architecture. C'est autour d'une défense en profondeur plus dynamique qu'il doit organiser sa cyber-protection.

Ambiguïté de la finalité (pourquoi ?)

Il reste une dernière question à résoudre concernant la finalité. Une réponse immédiate semble plus simple, mais ne masque-t-elle pas des intentions plus cachées ?

EXEMPLE 1 DDOS : divers rapports ont essayé de qualifier cette attaque contre l'Estonie[78] comme première cyber-guerre contre un État, en désignant prudemment la Russie comme donneur d'ordre. C'est probablement exagéré étant donné la fragilité des réseaux en place. La cyber-attaque n'a fait qu'accompagner les nuits d'émeutes. Le pays a développé depuis sa résilience et une attaque de ce type aujourd'hui aurait bien moins d'effets.

EXEMPLE 2 APT : la motivation revendicatrice de la franchise Anonymous justifie-t-elle une diffusion publique de quelques gigaoctets de données intrusives ? L'activité délicate de la société HBG*ary* se développe dans un environnement concurrentiel et une opération de déstabilisation plus profonde est fortement plausible.

EXEMPLE 3 SCADA : jamais ver informatique n'a donné lieu à autant de déclarations parfois contradictoires. L'Iran a accusé un État ou une organisation étrangère de l'avoir délibérément visé. Bruce Schneier, analyste éclairé des sujets de cybersécurité, a qualifié d'intéressante l'hypothèse selon laquelle la centrale nucléaire de Bouchehr aurait été visée, tout en considérant qu'on manquait de preuves. Début octobre 2010, à l'occasion d'un article sur l'Unité 8200, *le Figaro* écrivait : « *Des indices découverts dans les algorithmes du programme Stuxnet, ayant infecté, entre autres, les systèmes informatiques iraniens, feraient référence à l'héroïne biblique Esther. Les liens éventuels entre cette offensive virtuelle et Israël ne seront sans doute jamais prouvés, mais la suspicion des milieux du renseignement est forte* ». Lors de son pot de départ, le général israélien Gabi Ashkenazi[79] a reconnu être le père du ver *Stuxnet*… Tout ce que nous dit la science numérique, c'est que

(76) L'analyse forensique en informatique signifie l'analyse d'un système informatique après incident.

(77) Robert Erra, « The Malicious Flash Crash Attacks ou pourquoi il faudra peut-être ralentir les transactions électroniques », forum ATENA 2011, http://www.forumatena.org/files/8juin2011/Robert-Erra.pdf

(78) La page anglaise de *Wikipedia* est plus complète et plus nuancée que la page française : http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

(79) Voir http://www.lemonde.fr/technologies/article/2011/02/16/un-general-israelien-revendique-la-creation-du-virus-stuxnet_1481079_651865.html

l'écriture et le test d'un tel programme sont le fait de professionnels aguerris.

EXEMPLE 4 HFT : parfois la finalité est claire. L'objectif des marchés financiers est le profit. Mais personne ne parlera ici de cyber-conflit ou d'attaque délibérée. Il s'agit d'une bataille entre machines et plus précisément entre algorithmes délibérément obscurs dont les programmeurs sont, par ailleurs, très recherchés. La justification économique de ces programmes qui génèrent parfois 5 000 cotations en une seule seconde pour une même action reste à prouver. La conclusion de la présentation de ce cyber-incident propose quelques termes à retenir pour comprendre la prochaine crise : *High Frequency Trading* (HTF), *Quote Stuffing*, *Dark Pool*, *Crossing Networks*, *Iceberg Order* [*Wikipedia*: *Dark Liquidity Pool*], *Gaming*: *Dark pools are open to gaming, but it is a risky business* (*Wikipedia*), *Electronic Currency Network* (ECN). Une hypothèse malveillante n'est pas exclue, même s'il est très difficile dans un environnement aussi hermétique d'établir des preuves, comme le montrent les rapports[80] ou commentaires.

Les affrontements par machines interposées vont selon toute vraisemblance se généraliser. Elles entretiennent naturellement les 25 techniques de la désinformation. Même les mathématiques peuvent générer le chaos, comme le montrent les théories fractales. La sécurité des contenus en circulation (propriété, authenticité, traçabilité) et des calculs et traitements (transparence des opérations / secrets, signification des traitements, vérification en temps réel de la sémantique des calculs)[81] deviendront des enjeux majeurs de notre cyberdépendance. La difficulté de définir des mesures de sécurité adéquates autour des principes intangibles d'une défense en profondeur proactive, et d'une traçabilité des incidents inévitables dans un cyberespace où la sécurité absolue n'existe pas, relève des quatre ambiguïtés mentionnées. Comment faire pour se protéger contre une menace mal appréhendée ou non connue ?

