N° 03/2012

recherches & documents

mars 2012

Cyber Dissuasion

Bruno Gruselle *Maître de recherche à la Fondation pour la Recherche Stratégique*

Bruno Tertrais *Maître de recherche à la Fondation pour la Recherche Stratégique*

Alain Esterle *Chercheur associé à la Fondation pour la Recherche Stratégique*

FONDATION *pour la* RECHERCHE STRATÉGIQUE

WWW.FRSTRATEGIE.ORG

Édité et diffusé par la Fondation pour la Recherche Stratégique
4 bis rue des Pâtures – 75016 PARIS

ISSN : 1966-5156
ISBN : 978-2-911101-68-7
EAN : 9782911101687

SOMMAIRE

Introduction

Dans un monde où près du tiers des habitants ont accès à internet et dans lequel la plupart des entreprises, des organisations et des États dépendent déjà largement des outils informatiques et des moyens de communication pour leur fonctionnement quotidien, la question de la sécurité numérique est devenue une préoccupation stratégique pour les États comme pour les entreprises et, dans une moindre mesure, les citoyens.

Certains incidents particulièrement médiatisés – comme la paralysie d'une partie des systèmes informatiques estoniens en 2007, les vols de données effectués sur des serveurs du Pentagone cette même année, mais également les dégâts réels ou supposés engendrés par le ver *Stuxnet* en 2010 sur des machines du programme nucléaire iranien – sont venus, au cours des dernières années, renforcer l'idée que les cyber-attaques devaient être placées au rang des menaces majeures pour la sécurité des États, des sociétés et de l'Économie globale.

Ainsi, les responsables policiers britanniques estiment qu'en 2007 **la seule fraude en ligne** générait au niveau mondial environ 52 milliards de livres pour les criminels[1]. Si les données fournies sur l'impact financier global de la criminalité numérique sont difficiles à vérifier – à la fois s'agissant d'estimations fournies par les principaux opérateurs du secteur de la sécurité numérique mais également dans la mesure où (1) les victimes omettent souvent de déclarer leur sinistre et (2) les outils statistiques des services de police s'avèrent généralement peu adaptés[2] –, la dépendance du secteur privé envers le numérique semble être établie, ainsi que le montre les nombreuses enquêtes menées auprès des principales entreprises aux niveaux national comme international.

Les estimations globales des pertes générées par le crime informatique et les vols de données illustrent toutefois l'ordre de grandeur de l'impact sur l'économie des risques numériques. Ainsi, la société de logiciels de sécurité McAfee estimait en 2009 le coût pour l'Economie mondiale du vol de données – incluant le détournement de propriété intellectuelle – à 1 000 milliards de dollars par an[3]. Dans son étude annuelle des activités criminelles à caractère numérique dans le monde, la société Norton estime que celles-ci causent des pertes s'élevant à 338 milliards de dollars dont 114 seraient obtenus de façon directe[4].

Le chiffre avancé par McAfee provient d'une enquête menée auprès de plusieurs centaines d'entreprises à caractère transnational et implantées aux États-Unis, en Europe et en Asie. Celle-ci conclut que chaque multinationale perd en moyenne, à travers le vol

---

[1] Association of Chief Police Officer of England, Wales and Northern Ireland, « ACPO e-Crime Strategy », August 2009, p. 2.

[2] Thierry Breton, « Chantier sur la lutte contre la cybercriminalité », rapport remis à monsieur le ministre de l'Intérieur, de la sécurité intérieure et des libertés locales, 25 février 2005, p. 6.

[3] http://information-security-resources.com/2009/02/14/businesses-lose-1-trillion-to-cyber-crime/

[4] Norton, « Global cybercrime costs USD 114 billion annually – study », September 8th, 2011.

de données, l'équivalent de 4,6 millions de dollars par an[5]. Ce qui représente un montant comparable au chiffre d'affaires mondial du crime organisé[6] et qui s'avère supérieur à celui du trafic de stupéfiants tel qu'il est estimé par l'Office des Nations Unies contre la Drogue et le Crime (UNODC)[7].

Au-delà des incidents ayant eu un impact sur l'Économie mondiale en entraînant des pertes, notamment financières, qui s'avèrent colossales, les États se montrent de plus en plus préoccupés par les risques de voir des attaques numériques atteindre leurs intérêts vitaux. Aux États-Unis, les intrusions sur les réseaux classifiés du Pentagone en 2008[8] ou encore les actions d'espionnage conduites contre des programmes majeurs d'armement, y compris le *Joint Strike Fighter*, ou contre des gouvernements alliés ont montré aux responsables américains la gravité du risque et les possibilités de voir exploitées des vulnérabilités au sein de systèmes considérés comme vitaux pour les opérations militaires. Globalement, les services américains considèrent que les réseaux gouvernementaux et les systèmes critiques font l'objet de plus de 1,8 milliard d'attaques mensuelles de sophistication plus ou moins importante[9].

En 2011, les révélations concernant la conduite par la Chine d'une campagne d'espionnage à l'échelle mondiale ont à nouveau illustré – après la mise à jour du réseau « *Ghostnet* » opéré par l'Armée Populaire de Libération – la réalité des craintes américaines. L'ampleur de la campagne chinoise et la variété des cibles – qu'il s'agisse d'entreprises, de gouvernements ou d'organisations internationales – ainsi que les moyens qui y ont été consacrés en font en effet une opération sans précédent en termes de quantité d'information obtenue[10].

Or, face aux risques informatiques connus, fonder sa sécurité numérique sur des solutions uniquement défensives s'avère de plus en plus inadapté. D'une part, l'asymétrie intrinsèque entre l'efficience des armes numériques et les moyens de protection et de défense s'avère fournir aux agresseurs un avantage de plus en plus important alors que les investissements de sécurité ne font que croître pour traiter un spectre finalement limité de menaces. D'autre part, les agresseurs potentiels ne se trouvent pas soumis à des risques suffisants pour les dissuader de conduire des actes dont les conséquences sont susceptibles d'être de plus en plus significatives. Au contraire, les vulnérabilités existantes et la sensation d'impunité semblent inciter les acteurs malveillants à multiplier leurs opérations à des échelles et avec des objectifs souvent très ambitieux.

---

[5] McAfee, « Unsecured Economies: protecting vital information, The first global study highlighting the vulnerability of the world's intellectual property and sensitive information », 21 January 2009, p. 3.

[6] United Nations Office on Drugs and Crime, « Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes », October 2011, p. 7. Le rapport de l'UNODC estime que l'argent généré par les activités criminelles transnationales représente 1 600 milliards de dollars par an soit 2,7 % du PIB mondial.

[7] http://www.unodc.org/

[8] William Lynn III, « Defending a New Domain », *Foreign Affairs*, Sep/Oct2010, Vol. 89, Issue 5.

[9] Center for New American Security, « America's Cyber Future: Security and Prosperity in the Information Age », June 2011, p. 7.

[10] Dmitri Alperovitch, « Revealed: Operation Shady RAT », McAfee, August 2011, p. 2.

En l'état, l'exploitation grandissante des failles des systèmes informatiques et des réseaux numériques et l'aggravation des conséquences qui peuvent en découler – qu'il s'agisse d'infrastructures critiques, militaires ou gouvernementales – conduisent à s'interroger sur le fait que certaines actions malveillantes peuvent s'apparenter à des actes de guerre et dès lors nécessiter des représailles, ces dernières pouvant être numériques voire même physiques. De fait, dans le récent document de stratégie internationale pour le cyberespace, la Maison Blanche a souligné le droit à l'autodéfense face à des actions se déroulant dans le domaine numérique[11].

Ces éléments conduisent à s'interroger sur la possibilité de mettre en place, dans le contexte plus large d'une révision des stratégies de cyber-défense, les outils, les moyens et les organisations dont la finalité serait ***de dissuader les agresseurs potentiels de causer des disruptions massives*** aux sociétés numériques. L'objectif devrait être finalement de passer d'une stratégie de défense statique fondée sur des « lignes Maginot » numériques pour créer une approche comprenant un spectre plus large de solutions de sécurité.

Ainsi, de nombreux pays ont annoncé plus ou moins ouvertement leur volonté de faire évoluer leurs capacités de cyber-défense (en se dotant de commandement *ad hoc* et de moyens de riposte), afin de répondre aux attaques, d'où qu'elles viennent, qui pourraient menacées les infrastructures indispensables au bon fonctionnement de leurs secteurs d'activité d'importance vitale.

Parmi les évolutions envisageables, la possibilité de conduire des opérations offensives contre des personnes ou des organisations susceptibles de commettre des actions malveillantes mérite donc d'être explorée. Il s'agirait en particulier de faire peser sur les attaquants potentiels la menace de représailles suffisamment significatives pour influer sur leur calcul stratégique et ainsi peut être les dissuader d'engager les actions les plus destructrices.

L'élaboration d'une telle stratégie de cyber-dissuasion s'inscrit en définitive dans le besoin de redéfinir les stratégies des pays occidentaux en matière de sécurité numérique. Elle passe donc par une réflexion sur les moyens qui doivent être développés pour répondre aux enjeux de sécurité actuels et futurs dans le domaine cyber. Elle nécessite également de rebâtir la philosophie qui sous-tend les approches des problématiques de sécurité numérique de façon notamment à répondre au besoin de coordination opérationnelle entre les diverses parties prenantes : acteurs privés, administrations, forces de sécurité et public au sens large.

Cette étude propose ainsi des pistes permettant de définir une stratégie de cyber-dissuasion en s'intéressant à la fois aux aspects doctrinaux mais également aux problématiques fonctionnelles, organisationnelles et techniques. Dans ce cadre, elle vise à préciser les outils qui pourraient être utilisés pour permettre le fonctionnement d'un système de cyber-dissuasion.

[11] White House, « International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World », May 2011, p. 10.

Les vulnérabilités de l'espace numérique et les risques associés sont déjà importants et devraient s'aggraver à l'horizon 2020

Il est nécessaire d'établir le degré de gravité des risques numériques, les vulnérabilités exploitables et les perspectives de leur développement

Le degré de dépendance de notre société – en termes économiques, sociaux ou de sécurité – envers les outils informatiques et de communication et, singulièrement, envers internet en tant que fédérateur des solutions numériques et comme colonne vertébrale d'échange entre les divers objets connectés et les personnes physiques ou morales, est d'ores et déjà important et il va aller en augmentant.

Même si les problématiques de sécurité sont prises en compte dans le développement des futurs systèmes et solutions numériques et dans celui de l'Internet du futur, ces derniers resteront vulnérables face à des acteurs malveillants cherchant à exploiter les failles de ces outils complexes pour leur bénéfice, pour neutraliser durablement des processus ou des opérations, pour dérober des données ou encore, pour causer des dégâts aux personnes ou aux biens.

Si l'on considère souvent que les attaques informatiques sont avant tout un risque pour le secteur privé – dans la mesure où les services ou les moyens de l'État sont finalement peu attaqués en comparaison des acteurs privés – cette logique cesse d'être applicable quand l'on considère la multitude de réseaux et moyens vitaux opérés par des acteurs non étatiques (eau, électricité, transports) ou encore le coût pour l'économie des activités criminelles dans le domaine numérique[12].

Ainsi, si les risques numériques n'ont pas forcément de conséquences existentielles pour le pays, ils sont toutefois de nature à créer des perturbations graves qui peuvent être ponctuelles ou davantage discrètes/distribuées dans le temps. A plus long terme, avec le développement de l'Internet des objets et la montée en puissance du *cloud computing* et des nouveaux usages d'Internet par exemple, ***certains actes malveillants peuvent venir menacer la société de façon plus générale en affectant de manière simultanée une part plus importante de la population ou des aspects plus vitaux du fonctionnement de la Nation.***

Parmi les intérêts qui pourraient être couverts par une posture de cyber-dissuasion, il faudrait vraisemblablement inclure :

- ***Les moyens d'infrastructure*** **et les applications critiques** pour le fonctionnement d'Internet : la fiabilité du réseau mondial au niveau national, déjà nécessaire aujourd'hui, devrait devenir indispensable à moyen et à long termes au fur et à mesure de l'intégration de nouvelles applications ; au moins à court terme, l'Internet des objets et l'informatique en nuage.