Comprendre une cyber-agression et pouvoir la traiter juridiquement, le cas échéant, revient à lever au moins partiellement les quatre ambigüités décrites ici. Mais il ne faut jamais oublier que la réalité technique et même mathématique impose ses propres lois. Vouloir une chose et son contraire, arbitrer entre liberté, sécurité et facilité d'emploi[82] replace toujours l'homme au centre du cyberespace. Et c'est heureux !

Conclusion

La lutte contre la cybercriminalité est une composante essentielle d'une politique de défense et de sécurité des systèmes d'information. Le fonctionnement de nos sociétés modernes est dépendant, parfois à l'excès, de leur résistance aux agressions diverses et permanentes. La cyber-sécurité se gagne par une approche globale avec des défis de quatre ordres : juridique, géopolitique, technique et culturel. Nous avons essayé de montrer à travers la présentation et l'analyse des caractéristiques singulières des attaques dans le cyberespace que relever ces défis ne peut être le simple fait d'outils, aussi sophistiqués soient-ils, ou d'investigations à l'emporte-pièce, mais nécessite une coopération éclairée de l'ensemble des traitants, depuis une veille attentive jusqu'à la répression quand elle est opportune.

Prenant acte de l'évolution de la menace et de la multiplication des attaques informatiques de grande ampleur, le Gouvernement[83] a décidé d'adopter un ensemble de mesures visant à accélérer la montée en puissance du dispositif français de défense et de sécurité des systèmes d'information. Deux de ces mesures participeront de l'effort national de lutte contre la cybercriminalité. La création d'un « groupe d'intervention rapide » a pour objectif une capacité d'intervention sur les systèmes d'information de l'État et des opérateurs critiques pour réaliser trois grandes missions : rechercher et détecter les compromissions ; superviser les opérations de traitement d'incident ou de reconstruction des systèmes ; porter assistance à nos alliés en cas de crise informatique. La création d'un réseau d'alerte permanent, maintenu à jour et régulièrement validé par des exercices, facilitera les échanges d'informations techniques et opérationnelles utiles à la cybersécurité des opérateurs d'importance vitale.

• • • (80) Le rapport de la SEC est ici : http://www.sec.gov/news/studies/2010/marketevents-report.pdf
(81) Michel Riguidel, « Personnalisation de l'infrastructure et transparence du réseau », Forum ATENA 2011, http://www.forumatena.org/files/8juin2011/Michel-Riguidel.pdf
(82) Daniel E. Geer, ESSAY Cybersecurity and National Policy, Volume 1—7 avril 2011, Voir http://www.harvardnsj.com/wp-content/uploads/2011/01/Volume-1_Geer_Final-Corrected-Version.pdf
(83) Le Premier ministre a présenté, lors du Conseil des ministres du mercredi 25 mai 2011, une communication relative à la protection des systèmes d'information.

L'ANSSI

La lutte contre la cybercriminalité s'inscrit dans une politique globale de défense et de sécurité des systèmes d'information. Les missions des services spécialisés dans sa répression, qui ne seront pas décrits ici, s'inscrivent dans ce cadre national et international.

« Dans le cas d'une attaque informatique, la réactivité prime. Les attaques informatiques se déplacent à la vitesse du courant électrique, une vitesse proche de celle de la lumière. Dans certaines situations, il peut être utile de prendre des décisions rapidement, notamment pour éviter une trop grande infection.

Il faut, y compris pour des raisons juridiques, que l'État identifie clairement une autorité chargée d'édicter les règles au sein de l'administration, mais aussi vis-à-vis des opérateurs. Dans cette perspective, le Président de la République a décidé l'année dernière que la France se doterait d'une autorité de défense des systèmes d'information. Cette décision s'est concrétisée par le décret du Premier ministre du 11 février 2011, qui attribue à l'ANSSI la fonction d'autorité nationale de défense des systèmes d'information. En cette qualité et dans le cadre des orientations fixées par le Premier ministre, elle décide les mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et coordonne l'action gouvernementale.

Pour faire court et reprendre une formule de Francis Delon[84] : en cas d'attaque informatique majeure, l'ANSSI prend la main [...] »[85].

Ses missions

L'ANSSI a été créée en juillet 2009[86], sous la forme d'un service à compétence nationale. Elle 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. En plus de la sécurité des systèmes d'informations de l'État, l'ANSSI a une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale[87]. Elle contribue à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion.

La création de l'ANSSI est l'une des suites données à la publication, le 17 juin 2008, du Livre blanc sur la défense et la sécurité nationale[88]. Ce Livre blanc, retenant le risque d'une attaque informatique contre les infrastructures nationales comme l'une des menaces majeures les plus probables des quinze prochaines années, a mis en exergue l'impact potentiellement très fort de telles attaques sur la vie de la nation. Notre dépendance aux processus informatiques croît en effet sans cesse avec le développement de la société de l'information et l'utilisation de plus en plus poussée de l'informatique dans les processus essentiels de l'État et de la société. En conséquence, le Livre blanc annonçait la mise en place d'une capacité de prévention et de réaction aux attaques informatiques, et à en faire une priorité majeure de son dispositif de sécurité nationale. En particulier, dans le domaine de la défense des systèmes d'information, il soulignait la nécessité de disposer d'une capacité de détection précoce des attaques informatiques, et d'une organisation propre à contrer les attaques les plus subtiles comme les plus massives. Dans le domaine de la prévention, il proposait un recours accru à des produits et à des réseaux de haut niveau de sécurité, et la mise en place d'un réservoir de compétences au profit des administrations et des opérateurs d'infrastructures vitales.

Le centre opérationnel

L'ANSSI a notamment pour mission de détecter et réagir au plus tôt en cas d'attaque informatique, grâce à un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés aux attaques. Le Centre opérationnel de la sécurité des systèmes d'information (COSSI) assure la mise en œuvre de la fonction d'autorité de défense des systèmes d'information dévolue à l'ANSSI. Son action s'exerce en priorité au profit des administrations de l'État, ainsi

(84) M. Francis DELON, conseiller d'État, a été secrétaire général de la défense nationale de juillet 2004 à janvier 2010. Il a été nommé secrétaire général de la défense et de la sécurité nationale le 13 janvier 2010.

(85) Audition de M. Patrick Pailloux, directeur général de l'ANSSI, Assemblée nationale, Commission de la défense nationale et des forces armées, mercredi 1er juin 2011. Voir http://www.assemblee-nationale.fr/13/cr-cdef/10-11/c1011041.asp#P6_249

(86) Décret n°2009-834 du 7 juillet 2009 (Journal officiel du 8 juillet 2009). Elle est l'héritière d'une longue série d'organismes chargés d'assurer la sécurité des informations sensibles notamment de l'État : la Direction technique du chiffre (DTC), créée en 1943 à Alger ; le Service central technique du chiffre (STC-CH), qui lui a succédé à Paris en 1951 ; le Service central du chiffre et de la sécurité des télécommunications (SCCST), créé en 1977 ; le Service central de la sécurité des systèmes d'information (SCSSI) en 1986 ; la direction centrale de la sécurité des systèmes d'information (DCSSI) créée par le décret n°2001-693 du 31 juillet 2001 au sein du Secrétariat général de la défense nationale. Voir http://www.ssi.gouv.fr/

(87) L'« Instruction Générale Interministérielle relative à la sécurité des activités d'importance vitale » décrit le dispositif national. Voir http://www.circulaires.gouv.fr/pdf/2009/04/cir_1338.pdf

(88) Voir http://www.livreblancdefenseetsecurite.gouv.fr/

que des opérateurs d'importance vitale. Le COSSI assiste également les divers acteurs de la société de l'information, notamment par les alertes, les avis et les autres publications qu'il met en ligne sur le site internet du CERTA.

Le COSSI assure un service permanent de veille, de détection et d'alerte destiné à déceler les vulnérabilités susceptibles d'affecter la sécurité des systèmes d'information, à proposer les mesures de contournement nécessaires, et à détecter les attaques visant les systèmes d'information de l'État. En cas d'incident, il assiste les services concernés en termes de prévention, de détection, de protection et de réaction. En cas de crise, il prépare les mesures de défense nécessaires et coordonne leur mise en œuvre. Il assure, au niveau central, la planification des mesures de réponse aux attaques informatiques, notamment dans le cadre des plans VIGIPIRATE[89] et PIRANET (plan d'intervention de la famille Pirate dédié au cyberespace). Il organise des exercices afin d'évaluer les dispositifs techniques et organisationnels de prévention, de détection, de protection et de réaction mis en place, d'entraîner les personnels concernés et de mesurer le degré de préparation de la Nation.