- ***Les systèmes informatiques*** permettant le fonctionnement, la maintenance et la gestion des infrastructures critiques du pays : grille électrique (distribution, transport, gestion), réseaux de transport de personne et de biens, réseaux de distribution

[12] Eric Sterner, « Retaliatory Deterrence in Cyberspace », *Strategic Studies Quarterly*, Spring 2011, p. 64.

de biens de première nécessité (en particulier eau), télécommunications gouvernementales (y compris les systèmes de commandements, de communication et de contrôle à vocation militaire), etc. La sécurité, la protection et la résilience de ces systèmes sont d'ores et déjà considérées par les instances nationales de planification de sécurité et de défense comme un impératif.

➡ ***Certaines données ou informations*** dont la divulgation ou l'utilisation seraient de nature à compromettre la sécurité de nos ressortissants, celle de nos forces ou du territoire national. Sur ce point, il convient d'être extrêmement prudent sur la nature des informations dont le pillage serait couvert par la manœuvre de dissuasion. En effet, le vol de données s'avère être l'un des crimes les plus banals dans le domaine numérique.

Les menaces pesant sur l'espace numérique ont d'ores et déjà des conséquences de sécurité importantes

Pourtant, force est de constater que les risques associés à l'emploi d'Internet n'affectent en rien son taux de croissance. L'accroissement simultané des vulnérabilités et des menaces est analysé par les autorités responsables des politiques de cybersécurité et les grandes entreprises fournisseuses d'outils et services de sécurité. Tous les systèmes d'échanges d'informations électroniques sont vulnérables et ils sont soumis à des attaques à partir du moment où leur marché se développe : les logiciels malveillants se diversifient et un nouveau marché des outils d'attaques – comme par exemple, la location de réseau d'ordinateurs zombis – se développe pour exploiter les failles détectées de ce système.

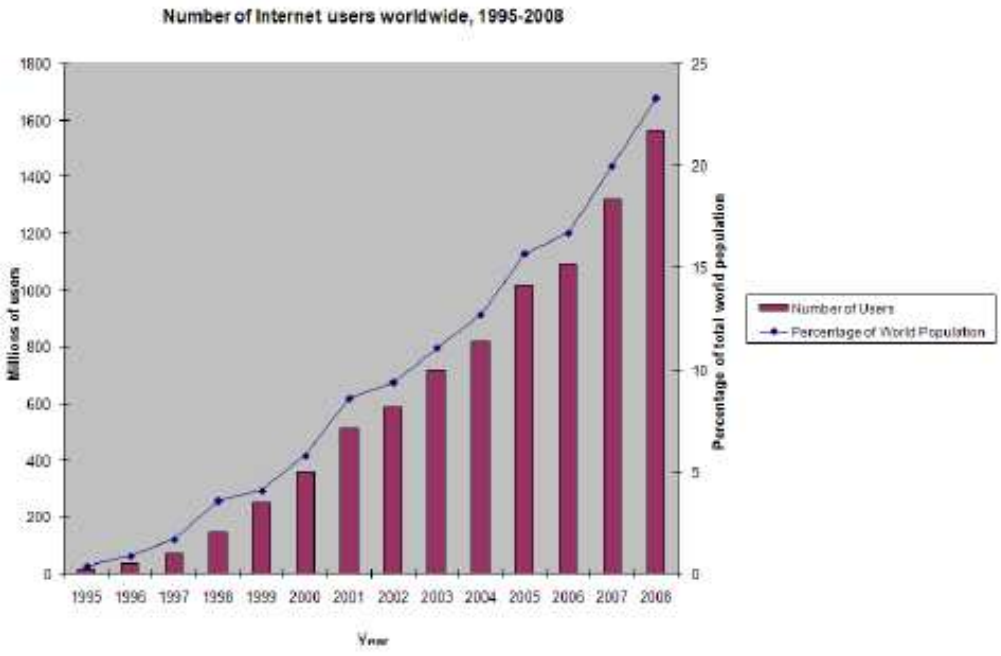


Figure 1 : Croissance du nombre d'usagers d'Internet (source : Internet World Stats)

La figure suivante offre un bilan graphique récent du paysage des cyber-menaces. Il apparaît clairement que l'ensemble des menaces connaît un développement significatif qui correspond *a priori* avec l'accroissement du degré de pénétration des technologies de l'information au niveau global.

Le coût des incidents et attaques affectant les systèmes d'information est bien sûr difficile à évaluer, faute d'une ***méthodologie uniforme et du fait d'une forte incertitude sur le taux des incidents déclarés par rapport aux incidents reconnus.*** Il existe aussi des attaques qui passent inaperçues ou qui ne sont pas détectées ou identifiées comme telle par négligence ou du fait de l'absence de compétences « sécurité » au sein de l'organisation concernée. Il est donc impossible d'établir une valeur absolue des pertes financières résultant des cyber-attaques, même si l'estimation la plus couramment admise est que le coût des dommages affectant les systèmes d'information est comparable au chiffre d'affaires mondial du crime organisé[13] et vraisemblablement du même ordre de grandeur, comme nous l'avons vu, que les bénéfices provenant du trafic de stupéfiants.

[13] http://www.fbi.gov/about-us/investigate/organizedcrime/overview

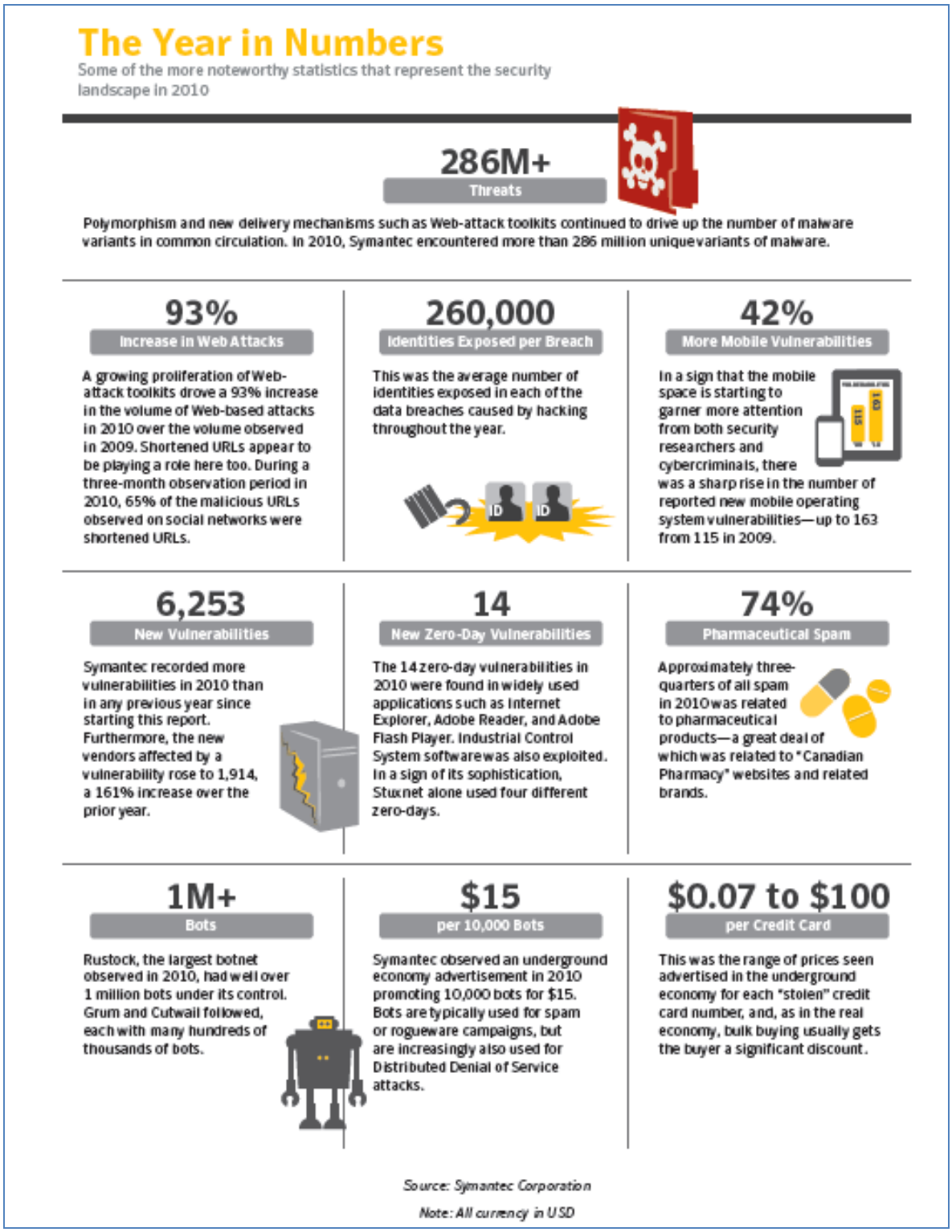


Figure 2 : Les principales menaces en 2010 en chiffres (source : Symantec)

Il est néanmoins intéressant de suivre l'évolution dans le temps des pertes financières associées à un même corpus. Les plaintes déposées aux États-Unis et ayant conduit à une poursuite judicaire fournissent, dans cette perspective, des données utiles. Elles suggèrent en effet une croissance d'un ordre de grandeur par décennie, grosso modo comparable au taux de croissance de la pénétration mondial d'Internet.

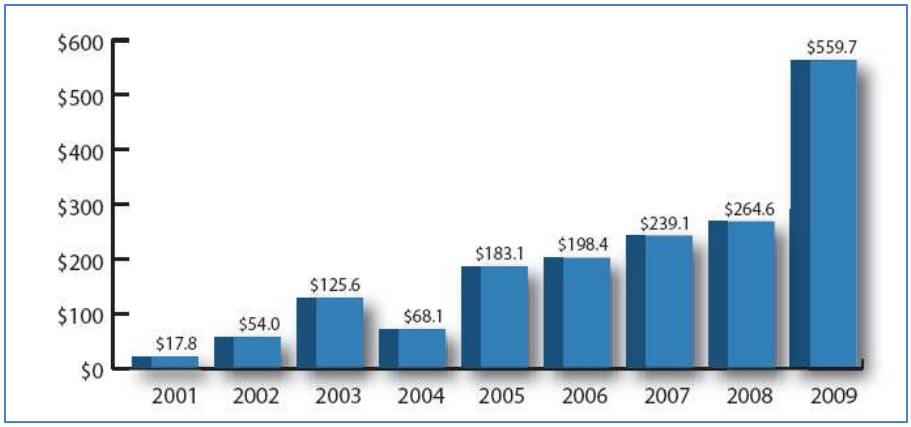


Figure 3 : Yearly Dollar Loss (in millions) of Referred Complaints in the US
(source : Internet Crime Complaint Center 2009 Report[14])

A la lumière des données disponibles, ***il existe donc apparemment une corrélation entre la montée en puissance des usages des technologies de l'information, en particulier d'Internet, l'accroissement des actes malveillants et les pertes financières associées***. En creux, cette corrélation suggère que les bénéfices – économiques, sociaux, culturels... – qui sont tirés de l'utilisation grandissante des systèmes numériques sont considérés par les utilisateurs comme supérieurs aux pertes causées par les risques et vulnérabilités qui leur sont intrinsèquement liés.

Ce constat amène finalement à s'interroger sur le besoin de mettre en place une dissuasion numérique. Comme nous l'avons évoqué, la volonté affichée de gouvernements de plus en plus nombreux de développer des capacités étatiques offensives crée les conditions d'un changement profond du niveau (et de la nature) de la menace. C'est bien ce problème spécifique et nouveau qui appelle une réponse sous la forme de l'élaboration d'un dialogue dissuasif à la fois avec les acteurs étatiques mais, éventuellement, avec les groupes ou les personnes qui commettent pour leur propre profit ou, éventuellement, au profit d'États tiers, des actes numériques malveillants.

[14] http://www.ic3.gov/media/annualreports.aspx

Les acteurs malveillants de l'espace numérique sont nombreux et leurs motivations appartiennent à des ensembles diversifiés

On peut distinguer grossièrement trois catégories d'acteurs qui dans le domaine numérique exploitent les failles et les vulnérabilités des systèmes pour en tirer un profit, créer des effets néfastes pour les utilisateurs ou, dans certains cas, faire valoir leur position ou leur point de vue.

Aux cyber-attaquants classiquement répartis en fonction de leurs motivations (performance technique, financement, idéologie, pression sur autrui), il convient maintenant de rajouter le personnel militaire entraîné pour pouvoir mener des actions offensives dans le cyberespace.

Encadré 1 : Catégorisation des acteurs

- ***Les cyber-activistes*** *utilisent internet pour faire valoir leurs positions idéologiques qu'elles soient politiques, religieuses ou éthiques. Leurs modes d'action restent souvent toute à fait légaux (blogs, forums publics ou privés...), mais peuvent aussi inclure des campagnes de dénonciation utilisant des moyens illégaux (défiguration de sites, dénis de services). Depuis 2010, Wikileaks a développé un nouveau mode d'intervention avec la mise en ligne systématique de documents protégés, voire classifiés, et le groupe Anonymous a engagé des campagnes de hacking de sites officiels ;*

- ***Les cybercriminels*** *exploitent les réseaux et les systèmes informatiques pour en tirer un gain financier direct ou indirect : vols de données, espionnage industriel, sabotage, contrefaçon de matériel électronique ou de logiciels*[15]*. Le développement de ce type d'activité donne lieu à une division du travail avec des mécanismes bien rodés de blanchiment d'argent*[16] *;*

- ***Les cyber-terroristes*** *utilisent le réseau pour recruter, préparer des actions spécifiques ou encore communiquer à des fins opérationnelles et ceci de façon relativement discrète, même si on ne peut écarter la possibilité, non encore avérée, de les voir viser les outils informatiques des entreprises afin, par exemple, de mener une action de sabotage avec des effets de grande ampleur (système financier, réseaux critiques/vitaux ;*

- ***Les cyber-guerriers*** *sont les membres des services mis en place par des États pour conduire des actions offensives (espionnage, sabotage, neutralisation de systèmes informatiques) contre des cibles désignées par leur gouvernement mais qui travailleraient également de façon continue à espionner à la fois les acteurs publics et privés pour obtenir des informations et des savoir-faire protégés par le secret.*

[15] Club de la Sécurité de l'Information Français, « Panorama 2008 de la cybercriminalité », pp. 76-94.

[16] Voir notamment « Les marchés noirs de la cybercriminalité », CEIS, juin 2011

Cette classification doit cependant être utilisée avec précaution car, dans la pratique, un événement spécifique peut très bien impliquer des groupes et acteurs de catégories et motivations différentes qui se trouvent mobilisés autour d'un objectif commun. Comme de nombreux indices le laissent à penser, ce fut, par exemple, le cas lors des attaques contre l'Estonie et la Géorgie[17] en 2007 et 2008. La collusion, en Chine et en Russie, entre des structures gouvernementales voire militaires et des groupes militants pour mener des attaques à l'encontre de pays étrangers a été récemment analysée en détail par Alexandre Klimburg[18].

Plusieurs facteurs accroissent la vulnérabilité des outils nécessaires au fonctionnement de l'espace numérique

La dépendance grandissante des chaînes d'approvisionnement envers des solutions d'origine asiatique crée des vulnérabilités spécifiques

La fabrication d'outils logiciels, de matériels et de composants informatiques est devenue depuis plusieurs années la responsabilité quasi-exclusive de sociétés et d'entreprises implantées en Asie. Il convient notamment de souligner que les plus grands fondeurs de semi-conducteurs sont chinois et taïwanais[19].

Hors d'un cadre soigneusement contrôlé de bout en bout – c'est-à-dire depuis le composant de base, jusqu'au système assemblé et à l'installation des logiciels –, il n'y a pas de méthode permettant de vérifier à coup sûr qu'un logiciel ou un composant n'a pas été « piégé » au moment de son développement. Or, s'il existe, un tel piège pourra dans des conditions prédéfinies déclencher une attaque, éventuellement de grande ampleur, sans que l'auteur de l'agression n'est besoin de donner d'instructions complémentaires.

En 2006, le FBI a détecté la production par la Chine de routeurs CISCO contrefaits et vendus sur le marché américain sous l'appellation CISCO. Outre les conséquences de la fraude économique, cet événement montre l'existence d'une menace spécifique liée à la fiabilité des chaînes d'approvisionnement. La possibilité d'implanter des chevaux de Troie dès la phase de production des composants de base des systèmes d'information montre que les grands fournisseurs occidentaux de solutions numériques sont d'ores et déjà vulnérables dans ce domaine.

La prise de contrôle en 2005 par la société chinoise Lenovo de la division « *personal computer*/PC » d'IBM[20] illustre également le fait que le niveau de dépendance global des utilisateurs de solutions numériques envers des solutions qui seraient uniquement d'origine asiatique et singulièrement chinoises risque de continuer à s'aggraver.

[17] US Cyber Consequences Unit, « Overview of the Cybercampaign against Georgia in August of 2008 », August 2009, p. 3.

[18] Alexandre Klimburg, « Mobilizing Cyber-Power », *Survival*, Volume 53, Issue 1, January 2011.

[19] http://fr.wikipedia.org/wiki/Fonderie_ %28 %C3 %A9lectronique %29

[20] http://www.presence-pc.com/actualite/Lenovo-rachete-IBM-9669/

A - Concentration du marché

L'évolution du marché des télécommunications est marquée depuis plusieurs années par des opérations de concentration verticale (e.g. rachat de *Skype* par *Microsoft*). En effet, les grands industriels du secteur cherchent à présenter à leurs utilisateurs une offre globale de communication, d'accès à des contenus et à des services « clés-en-mains ». Le développement de l'informatique en nuage devrait confirmer cette tendance à moyen terme.

In fine, l'industrie informatique pourrait de rassembler en un nombre réduit de pôles industriels (Google, Microsoft, Apple...), chacun étant à même de fournir une palette de produits et services, qui devront vraisemblablement faire l'objet d'une certification « maison » pour fonctionner avec les divers systèmes d'exploitation[21].

Une telle réorganisation du marché avec un effet de silos pourrait faire obstacle à des migrations éventuelles et réduire la flexibilité de l'approvisionnement. Elle renforcerait aussi les problèmes de dépendance et les risques inhérents à toute chaîne d'approvisionnement non contrôlée.

B - Développement des capacités numériques de la Chine

Le paysage industriel est aussi marqué par la croissance spectaculaire des capacités de recherche et d'industrialisation chinoises : rachat de la production d'ordinateurs IBM par Lenovo, mise au point du deuxième superordinateur au monde en termes de capacités de calcul – *Milky Way One*, 1 000 milliards d'opérations à la seconde –, couverture de 60 % de l'activité nationale par le navigateur chinois *Baidu*, concurrent de Google, etc.

L'équipementier des télécommunications grand public Huawei affiche aussi une croissance soutenue de l'ordre de 20 % par an, avec un chiffre d'affaires de 16 milliards d'euros et un résultat net de 2 milliards en 2009. La stratégie du groupe est largement tournée vers l'exportation et la coopération internationale. Il a effectivement noué des partenariats avec 45 des 50 plus grands opérateurs mondiaux. Il a également créé une filiale commune avec Symantec et porté un projet de centre de R&D qui serait implanté en France.

Selon certaines sources, Huawei s'oriente vers une forte rationalisation technique. Il s'engage dans les services d'informatique en nuage, mais en se libèrant des lourdeurs inhérentes aux systèmes en concentrant dans un même rack l'ensemble des fonctions et sous-ensembles de gestion de réseau (routeur, *switch*, hébergeur). Ce mode *all-in-one* se traduit par une décroissance de la production de hardware et le transfert de nombreuses fonctions vers des solutions logicielles, plus souples à configurer et à faire évoluer. La même approche prévaut pour le passage d'une génération à l'autre dans le domaine des télécommunications civiles (3G et 4G utilisant le même hardware).

Ceci n'empêche pas des industriels européens de continuer à pénétrer le marché chinois à l'instar d'Alcatel-Lucent (ou plutôt sa filiale *Alcatel-Lucent Shanghai Bells*) qui a remporté en juin 2011 le contrat de China Telecom, premier opérateur mondial avec 120 millions d'abonnés, pour le transfert du réseau commuté au réseau IP dans 6 provinces.

[21] Voir par exemple la politique d'Apple Inc. en matière de dissémination d'applications.

Cette évolution des télécommunications grand public s'accompagne d'une évolution semblable pour les produits de sécurité et les équipements sécurisés. Les propositions chinoises qui, il y a quelques années encore, étaient généralement 50 % moins chères que les produits européens mais de qualité médiocre, présentent aujourd'hui une qualité comparable tout en demeurant 10 % en dessous du prix du marché. Elles deviennent dès lors davantage compétitives sur les marchés en Europe[22].

Au total, les mutations industrielles laissent envisager une concentration des acteurs, ***une concentration de l'offre et un transfert vers la Chine de pôles majeurs d'activités.*** *Ceci devrait accentuer les enjeux en matière de contrôle des chaînes d'approvisionnement avec le besoin d'une politique incitative et ciblée pour préserver un minimum de produits fiables sur l'ensemble du champ souverain.*

Plusieurs pays émergents portent une attention spécifique aux questions d'actions offensives dans l'espace numérique

Les puissances émergentes considèrent d'abord le cyberespace comme un champ de croissance économique exceptionnel et un accélérateur industriel et technique dans de multiples secteurs.

Mais certains le perçoivent également comme un risque pour les régimes politiques en place. Ceci se traduit généralement par la mise en place de contrôles et de barrières visant à contrôler l'accès et les utilisations d'Internet (Iran, Chine). Ils y voient aussi un enjeu géopolitique majeur pour l'évolution des relations internationales. C'est sans doute dans cette perspective qu'il faut apprécier la décision récente des BRICS[23] de construire un réseau fibré sous-marin contournant les États-Unis.

Certains de ces pays pratiquent ainsi des politiques visant à contrôler les points d'accès à Internet en établissant une passerelle unique. Cette approche est bien sûr en contradiction directe avec le schéma d'un Internet ouvert mais peut avoir un double avantage de politique interne (contrôle du contenu des informations transfrontières) et de politique externe (défense avancée vis-à-vis d'éventuelles attaques logiques, dans le cadre d'un schéma de défense en profondeur).

Au-delà de la surveillance et du contrôle d'Internet, la politique de l'Armée Populaire de Libération chinoise en matière numérique se développe autour de capacités offensives destinées à des activités de cyber-espionnage comme, vraisemblablement, à des actions visant à neutraliser ou à paralyser temporairement les moyens informatiques adverses. Depuis 2006, plusieurs événements ont montré l'implication des services chinois dans plusieurs affaires d'espionnage visant des systèmes occidentaux : États-Unis, Allemagne[24], Organisations des Nations Unies... Les analyses effectuées par les

[22] Discussion personnelle avec des responsables de la DGA (note d'Alain Esterle).

[23] Brésil, Russie, Inde, Chine, Afrique du Sud, troisième réunion à Sanya (Chine) le 14 avril 2011.

[24] Au point de conduire à des réactions de la Chancelière et du gouvernement vis-à-vis des autorités chinoises. http://news.softpedia.com/news/Germany-Attacks-China-For-Starting-The-Cyber-War-68994.shtml

entreprises de sécurité numérique semblent indiquer l'existence d'une – voire de plusieurs – opération globale d'espionnage informatique visant les gouvernements étrangers, les multinationales ainsi que certaines organisations globales[25].