Pour l'accomplissement de ses missions, le COSSI entretient des relations opérationnelles avec de nombreux organismes, notamment les autres centres français de SSI, publics ou privés, ses homologues étrangers, les industriels du secteur des technologies de l'information et des communications, les opérateurs de communications électroniques et les opérateurs d'importance vitale. Il dispose d'une capacité d'inspection et d'audit pour évaluer la sécurité des systèmes d'information des services de l'État et aider leurs responsables à en améliorer le niveau. Cette capacité peut également être mobilisée dans le cadre du soutien et du contrôle qu'exerce l'État sur les opérateurs d'importance vitale.

La défense des systèmes d'information

Espace de libertés, de partage et de développement économique, le cyberespace est, comme les espaces du monde matériel, un terrain d'affrontement. En temps de paix comme lors de conflits, les systèmes d'information qui composent le cyberespace français – qu'ils appartiennent à l'État, à des entreprises ou des institutions nationales – peuvent être victimes d'attaques émanant directement ou indirectement de puissances étrangères, de groupes terroristes ou d'activistes, décidés à atteindre notre pays dans sa vie quotidienne ou dans le fonctionnement de la vie démocratique, dans son économie, dans sa liberté de manœuvre. La perturbation ou la destruction de ces systèmes d'information, l'altération de la disponibilité ou la modification du comportement des processus qu'ils contrôlent, ou encore l'espionnage sont parmi les objectifs de telles attaques. Lorsque certains systèmes d'information de l'État ou les systèmes d'information de certains opérateurs d'importance vitale à la vie de la nation sont visés, la France est en situation légitime de mettre en œuvre tous les moyens nécessaires à la défense de ses systèmes d'information.

La lutte contre la cybercriminalité

L'ANSSI n'est pas un service de justice ou de police. Elle ne reçoit pas les plaintes, ni ne conduit aucune action particulière relative aux contenus illicites. Elle traite sur le plan technique et en premier ressort les incidents concernant l'administration et les opérateurs d'importance vitale. L'articulation avec les services spécialisés dans la répression du cybercrime se fait dans un deuxième temps à l'initiative du gestionnaire ou de l'autorité d'emploi du système d'information et de communication visé.

La dimension internationale

L'ANSSI entretient des relations avec ses homologues de nombreux pays, parmi lesquels notamment : le BSI en Allemagne (www.bsi.bund.de); le CESG au Royaume-Uni (www.cesg.gov.uk) ; la NLNCSA aux Pays-Bas ; la NSA (www.nsa.gov/ia/) et le DHS (www.dhs.gov/cyber) aux États-Unis et l'ENISA (www.enisa.europa.eu) de l'Union européenne. Elle participe aux négociations internationales, et notamment à la promotion de la confiance dans la société de l'information dans le cadre européen. Il existe des accords de reconnaissance mutuelle pour les produits certifiés, avec les homologues. La relation en matière de cyberdéfense a été notamment renforcée dans le cadre de divers accords bilatéraux.

* * *

• • • (89) Voir http://www.sgdsn.gouv.fr/site_rubrique98.html

Observations des membres du conseil d'orientation : Direction générale de la gendarmerie nationale

Les réseaux numériques ne constituent pas des zones de cyberconflits sauf si l'on considère les attaques perpétrée contre l'Estonie ou la Georgie. En fait tout est une question de finalité. Si dans le deuxième cas il y avait effectivement une action de guerre et donc de conflit entre deux États en revanche pour le cas de l'Estonie rien n'est certain. On sait simplement que des attaques venues de Russie sont à mettre au crédit de hackeurs agissant conjointement mais sans apporter la preuve que les actions étaient commanditées par un organisme étatique. On ne peut parler de cyberconflit que lorsque l'ordre d'attaque a été donné par un Etat. À défaut de ce justificatif, on ne peut qu'émettre une supposition.