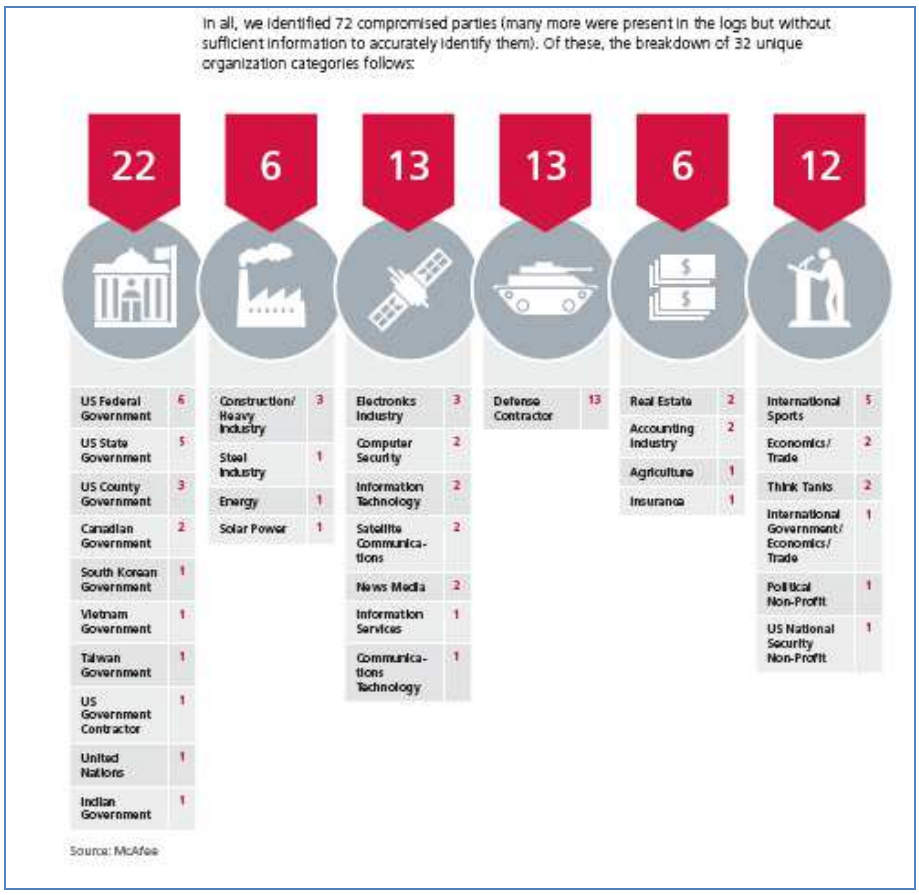


Figure 4 : Les opérations d'espionnage chinoises auraient atteint 72 cibles depuis 2006 permettant de voler des milliards d'octets de données (Source : McAfee)

La politique numérique de la Chine mise sur l'appropriation des technologies de l'information et des communications à la fois dans une logique de gain économique mais également pour fonder une stratégie de guerre de l'information dans laquelle les moyens mis à disposition de l'armée populaire sont utilisés pour infiltrer les systèmes informatiques connectés à Internet et ainsi faire peser sur les États – en particulier occidentaux – et les utilisateurs une menace permanente pour la sécurité de leurs infrastructures, la confidentialité de leurs échanges et la sureté des données stockées[26]. De ce point de vue, la Chine dispose d'ores et déjà d'un outil de cyber-dissuasion qui s'avère être également un moyen de pratiquer des activités d'espionnage à une échelle globale.

[25] Dmitri Alperovitch, « Revealed: Operation Shady Rat », McAfee White Paper, July 2011.

[26] Magnus Hjortdal, « China's Use of Cyber Warfare: Espionnage meets Strategic Deterrence », *Journal of Strategic Security*, Volume IV Issue 2 2011, pp. 1-24.

Les risques internes aux organisations constituent une source préoccupante de vulnérabilité numérique malgré une prise de conscience générale des risques associés aux outils informatiques

Sans qu'il soit possible d'établir en la matière une statistique rigoureuse, il est couramment admis qu'une proportion non négligeable des attaques proviendrait de personnes internes à l'organisme en charge ou connecté au réseau infecté. Qu'il s'agisse d'actions intentionnelles ou de négligences, elles constituent une forme de vulnérabilité permanente qui est renforcée par la faiblesse de la culture en sécurité des systèmes d'information au sein de la plupart des entreprises et des organisations gouvernementales.

Bien que l'importance du risque numérique pour le fonctionnement des entreprises et des organisations soit généralement reconnue, les budgets consacrés à la sécurité informatique sont souvent inadaptés pour faire face au niveau de risque encouru.

Au sein du budget consacré par les entreprises aux systèmes d'information, la sécurité numérique représente une part hétérogène allant de 1 % à plus de 6 %[27]. De façon générale, 56 % des chefs d'entreprise interrogés lors d'une enquête menée en 2009 indiquent que la part du chiffre d'affaires consacrée à la sécurité informatique est inférieure ou égale à 1 % du chiffre d'affaires. Seuls 10 % affirment consacrer plus de 2 % de leur chiffre d'affaires à la sécurité numérique. Enfin, une forte proportion n'a pas une vision claire sur les investissements en la matière : 34 % des interrogés concèdent ne pas connaître la part du chiffre d'affaires consacrée à cette activité[28].

Pourtant, la quasi-totalité des chefs d'entreprise considèrent que les dispositifs de sécurité informatique constituent une précaution indispensable. Plus de 80 % estiment que ceux-ci ne constituent pas un frein à la productivité[29]. Ces proportions sont à peu près les mêmes en ce qui concernent les salariés[30]. Pourtant les investissements réels en matière de sécurité numérique sont loin de refléter cette prise de conscience apparente.

Mais la prise en compte de la nature des risques est encore inadéquate au regard de l'évolution rapide des vulnérabilités. La sécurité des ordinateurs de bureau et des réseaux d'entreprise est d'ailleurs souvent limitée au déploiement de solutions basiques qui s'apparentent à des « lignes Maginot » numériques.

Ainsi, l'usage d'antivirus, de pare-feux et de logiciels anti-spam s'est largement généralisé dans l'univers économique tout comme dans le monde institutionnel. Mais les organisations privées comme publiques peinent encore à adopter des mesures de sécurisation spécifiques, davantage contraignantes – chiffrement des données, authentification, contrôle d'accès – qui permettent de mieux gérer les risques d'incidents provenant de l'intérieur du réseau.

[27] CLUSIF, « Menaces informatiques et pratiques de sécurité en France, Edition 2008 », 2008, p. 13.

[28] TNS-SOFRES, « l'insécurité numérique des entreprises – synthèse », novembre 2009.

[29] TNS-SOFRES, « L'insécurité numérique des entreprises – volet chefs d'entreprises », novembre 2009, p. 47.

[30] TNS-SOFRES, « L'insécurité numérique des entreprises – volet salariés », novembre 2009, p. 45.

Le besoin de sécurité est également encore largement sous-estimé pour certains équipements nomades – *smartphones*, ordinateurs portables et tablettes, clefs USB – qui ne sont que très rarement équipés de solutions de sécurité propres et constituent des points d'entrée vulnérables dans les systèmes d'information des sociétés[31]. De la même façon, les données présentes sur les postes individuels sont rarement chiffrées alors même que l'enquête du CLUSIF montre que ces informations font souvent l'objet de pertes ou de vols[32].

Les salariés considèrent que l'utilisation de clefs USB personnelles ou de leur messagerie personnelle constitue des pratiques à risques pour l'entreprise, comme l'a montré le mode de propagation du code malveillant qui avait infecté les réseaux du Pentagone en 2008. Pourtant, la plupart indiquent que le niveau de protection informatique dont ils disposent est suffisant pour les protéger de la plupart des menaces[33]. La possibilité d'accéder en permanence à leurs données personnelles comme professionnelles avec des ***outils et des logiciels similaires si ce n'est identiques constitue pour les salariés et les fonctionnaires une attente vis-à-vis de leurs employeurs***. Les politiques de sécurité prennent encore mal en compte le fait que les évolutions des usages des technologies de l'information ont conduit à multiplier les vulnérabilités internes. Elles se sont d'ailleurs notamment accrues pour les réseaux qui ne sont pas directement connectés à Internet et où une intervention humaine est nécessaire pour introduire au sein du réseau un logiciel malveillant.

La stabilité macroscopique actuelle du réseau et des systèmes informatiques ne semble pas devoir être remise en cause

De nombreux experts[34] considèrent comme peu probable qu'une cyber-attaque puisse à elle seule se propager à grande échelle dans l'Internet et provoquer son effondrement[35]. Actuellement, l'Internet est doté de suffisamment de nœuds de haute connectivité pour qu'en cas de rupture d'un nombre quelconque de nœuds distribués de façon aléatoire, le réseau mondial reste opérationnel.

En revanche, une attaque ciblant spécifiquement 5 % des nœuds à haute connectivité pourrait provoquer un effondrement de l'Internet en une série d'îlots, chacun interconnectant un maximum d'une centaine de calculateurs entre eux[36].

---

[31] En 2006 et 2007, il semble que les campagnes de piratage organisées contre des machines du DoD (et de la NDU), vraisemblablement par les services Chinois, ait été rendu possible par l'introduction d'un cheval de Troie placé sur une clef USB dans le réseau militaire américain.

[32] La compromission de données par des personnes appartenant aux entreprises, de façon volontaire ou pas, constituent l'une des préoccupations majeures des grands opérateurs du monde numérique. Entretiens, novembre 2009.

[33] TNS-SOFRES, « L'insécurité numérique des entreprises : synthèse », novembre 2009.

[34] Michel Riguidel, « Les technologies numériques du futur : Nouvelles menaces, nouvelles vulnérabilités », *Cahiers de la sécurité No. 6*, Institut d'Etudes Politiques de Lyon, 2008.

[35] L'attaque de 2003 contre les 13 serveurs DNS racine et la mise hors jeu momentanée de 8 d'entre eux, en réduisant localement l'activité mais sans empêcher un rétablissement rapide.

[36] « Future Global Shocks », OECD Review of Risk Management Policies, OECD, 2011

L'évolution future des pratiques numériques et des outils associés est susceptible de modifier les enjeux et les vulnérabilités dans l'espace numérique

Trois facteurs sont de nature à influencer les conditions d'élaboration et de mise en œuvre de doctrines en cyber-dissuasion à moyen terme : innovations technologiques, stratégies industrielles, orientations géopolitiques.

Si le futur de l'environnement numérique ne peut précisément être défini à moyen terme, du fait notamment du rythme élevé de l'innovation dans ce domaine, plusieurs tendances technologiques liées ont déjà émergé qui devraient se confirmer. Elles sont notamment liées à la croissance du nombre d'objets connectés à internet ou gérés au travers du réseau et aux phénomènes de nomadisation et de recherche de mobilité. Le développement de l'informatique en nuage répond également à des impératifs économiques et se développe en parallèle d'une externalisation croissante des services informatiques des entreprises.

En outre, la mise en commun et la distribution (donc l'achat) via Internet des capacités de calcul et de traitement de machines (ou de réseau de machines) distantes ont été rendues possibles par l'accroissement des performances du réseau. Elles pourraient permettre à terme d'agréger les capacités de calcul de plusieurs dizaines de machines pour parvenir à des niveaux compatibles voire supérieurs à ceux de supercalculateurs. Enfin, la convergence des moyens de gestion des flux de communication vers une norme unique basée sur les protocoles internet est de nature à créer de nouvelles vulnérabilités dans des systèmes jusqu'alors isolés du réseau mondial.

Le développement de ces tendances aura des conséquences en termes de sécurité et au niveau des besoins de protection des infrastructures, des personnes et des biens. En particulier, l'accroissement du nombre et du type des objets (intelligents) connectés entre eux, aux personnes et au(x) réseau(x) devrait conduire à augmenter les risques de détournement et contribuer à aggraver les conséquences potentielles d'actes malveillants.

Convergence des protocoles de traitement des flux de données et des communications vers la norme IP (Internet Protocole)

La convergence vers la norme *Internet Protocol*[37] pour l'ensemble des réseaux de communication est une opération déjà largement engagée. Cela ne va pas sans risques : l'emploi d'un même protocole pouvant par exemple généraliser la présence d'une vulnérabilité donnée à l'ensemble des systèmes connectés et donc accroître les effets d'une attaque fondée sur son exploitation.

[37] http://en.wikipedia.org/wiki/Internet_Protocol

Une étude récente sur le sujet a abouti à une série de conclusions intéressantes, notamment en matière de résilience des réseaux IP, d'organisation de la sécurité et de gestion du changement[38].

Encadré 2 : Conclusions sur l'impact de la convergence IP en matière de sécurité

- La migration des protocoles de communication vers la norme IP est en cours et probablement irréversible ;
- Le rythme de migration est variable d'un opérateur à l'autre mais est en général plutôt lent, les réseaux existants (« *legacy networks* ») continuant à fonctionner tant qu'ils restent économiquement rentables ;
- Les technologies utilisées pour cette migration sont connues et il y a un consensus sur les moyens à utiliser ;
- Les réseaux IP sont plus ouverts aux attaques extérieures, mais les méthodes et mesures de sécurité sont beaucoup plus puissantes que celles utilisées pour les réseaux existants ;
- Les réseaux IP sont intrinsèquement plus « résilients » aux surcharges de trafic, aux dysfonctionnements de sous-systèmes et aux désastres naturels, pourvu qu'ils aient été construits selon les méthodes standards prévues à cet effet ;
- Un développement rapide de l'écosystème de télécommunication va faire apparaître de nouveaux défis, et l'industrie devra les résoudre avant de déployer tous les services sur un même réseau ;
- L'organisation interne des opérateurs ne changera pas considérablement avec l'introduction de structures IP et la dépendance à ces dernières, mais le point principal sera de maintenir une sécurité physique de tout premier ordre pour ces structures, une fourniture d'énergie permanente et une réponse aux incidents précise et rapide ;
- D'un point de vue organisationnel, un personnel qualifié moins nombreux et travaillant dans un plus petit nombre de lieux sera nécessaire pour gérer ces réseaux futurs ;
- Les choix politiques liés à cette migration devront établir une coordination entre des parties-prenantes, tracer un chemin parmi des intérêts contradictoires, et résoudre des contradictions entre certaines priorités. Ces activités sont et seront dans tout l'avenir prévisible principalement basées sur les politiques des États, bien que des coopérations transnationales doivent être recherchées autant que possible.

[38] « Analysis of the security and resilience challenges brought about by the convergence of previously separate and distinct communication networks towards IP networks », IDC, 2010, étude commanditée par la Commission européenne.

➡ Une action au niveau de l'Union européenne peut aider à coordonner les politiques nationales et les efforts de standardisation, créer des plates-formes pour un dialogue industriel à l'échelle européenne et favoriser la coopération internationale pour les réactions aux cas d'urgence.

Il faut aussi noter que la ***convergence IP devrait avoir à terme un impact sur les télécommunications spatiales*** en remettant à l'ordre du jour, après l'échec des projets de constellations en orbites basses et moyennes des années 1990, la question des liaisons Internet satellitaires. Une telle évolution pourrait s'appuyer sur le précédent du satellite Ka-Sat d'Eutelsat (la bande Ka permet une liaison haut débit avec une antenne de petite dimension) mis en orbite en 2010.

Ces nouvelles perspectives dans le domaine des satellites devront être prises en compte pour les questions d'élaboration de capacités offensives futures (neutralisation de satellites) mais aussi pour les collectes massives de données permettant une attribution plus rapide des attaques.

Au total, la poursuite de la convergence IP pourrait conduire à une meilleure résilience générale des réseaux, tout en les laissant plus ouverts à des attaques extérieures. Un regain des liaisons Internet par satellite pourrait voir le jour, avec des implications en matière de capacités offensives et d'attribution des attaques

Le développement du nomadisme et de la cyber-mobilité devrait continuer à s'accélérer

Le nomadisme devrait s'accélérer en parallèle de la convergence des protocoles de communication vers la norme IP.

D'ores et déjà, les téléphones mobiles et les terminaux mobiles (tablettes ou *netbooks* par exemple) s'avèrent être des outils indispensables pour les cadres des entreprises du secteur privé ainsi que pour la plupart des hauts-fonctionnaires. Avec le développement de nouveaux protocoles de communication, qui devraient permettre d'accroître les débits des communications sans fil pour les faire converger vers des niveaux proches de la fibre optique (autour de 80-100 Mo/s en débit montant), le spectre des services qui pourront être fournis via les terminaux portables devrait continuer à augmenter. De la même façon, le nombre de personnes connectées et utilisant des services dématérialisés devrait également croître plus rapidement que ce n'est le cas aujourd'hui.

La banalisation des logiciels de pilotage de production, permise notamment par une dynamique de convergence des formats numériques, répond à une logique économique de réduction des coûts de développement et de maintenance des systèmes informatiques et de communication. Cette évolution conduit à une généralisation de l'informatisation dans le monde industriel pour la télémaintenance ou la gestion à distance de systèmes de production ou d'équipement, alors même que celle-ci se limitait dans les années 1990 à certaines infrastructures clefs de distribution (eau, électricité, gaz et pétrole).

C'est en particulier dans la gestion à distance des processus industriels et des infrastructures que les entreprises ont pu profiter de l'interopérabilité des systèmes et du développement d'offres logicielles commerciales. Ainsi, les systèmes de commande et d'acquisition de données de surveillance – SCADA[39] – s'appuient massivement sur des technologies publiques en particulier pour communiquer au sein d'un réseau commun et parfois échanger des données via internet afin de réduire les coûts qui seraient générés par l'utilisation d'un réseau dédié : protocoles internet de communication, *bluetooth* et *wi-fi* (et à plus long terme des protocoles de type *Wi-MAX*).

En parallèle, les interconnexions entre les systèmes d'information à caractère administratif des entreprises et les infrastructures physiques de production, largement automatisées, ont tendance à se développer en accroissant de fait les points d'entrée possibles pour l'injection de logiciels malveillants. Ils se trouvent ainsi de plus en plus exposés à des logiciels malveillants exploitant les failles existantes ou anciennes souvent connues par les fabricants de logiciels, même si, dans la plupart des cas, les systèmes d'exploitation informatiques embarqués (« *embedded* ») des SCADA font l'objet de clauses particulières interdisant la mise en place à distance de mises à jour de sécurité[40].

La nomadisation croissante devrait conduire à de nouvelles vulnérabilités et une exposition accrue des infrastructures vitales à des attaques à distance, demandant un renforcement spécifique des capacités de cyber-défense de la part des opérateurs concernés. Une meilleure intégration des infrastructures critiques dans le domaine de la protection des activités dites « de souveraineté » devrait devenir indispensable pour bâtir une cyber-dissuasion crédible.

L'Internet des objets (IoT) devrait progressivement devenir une réalité

Ce domaine rassemble en réalité un spectre assez large d'axes de développement dont la concrétisation devrait s'effectuer progressivement. Il s'agit en effet de permettre la connexion de l'ensemble des objets du quotidien à Internet pour favoriser à la fois l'automatisation de leur gestion et de leur fonctionnement mais également une interaction permanente et contextuelle avec eux pour tous les utilisateurs, qu'il s'agisse de personnes ou d'autres objets physiques ou virtuels.

Les outils qui permettront cette évolution sont l'indispensable migration vers le protocole IPv6[41] – indispensable pour connecter des dizaines de milliards de systèmes à Internet – et le développement des puces de *Radio Frequency IDentification* (RFID).

En 2010, à peine 1 % des utilisateurs d'Internet pouvaient opérer en IPv6 et, malgré un programme incitatif de la Commission européenne, le changement risque d'être long du

[39] http://en.wikipedia.org/wiki/SCADA

[40] Entretiens de Bruno Gruselle, octobre 2009.

[41] Passant d'un adressage IPv4 en 32 bits à des adresses sur 128 bits beaucoup plus nombreuses – ce qui résout à moyen terme le problème du nombre limité d'adresses disponibles.

fait du besoin de fonctionner en bi-mode pendant plusieurs années. Quant aux RFID, l'évolution attendue est régulière mais plutôt modérée.

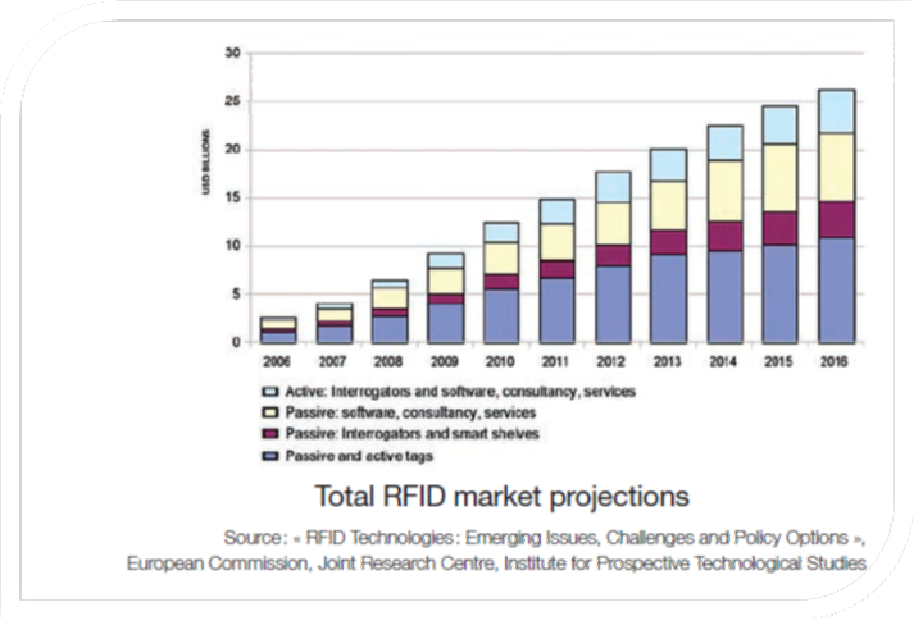


Figure 5 : Accroissement du marché des moyens utilisant des puces Radio Frequency IDentification (source : Agence Nationale de la Recherche)

De nombreux programmes européens préparent dès maintenant la généralisation des puces RFID pour interconnecter les individus avec les objets et systèmes de la vie courante. A titre d'exemple, le véhicule du futur devra à la fois offrir des informations aux conducteurs et passagers sur la route et sur son environnement[42]. Il devra également pouvoir s'insérer dans la circulation en interagissant avec les autres utilisateurs et les autres objets proches (véhicules, signalisation…). A terme, l'internet des objets devrait s'étendre à beaucoup d'autres domaines, en particulier la médecine, la domotique et la gestion de la distribution des services. L'adossement de l'internet des objets à des services de cartographie numérique offrant à l'utilisateur un niveau important d'interactivité et l'accès aux données locales devrait également voir le jour comme en témoigne la montée en puissance des outils de géo-localisation et l'émergence du marquage géographique numérique (*geo-tagging*)[43].

[42] http://lexpansion.lexpress.fr/high-tech/microsoft-va-equiper-les-voitures-toyota-de-services-Internet_251989.html

[43] Sur ce point voir : « *Cartographie numérique et développement des territoires* », Etude thématique rédigée par ITEMS International et Auber Olivier publié le 26 mars 2008. http://www.oten.fr/?article4031

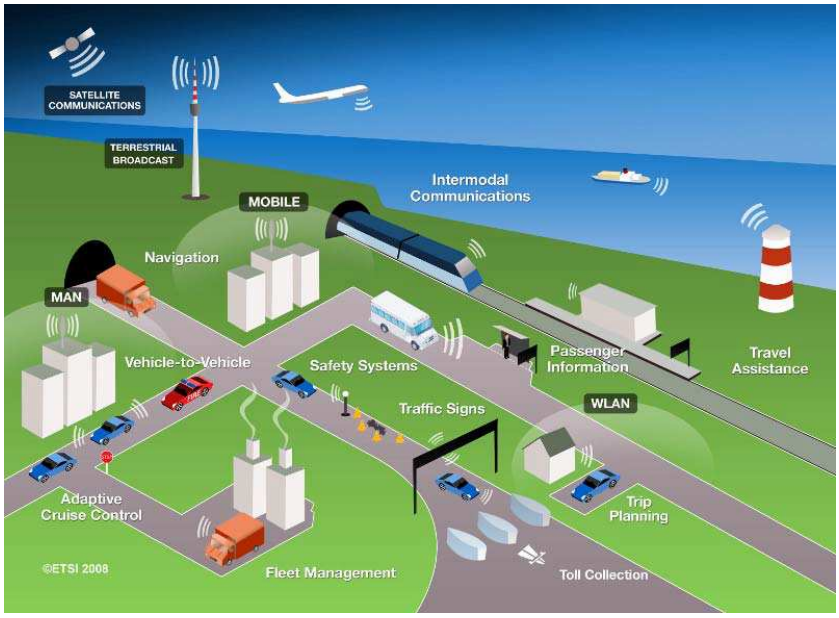


Figure 6 : Schéma de principe d'intégration d'objets dans un réseau de communication (source : European Digital Rights)

Le besoin d'assurer la sécurité et l'intégrité physiques et logicielles du réseau et des capteurs/objets associés ou connectés – contre des accès malveillants (sabotage) ou des tentatives d'intrusion au sein d'un système[44] – sera d'autant plus important que le fonctionnement des (sous)ensembles connectés aura un impact sur des applications critiques pour les personnes et les infrastructures clefs (gestion d'actes médicaux, des réseaux de transport, des flux de personnes ou de matériaux sensibles/polluants...). Or, la complexité intrinsèque d'un futur internet des objets – très fort besoin d'interopérabilité entre des normes de fonctionnement différentes, compatibilité des formats, communications rapides – devrait aller de pair avec le développement de protocoles et de logiciels techniquement complexes et qui présenteront vraisemblablement de nombreuses failles et vulnérabilités. Comme pour la convergence vers la norme IP, les protocoles utilisés devraient présenter au minimum de fortes similarités voire employer une norme unique pour atteindre le niveau souhaitable/utile d'interconnexion et de compatibilité entre les systèmes.