Dans ces conditions, les réseaux numériques ne sont pas des champs de bataille militaires. Si tel était le cas, alors, comme dans un monde réel, chaque attaque sur les dispositifs numériques d'un État en utilisant des programmes informatiques malveillants constituerait un acte de guerre justifiant une déclaration de guerre au sens conventionnel du terme. Tout au plus, dans l'immédiat des perturbations peuvent être massives. Certes, plusieurs spécialistes français du renseignement sont également assez affirmatifs sur la volonté de certains groupes terroristes de concrétiser des cyber-attaques. Toutefois, on peut faire valoir qu'il ne saurait y avoir une destruction par un État d'une partie du système dans la mesure ou tout le monde a intérêt à le maintenir en fonctionnement afin de communiquer et cela dans l'intérêt de tous les pays y compris de celui qui attaque. Les mouvements terroristes n'ont pas davantage intérêt à y porter atteinte car cela serait contre productif au regard de la logique de communication allant jusqu'à la désinformation des personnes.

Dés lors, peut-on parler d'actes terroristes sur Internet comme certains en émettent l'idée. S'agissant d'un vecteur permettant la circulation de flux d'informations, il semble objectif d'écarter cette notion. Si la prise de contrôle du réseau permettait le cas échéant de prendre la main sur un avion sans pilote mais exclusivement manœuvrer à partir du réseau, nous pourrions envisager cette situation. Mais ce n'est pas le cas aujourd'hui. Dés lors Internet et terrorisme est en l'état de la technologie actuelle une notion à écarter même si l'on doit la garder à l'esprit. En revanche avec l'évolution du Web vers le 3.0, c'est-à-dire le web des objets la position pourra être revue

Le concept de Cyber-terrorisme est actuellement porté par la présidence polonaise de l'Union européenne dans le cadre des travaux mensuels du TWG (*Working Group on terrorism* - Europol). Ce projet n'a pas suscité grand intérêt de l'ensemble des délégations européennes, en particulier les grands pays ainsi que ceux qui ont été frappés par des actes terroristes au cours de ces dernières années.

D'une part, la quasi totalité des pays, dont la France, partagent l'analyse selon laquelle les organisations terroristes ne disposent pas actuellement des capacités pour organiser et mener des « Cyber-attaques » d'ampleur.

D'autre part, des questions se sont posées au sujet de la définition même du concept de « Cyber-terrorisme ». Le Cyber-espace est considéré comme un théâtre et les outils (Net, réseaux informatiques, etc...) comme des vecteurs susceptibles d'être utilisés par des terroristes au même titre que des explosifs, avions ou otages,etc...

Au reste il a été estimé que si le « Cyber-terrorisme » constituait une menace à ne pas négliger, les travaux initiés sur cette thématique pourraient faire doublon avec d'autres travaux en cours initiés depuis plusieurs années, et consacrés à la problématique globale de « Cyber-Criminalité » et/ou «cyber sécurité». L'inconvénient réside dans le risque d'une moindre prise en compte des individus ou groupes classés comme terroristes et représentant une menace réelle en terme de « cyber-attaque ».

La complexité de cette problématique conduit les acteurs à privilégier une approche «technique» liée à l'outil, aux réseaux sans distinguer le type de délinquance concernée.

Dans ces conditions, les objectifs poursuivis par les adversaires peuvent être :

Le jeu car il existe encore des individus qui s'y consacrent même s'ils sont de moins en moins nombreux.

Le mercantilisme (cybercriminalité avec des individus agissant seuls ou en groupes et pouvant aller jusqu'à l'organisation criminelle. L'objectif est de soutirer de l'argent aux victimes).

L'espionnage : Dans ce cas l'objectif poursuivi est la recherche d'informations par un État ou une entreprise (intelligence économique) ou le cas échéant l'injection d'informations par un État ou une entreprise à des fins économiques (IE et contrefaçon) ou politiques (désinformation).

Les réseaux numériques étant des vecteurs de communication, ils sont naturellement utile pour échanger de l'information comme cela a été le cas lors des attaques du 11 septembre par des acteurs terroristes, les organisations criminelles (Skype) pour échanger des informations sur par exemple l'organisation de transaction de produits stupéfiants avec la Colombie, enfin par les jeunes des banlieues pour se fixer des rendez-vous à l'exemple des manifestations de 2009.

Les atteintes portées à un système de traitement automatisé de données constituent dans la majorité des cas aujourd'hui un élément constitutif d'une infraction plus grave et non plus simplement une infraction individuelle et séparée.