Le risque associé à la perte de données s'aggravera vraisemblablement du fait de l'accroissement du volume des données personnelles ou confidentielles (par exemple médicale) transitant sur le réseau pour des applications de type IoT.

Si l'on peut difficilement prévoir précisément les effets de ces actions sur les entreprises et les États, on peut estimer à la lumière des données disponibles que, en termes financiers et au niveau mondial, les pertes équivalentes se chiffreront en centaines de milliards de dollars concernant notamment : le vol de données confidentielles, le détournement d'identité ou d'usage à des fins de falsification ou de contrefaçon, le

[44] European Commission Staff Working Document, « Early Challenges regarding the « Internet of Things » », 29 septembre 2008.

sabotage de production (dont le déni massif de service, la perturbation des systèmes informatiques critiques, la prise de contrôle à distance...).

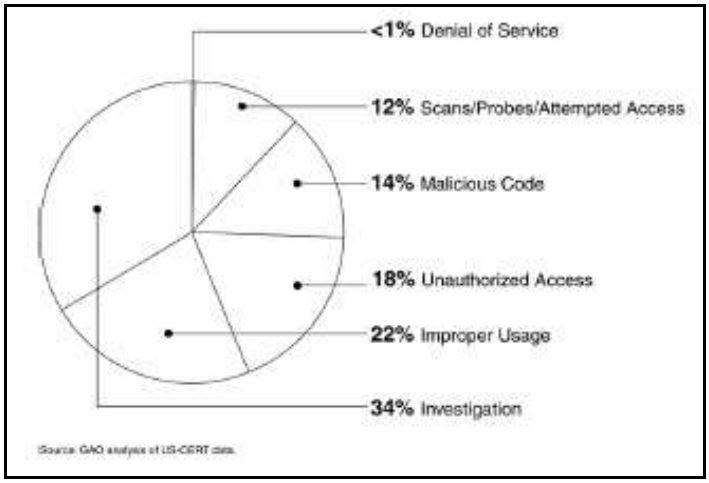


Figure 7 : Classification des incidents rapportés aux CERT américains entre 2006 et 2008 (source : Government Accountability Office)

La seule partie ***concernant la perte de données*** – qui semble être la part la plus importante des malversations numériques – représente vraisemblablement à l'heure actuelle un total compris entre ***200 à 250 milliards de dollars de perte de chiffres d'affaires pour les principales multinationales***[45]. Ce chiffre devrait continuer à augmenter avec en parallèle une montée en puissance des risques physiques accompagnant le développement de l'internet des objets et des difficultés de sécurisation des systèmes de gestion des processus et des infrastructures. Pour autant, il convient de souligner que ces risques à caractère industriel – qui sont réels si l'on regarde le cas Stuxnet – ne se matérialisent que dans des conditions très précises : l'élaboration de systèmes malveillants comme Stuxnet nécessite des travaux de recherche importants, l'utilisation de plusieurs « *0 day exploits* »[46] et l'écriture de plusieurs logiciels complexes.

Les infrastructrures vitales et des données ayant un caractère stratégique seront directement concernées par de nouveaux types de vulnérabilités générées par le développement de l'Internet des objets. Ces risques particuliers devront être pris en compte pour la conception et la mise en œuvre de capacités défensives crédibles au sein d'une démarche de cyber-dissuasion.

[45] Il s'agit-là d'une estimation basée sur les données de McAfee ainsi que sur celles publiées par le Royaume Uni qui est l'un des pays ayant l'un des outils statistiques les plus performants en matière de crimes numériques.

[46] C'est-à-dire des failles de sécurité non détectées ou connues des concepteurs des plates-formes logicielles attaquées. Peter Sonner & Ian Brown, « Reducing Systemic Cybersecurity Risk », OECD/IFP Project on « Future Global Shocks », 14 January 2011, p. 44.

L'informatique en nuage devrait modifier profondément les habitudes de gestion des données et d'utilisation de logiciels

L'informatique en nuage est appelée à devenir une sorte de pendant immatériel de l'Internet des objets, en ce sens qu'il constitue une tendance lourde d'agrégation des moyens et processus informatiques. L'informatique dans les nuages – ou en nuage, de l'anglais : *cloud computing* – est un concept faisant référence à l'utilisation de la mémoire et des capacités de calcul d'ordinateurs et de serveurs ou de fermes de serveurs répartis géographiquement et liés par un réseau de communication global, qu'il s'agisse qu'internet ou de réseaux privés.

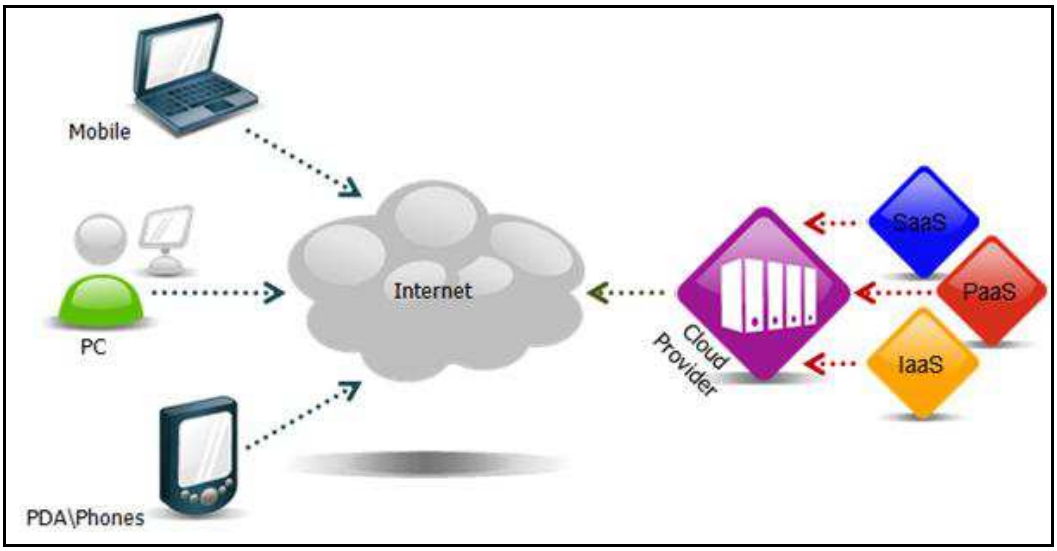


Figure 8 : Schéma de principe du Cloud Computing
(source : Think-security's blog[47])

En principe, toute fonction, système ou outil informatique peut être ainsi mis « en nuage » tout en restant accessible à distance. Ces fonctions, systèmes ou outils sont couramment regroupés en trois grands types de service[48] :

⇒ Software as a service (SaaS) : Fourniture de logiciels ou d'applications aux clients (le fournisseur offre un environnement au travers duquel le client a accès à ces applications).

[47] http://saboursecurity.files.wordpress.com/

[48] Voir la page Wikipedia sur le *cloud computing*. Il existe également d'autres services de type cloud qui dérive du SaaS : stockage de données (*Data as a Service*), fourniture ou gestion de réseaux privés (*Network as a Service*) ou encore sécurisation des accès numériques (*Identity and Policy Management as a Service*).

⇒ Platform as a service (PaaS) : Fourniture de ressources matérielles mais également d'une plate-forme logicielle permettant l'exécution des applications appartenant aux clients.

⇒ Infrastructure *as a Service* (IaaS) : Fourniture de ressources matérielles c'est-à-dire de puissance de calcul et d'espace de stockage dédiées à l'utilisation des clients.

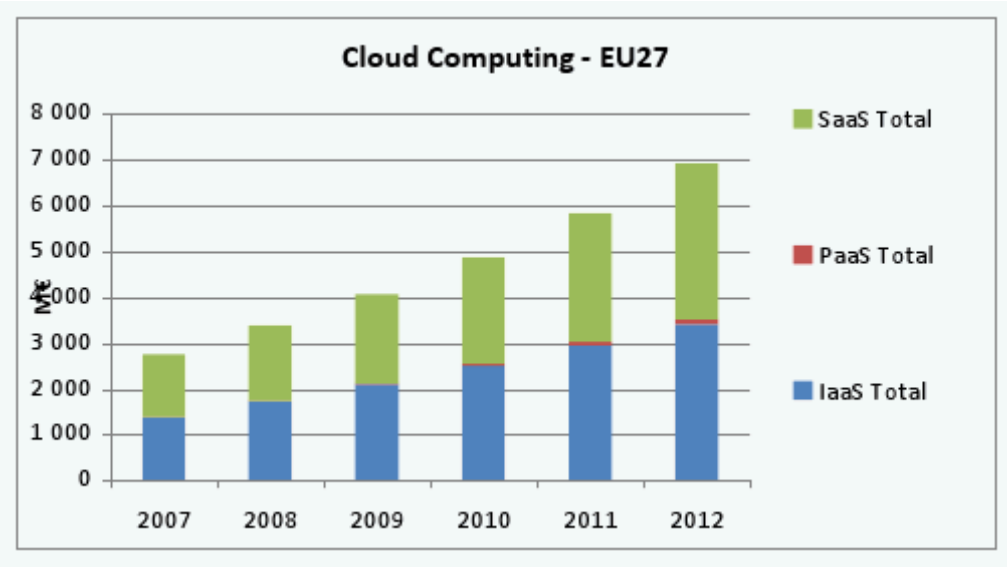


Figure 9 : État des parts du marché (en M€) des diverses offres de Cloud Computing (source : IDC[49])

Pour les prestataires, l'intérêt de l'informatique en nuage est d'optimiser l'emploi de ses infrastructures matérielles (*hardware*) entre ses clients. Un serveur d'hébergement pouvant ainsi être occupé jusqu'à 60 % en moyenne alors que l'occupation courante ne dépasse pas quelques pour cents.

Pour l'utilisateur, l'intérêt économique existe aussi : la sous-traitance de la gestion des outils informatique diminue les investissements (remplacés par des frais de fonctionnement), avec un fort gain de flexibilité en cas de réduction ou d'augmentation brutale d'activité et un transfert des problèmes de maintenance (e.g. mises à jour de logiciels). Par contre l'informatique en nuage peut créer des problèmes de contrôle sur la sécurité des données et outils ainsi transférés.

Les principales entreprises du secteur de l'informatique et des télécommunications ont d'ores et déjà lourdement investi pour proposer des solutions d'informatique en nuage, notamment côté américain (Microsoft, Google, Amazon, Apple, IBM) et dans une moindre mesure côté français (Bull, Atos, Cap Gemini et Orange).

[49] David Bradshaw, « Western European Software-as-a-Service Forecast, 2009–2013 », Apr 2009 – Doc # LT02R9, 2009. Cité par l'*European Network and Information Security Agency*.

Il s'ensuit l'émergence d'un marché global déséquilibré marqué par une prédominance américaine, due (1) à la réticence des entreprises et administrations européennes à transférer leurs moyens informatiques hors d'Europe et (2) à la rareté des fermes de serveurs (*data-centers*) implantées en Europe. Enfin, l'absence d'opérateurs européens majeurs est aggravée par une réglementation européenne requérant que les données des entreprises européennes restent hébergées sur le continent.

Bien que de nombreux travaux aient été menés sur les politiques de sécurité efficaces applicables à l'informatique en nuage[50], la résilience des fermes de serveurs face à des accidents ou à des pannes provoquées par des attaques numériques continue à s'avérer problématique.

Les incidents connus laissent à penser que la disponibilité des données, les capacités de calcul et les processus logiques abrités dans le « nuage » peuvent être remis en cause ponctuellement avec des conséquences plus ou moins importantes pour les clients[51].

En termes de sécurité, la montée en puissance du *cloud computing* constitue à la fois une source d'accroissement des risques mais également un gisement de progrès pour un meilleur contrôle des vulnérabilités intrinsèques au développement du rôle des réseaux informatiques, notamment internet[52]. De fait, les caractéristiques des architectures d'informatique dans les nuages engendrent cette dualité en termes de sécurité :

- ⇨ L'utilisation de plates-formes matérielles appartenant à un fournisseur externe, en particulier pour les SaaS, transfère les problématiques de gouvernance (dont la sécurité) des infrastructures, des logiciels et des données à un ou des tiers. Les questions relatives à la ségrégation des données par les fournisseurs de service, c'est-à-dire de la séparation des informations appartenant aux différents clients, mais également à la confidentialité des traitements de données, se posent également à la fois pour les entreprises et pour les particuliers[53].

- ⇨ Les interfaces de gestion des services du nuage – pour les architectures publiques ou hybrides – sont accessibles via internet et peuvent donc faire l'objet de piratage ou de détournement. Plus spécifiquement pour les services de type SaaS, les failles et les vulnérabilités inhérentes aux interfaces utilisateurs (navigateurs commerciaux ou interfaces spécifiques) viennent accroître les risques d'accès par des pirates ou des acteurs malveillants. Le piratage des interfaces clients par un acteur tiers peut conduire à la compromission de données stockées sur les serveurs délocalisés ou à la perte de contrôle des processus gérés au travers du nuage[54]. Les risques de compromission des processus dans le cas de service de type IaaS sont d'autant plus

[50] Voir notamment, European Network and Information Security Agency, « Cloud Computing: Benefits, risks and recommendations for information security », November 2009.

[51] Sur ce point voir notamment le rapport annuel 2009 du CLUSIF sur la cybercriminalité. http://www.clusif.asso.fr/ fr/production/ouvrages/pdf/PanoCrim2k9-fr.pdf

[52] European Network and Information Security Agency, « Cloud Computing: Benefits, Risks and Recommandations for Information Security », November 2009.

[53] Syntec Numérique, « Livre Blanc sur la sécurité du Cloud Computing : analyse des risques, réponses et bonnes pratiques », 2010.

[54] Ibid, p. 8.

grands que les machines fournies peuvent être virtuelles[55] et donc faire tourner en parallèle plusieurs applications provenant de plusieurs sources.

⇨ La question de localisations des données se pose pour les architectures publiques adossées à internet : la problématique est en effet de savoir si les pays accueillant des fermes de serveurs peuvent accéder dans le cadre de leur législation, aux données conservées sur leur territoire, par exemple à des fins d'enquête[56]. A l'heure actuelle, de nombreux fournisseurs de service (type SaaS) ne prennent pas d'engagement sur le lieu de stockage des données et implantent leurs fermes de serveurs dans des pays émergents pour des raisons économiques[57].

Tableau 1 : Répartition géographique des parts de marché dans l'informatique en nuage (source 451 Group[58], avril 2010)

	États-Unis	**Union européenne**	**Asie**
Cloud Computing en général	57 %	31 %	12 %
IaaS	93 %	6 %	1 %

La virtualisation des données et des processus logiciels – qui sous-tend la généralisation du *cloud computing* – ainsi que la délocalisation physique des serveurs les accueillant ***constituent également un facteur de complexification pour toute investigation qui ferait suite à un acte (ou à une série d'actes) malveillant.*** La question de l'attribution d'un acte numérique s'avère déjà complexe ; la délocalisation géographique ne devrait qu'accroître les difficultés, avec notamment le besoin de prendre en compte les aspects légaux locaux.

De fait, la généralisation de l'informatique en nuage – de la même façon que les autres phénomènes qui lui sont liés comme la tendance à une externalisation des processus et des outils informatiques ou encore le partage des capacités de calcul (*grid computing*) – ne crée pas à proprement parler de nouvelles vulnérabilités en matière numérique. En revanche, elle vient exacerber des risques qui existent d'ores et déjà.

C'est le cas, en particulier, pour les problématiques de sécurité des données confidentielles et de gestion des informations personnelles – y compris les données relatives à l'identité des personnes physiques ou morales – qui seront stockées au moins pour

[55] C'est-à-dire en réalité une partie de la capacité d'un ou de plusieurs serveurs qui ne sont pas dédiés aux seules applications du client mais sont partagés entre plusieurs clients.

[56] Syntec Numérique, « Livre Blanc sur la sécurité du Cloud Computing : analyse des risques, réponses et bonnes pratiques », 2010, p. 21.

[57] Entretiens de l'auteur.

[58] http://www.presence-pc.com/actualite/cloud-computing-europe-US-38844/

partie sur des serveurs délocalisés. L'accroissement des opérations réalisées en ligne, notamment des services administratifs à caractère personnel comme aujourd'hui les déclarations de revenus ou les demandes d'actes d'état civil, devrait accélérer le développement d'une identité en ligne (ou numérique) qu'il faudra authentifier pour conduire de façon sécurisée les interactions avec les administrations[59].

La criminalité numérique s'intéresse d'ores et déjà aux bénéfices qu'elle pourrait tirer du détournement d'identité ou du vol de coordonnées sécurisées notamment bancaires. L'enjeu est de taille, évalué à 32 milliards d'euros pour les États-Unis et 2,15 milliards d'euros au Royaume-Uni en 2007[60]. La progression du commerce électronique et des transactions en ligne – qui pesaient 31 milliards d'euros en France en 2010 selon le secrétariat d'État à l'économie numérique[61] – rend ce secteur particulièrement attractif pour les criminels. Cet intérêt préfigure sans doute la montée en puissance d'agressions numériques conduites à des fins de sabotage ou d'espionnage par une variété plus large d'acteurs contre les futurs systèmes permettant le fonctionnement de l'informatique en nuage.

En outre, l'usurpation d'identité ne sert pas seulement à conduire des opérations commerciales frauduleuses, elle peut aussi être utilisée comme clé afin de déverrouiller des accès numériques protégés dans le réseau en vue de réaliser des actes malveillants : espionnage, attaques de réseaux, extorsion, chantage. L'usurpation d'identité des utilisateurs des réseaux sociaux permet aussi à certains cybercriminels de cerner des cibles (*profiling* numérique) afin de commettre des actes malveillants.

Outre l'essor de la problématique de la gestion de l'identité numérique, le développement du *cloud computing* soulève le problème de la résilience d'internet, qui constitue plus que jamais la colonne vertébrale du fonctionnement du monde numérique, face à des actes malveillants et à certaines catastrophes naturelles. Si internet a été conçu comme un système robuste possédant de multiples redondances qui interdisent finalement une rupture complète de service, son fonctionnement peut être fortement perturbé voire interrompu à des niveaux locaux ou régionaux. Les vulnérabilités des serveurs racines[62], de l'infrastructure physique[63] ou encore du système d'adressage (les *Domain Name Server* ou DNS[64]) constituent autant de failles qui pourraient être exploitées pour

[59] Guillaume Desgens-Pasanau, Eric Freyssinet, « L'identité à l'ère numérique », collection Presaje, Editions Dalloz, 2009, pp. 9-12.

[60] Brigitte Acoca, analyste à l'OCDE, dans un rapport remis aux ministres réunis à Séoul – cité dans l'édition du *Monde* du 18 juin 2008.

[61] http://www.fevad.com/etudes-et-chiffres/bilan-e-commerce-en-2010#topContent

[62] Il en existe 13 au niveau mondial dont 7 utilisent d'ores et déjà le protocole d'adressage IPv6. Avec celui-ci le nombre d'adresses internet disponibles devrait passer de 2^{32} à 2^{128} et ainsi permettre de répondre aux besoins émergents en termes d'adressage, en particulier pour le cloud et l'IoT.

[63] Ainsi la rupture de câbles peut déconnecter des secteurs géographiques insuffisamment desservis comme en 2007 lorsqu'un câble sous-marin a été sectionné, provoquant l'interruption des communications avec la Guyane le jour même du premier tour de l'élection présidentielle.

[64] *Domain Name Server* – Serveur de nom de domaine, qui ont pour fonction de transformer une adresse internet (ex : www.defense.gouv.fr) en son adresse technique (par exemple 240.34.340.34) afin de pouvoir établir un dialogue entre les ordinateurs sur le réseau.

intercepter des flux de données, ou pour neutraliser temporairement et localement le réseau[65].

La résilience des fermes de serveurs face à des accidents ou à des pannes provoquées par des attaques numériques mérite également d'être prise en compte. Les incidents connus laissent à penser que la disponibilité des données, des capacités de calcul et des processus logiques abrités dans le « nuage » peut être remise en cause ponctuellement avec des conséquences plus ou moins importantes pour les clients[66].

La virtualisation des données et des processus logiciels ainsi que la délocalisation physique des serveurs les accueillant est également un facteur de complexification pour toutes les actions policières et répressives faisant suite à un acte (ou à une série d'actes) malveillant. A l'heure actuelle, la problématique de l'attribution d'un acte numérique s'avère déjà complexe même s'il existe des moyens de détecter les origines numériques d'une action donnée. Les enquêtes et la récupération de données et de preuves après des actes malveillants ou criminels peuvent se heurter aux législations locales des pays abritant les serveurs ou les machines utilisées.

L'informatique en nuage est un modèle économiquement attractif de gestion des moyens informatiques. Dans le cas des systèmes d'information sensibles, les risques associés restent toutefois importants. Ils devront être pris en compte dans l'élaboration des capacités de défense et de riposte.

Anonymisation des données, des échanges et des traces laissées sur Internet

Le développement d'Internet et des outils de communication et d'interaction qui lui sont liés ont conduit à engager de nombreuses réflexions sur la gestion des données personnelles des utilisateurs et la protection de leur identité numérique.

En effet, les données disséminées sur les réseaux informatiques et en particulier Internet, seront de plus en plus nombreuses, précises et variées. Elles pourraient à terme comprendre des informations médicales ou physiologiques sur les personnes, des données techniques concernant les bâtiments ou les infrastructures, etc. La diversification des outils et moyens de communication interconnectés est de nature à intensifier le nomadisme des salariés, en particulier des cadres, et le besoin de disposer en permanence des outils et des données nécessaires à la réalisation de leur emploi. Le besoin de sécurité pourrait devenir secondaire au regard des gains de productivité liés à la mobilité des cadres et au développement de nouveaux outils de travail connectés aux réseaux de l'entreprise et à internet. La question se pose *in fine* de savoir s'il sera pris en compte dans le processus de développement des réseaux futurs ou ajouté *a posteriori*. En effet, les défis techniques qui doivent être relevés pour assurer la plus grande efficacité des logiciels – interopérabilité des applications entre elles, facilité d'emploi et ergonomie, rapidité et fluidité d'exécution – peuvent éclipser l'intégration de dispositifs

[65] Sur ce point voir notamment le rapport annuel 2009 du CLUSIF sur la cybercriminalité : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k9-fr.pdf

[66] Ibid.

de sécurité permettant, entre autres, d'assurer la protection des données personnelles des utilisateurs.

A la problématique de la gestion de l'identité numérique, **il convient d'ajouter celles qui concernent le droit à l'oubli et de sécurisation des données gérées en ligne**. Il paraît assez peu concevable de détruire systématiquement les données présentes sur internet au bout d'un délai donné, de contraindre des États étrangers ne disposant pas d'une législation dans ce domaine et de tracer l'information litigieuse compte tenu de sa probable dissémination sur d'autres sites et blogs, notamment à cause des méthodes propres à l'espace numérique.

En revanche il pourrait être envisagé de créer la possibilité pour les particuliers et les entreprises de demander le retrait d'informations les concernant si elles s'avèrent inexactes, fausses ou datées ou la rectification de telles informations[67]. Outre la destruction des pages et informations concernées, une telle démarche implique le retrait des données des indexations des moteurs de recherche, ce qui paraît techniquement et politiquement complexe. ***En l'état, le législateur, français comme européen, reste assez vague sur les durées de stockage des données.*** Il fixe, par exemple, pour les fournisseurs d'accès un droit de stockage d'informations personnelles pendant un an. Les conditions de conservation des données et leur sécurisation constitue un enjeu spécifique notamment dans le contexte du droit des affaires et du droit pénal. En la matière, le cadre juridique existant mériterait d'être éclairci et complété pour établir les conditions indispensables au développement de l'économie numérique (*Business-to-Business* ou *Business-to-Consumer*)[68]. Une proposition de loi des sénateurs Yves Détraigne (MoDem) et Anne-Marie Escoffier (PRG) précise, outre des actions de formation à l'attention des jeunes, que l'adresse IP devienne, par exemple, une donnée à caractère personnel[69].

Or, qu'il s'agisse d'identité numérique ou de données personnelles, ***la principale difficulté vient du fait que coexistent dans le domaine deux besoins contradictoires.***

En premier lieu, la généralisation d'internet a contribué à « *anonymiser* » les utilisateurs qui cherchent autant que possible à intervenir sur internet, en tant que diffuseurs ou consommateurs de contenu, en conservant autant de liberté possible. Les problématiques liées au droit à l'oubli, au silence des puces ou à la capacité de déconnexion des individus et, dans une certaine mesure, des personnes morales traduisent en partie ce besoin. De la même façon, l'utilisation de pseudonymes ou le recours grandissant à des avatars illustrent la volonté d'éviter de révéler sa véritable identité.

A contrario, ***le besoin de sécurité s'avère également être le pilier des échanges numériques entre les personnes***, par exemple pour ce qui concerne les transactions économiques, et de façon plus générale comme la base de l'ensemble de l'édifice numérique. Les États doivent jouer le rôle de tiers de confiance pour protéger et garantir l'intégrité de l'identité des personnes mais se faisant, ils acquièrent la capacité nouvelle/sup-

[67] http://wiki.univ-paris5.fr/wiki/Informatique,_libert %C3 %A9s_et_vie_priv %C3 %A9e#Droit_.C3.A0_l.27 oubli

[68] Guillaume Desgens-Pasanau et Eric Freyssinet, « L'identité à l'ère numérique », Dalloz/Presaj, 2009, p. 153.

[69] http://www.senat.fr/noticerap/2008/r08-441-notice.html

plémentaire d'investigation qu'ils devront utiliser pour identifier les malfaiteurs au moins au niveau national.

La complexité de la collecte et de l'analyse de données à grande échelle représente toutefois une médiocre garantie d'anonymat. Par contre, le recours à des applications spécifiques permet de dissimuler la localisation d'un utilisateur et de masquer les liaisons établies avec un interlocuteur ou un site[70].

Conçue par le *Naval Research Laboratory* des États-Unis sur le principe du routage en oignon, le système TOR – le plus connu des moyens d'anonymisation – est maintenant disponible en logiciel libre et accessible à tous. Même s'il est difficile de présager si ce logiciel ou ses dérivés vont garantir dans la durée l'anonymat sur Internet, il convient de souligner que Wikileaks est réputé avoir protégé ses bases de données et l'identité de ses informateurs en utilisant des techniques dérivées de TOR.

Une approche différente a été engagée par le gouvernement américain au travers du développement d'un kit anti-censure destiné aux oppositions à certains régimes hostiles à Washington. Cet outil doit permettre à l'utilisateur de disposer de moyens pour diffuser en toute sécurité – et hors des circuits Internet surveillés – des informations recueillies sur place grâce à des réseaux parallèles (Internet et mobiles), des ordinateurs portables, des antennes et en utilisant des logiciels de cryptage. Il doit également permettre aux utilisateurs d'accéder à Internet sans utiliser les fournisseurs de service surveillés[71].

Les outils et procédures d'anonymisation qui se développent peuvent rendre de plus en plus difficile l'attribution des attaques à des auteurs clairement et rapidement identifiés, au détriment de la crédibilité des moyens de cyber-dissuasion.

[70] La plus connue des solutions d'anonymisation est le logiciel TOR. https://www.torproject.org/

[71] http://arstechnica.com/tech-policy/news/2011/01/uncle-sam-has-30m-to-bypass-chinese-iranian-net-filters.ars

Définition d'un concept et d'une doctrine en matière de dissuasion numérique, comparaison avec la dissuasion nucléaire et difficultés spécifiques

Objectifs et structure générale d'une dissuasion numérique

Le débat sur les stratégies de dissuasion numérique évolue autour de plusieurs questions, en particulier celle de savoir si l'importance des dégâts que peut potentiellement causer une attaque numérique (ou une série d'attaques) peut justifier la mise en place d'un système complexe à opérer et à mettre en œuvre. Ce débat est difficile à trancher dans la mesure où les données disponibles sont trop parcellaires ou proviennent (souvent) de sources dont l'objectivité est sujette à caution. De fait, il paraît difficile d'établir définitivement l'intensité réelle du risque numérique – qui prend la forme de ce que l'on pourrait appeler un bruit de fond constant –, c'est-à-dire des actions négatives permanentes qui affectent les systèmes informatiques mondiaux.

A contrario, on ne peut que constater au travers des exemples disponibles que plusieurs attaques importantes – y compris des intrusions de grande ampleur à finalité d'espionnage[72] – ont été constatées depuis 2007[73]. Ces événements témoignent sans doute de l'existence de vulnérabilités numériques de plus en plus exploitées par des acteurs malveillants ou, de façon plus prosaïque, la conséquence du fait que les systèmes informatiques et de communication tiennent une place de plus en plus critique dans nos activités quotidiennes à la fois pour des opérations physiques et matérielles, le stockage de données confidentielles ou personnelles ou encore, l'échange d'information entre des acteurs distants.

Face à une gamme étendue d'actes malveillants, la première question qui se pose est de savoir le rôle générique qu'aurait une dissuasion numérique.

A ce stade, on peut estimer qu'elle pourrait poursuivre deux principales finalités déclarées[74] :

- **Défendre des intérêts numériques spécifiques –** ils comprennent *a minima* les infrastructures nationales critiques mais qui pourraient s'étendre à d'autres intérêts nationaux – face aux menaces que les acteurs malveillants (d'origine étatique ou pas) peuvent générer ;

- **Eviter un enchaînement d'actions** par des acteurs malveillants ou les organisations qui les emploient qui amèneraient à accroître les effets négatifs sur les intérêts numériques défendus (*escalade*). Il est important de souligner que l'on se place ici délibérément dans une situation où l'asymétrie existante entre attaque et défense pourrait être réduite par l'intensité possible d'un conflit entre deux acteurs étatiques[75].

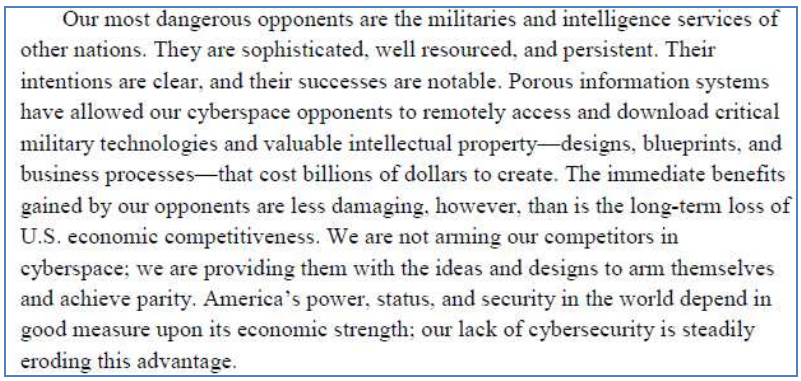
---

[72] http://news.softpedia.com/news/Germany-Attacks-China-For-Starting-The-Cyber-War-68994.shtml

[73] Thérèse Delpech, « La guerre informatique a commencé », *Politique Internationale*, N°130, Hiver 2010-2011, pp. 219-232.

[74] Martin C. Libicki, « Cyberdeterrence and Cyberwarfare », RAND, 2009, p. 7.

[75] Ibid, p. 33.



Our most dangerous opponents are the militaries and intelligence services of other nations. They are sophisticated, well resourced, and persistent. Their intentions are clear, and their successes are notable. Porous information systems have allowed our cyberspace opponents to remotely access and download critical military technologies and valuable intellectual property—designs, blueprints, and business processes—that cost billions of dollars to create. The immediate benefits gained by our opponents are less damaging, however, than is the long-term loss of U.S. economic competitiveness. We are not arming our competitors in cyberspace; we are providing them with the ideas and designs to arm themselves and achieve parity. America's power, status, and security in the world depend in good measure upon its economic strength; our lack of cybersecurity is steadily eroding this advantage.

Figure 10 : Extrait du rapport du CSIS sur la cybersécurité pour la 44ème présidence des États-Unis (CSIS – 2008)

Pour atteindre ces objectifs, au moins deux fonctions complémentaires sont indispensables :

➥ **Une fonction défensive** qui viserait à améliorer les capacités de protection des intérêts critiques défendus jusqu'à un niveau tel que le rapport coût/efficacité pour un attaquant devient trop élevé pour que l'agression présente un quelconque intérêt. En d'autres termes, il s'agit de rendre les attaques si coûteuses à réaliser pour des gains tellement limités que les acteurs malveillants seront amenés à y renoncer.

Pour être fonctionnelle, cette option suppose que quelques conditions initiales soient réunies :

⇒ ***Les moyens de défense et de protection doivent être fiables*** et leur efficacité doit être démontrée, au moins en partie, aux acteurs externes. La capacité des systèmes défendus à redevenir rapidement fonctionnels en cas d'attaque (leur *résilience*) participe également à la crédibilité de la défense et donc à la manœuvre de dissuasion. Il y a un équilibre (économique et opérationnel) à trouver entre la protection des systèmes et les outils et processus de récupération après un incident.

⇒ La défense numérique ne doit pas se limiter aux outils techniques et aux protocoles systémiques protégeant les outils, logiciels et infrastructures jugés critiques mais doit inclure l'élaboration des processus de récupération et de gestion des incidents visant à réduire autant que possible les conséquences d'une attaque et la durée de l'interruption des opérations (notion de récupération/résilience). La fonction de récupération comme complément aux moyens et systèmes de défense met un accent particulier sur la capacité des individus concernés et des organisations à réagir de façon efficace face à des attaques ou incidents : les exercices et entraînements constituent par conséquent un des outils clefs de la cyber-défense et de la dissuasion numérique.

⇒ Le coût de cette « défense » doit rester cohérent avec la valeur (économique ou stratégique) des cibles à protéger et le coût des dégâts engendrés par leur neutralisation (pendant des durées données). Le dimensionnement et l'organi-

sation du système de défense stratégique sont des décisions à prendre à la fois sur des bases financières mais également après une phase d'évaluation technique et politique des vulnérabilités. Il s'agit en effet de déterminer quels systèmes nécessitent quel niveau de protection sachant que les moyens de défense les plus efficaces sont dans les faits les plus coûteux. Les choix en matière de sécurité doivent reposer sur le coût relatif pour combler telle ou telle vulnérabilité par rapport à celui engendré par son exploitation.

- **Une fonction offensive** qui pourrait permettre de menacer un attaquant (i.e. : ses possessions, son territoire, ses outils/réseaux numériques ou de communication...) de représailles telles que les gains attendus d'une attaque s'avèreraient très inférieurs aux dégâts qui résulteraient des actions de rétorsion. La question se pose *in fine* de savoir si la capacité de représailles, qui sous-tend la validité de ce concept, est effectivement crédible dans l'environnement « cyber ». Cette fonction comprend une sous-fonction spécifique portant sur l'attribution des actes malveillants et l'identification des responsables.

Définitions relatives au cyberespace et spécificités de cet espace

Définitions

L'un des problèmes liés aux études et recherches portant sur le cyberespace vient de l'absence de définitions stabilisées et reconnues par l'ensemble des experts et acteurs du domaine. Cette difficulté concerne en particulier les incidents, attaques ou conflits affectant ou mettant en jeu des systèmes d'information.

A titre d'exemple, l'*East-West Institute* (EWI) a publié en avril 2011 un document proposant des définitions portant sur des situations, actions et procédures relatives aux systèmes d'information[76]. En particulier, ce document, sans définir la cyber-dissuasion au sens propre, mentionne l'existence d'« éléments dissuasifs dans le cyberespace » (*the cyber-deterrents*). *Un* ***élément cyber-dissuasif*** *est un mécanisme déclaré, présumé efficace pour décourager un cyber-conflit ou une action menaçante dans le cyberespace.*

Deux types d'éléments dissuasifs peuvent être envisagés :

- Une **cyber-capacité défensive** est une capacité permettant de se protéger efficacement contre une exploitation du cyberespace[77] ou des cyber-attaques[78] et de les repousser.

- Une **cyber-capacité offensive** est une capacité propre à déclencher une cyber-attaque

[76] « Russia-US Bilateral on Security – Critical Terminology Foundations », EWI, April 2011.

[77] Une exploitation du cyberspace consiste à exploiter une occasion ou une vulnérabilité numérique pour atteindre un objectif.

[78] Une cyber-attaque consiste à utiliser une cyber-arme afin d'endommager une cible désignée.

Plus généralement, ***la cyber-défense est définie comme un ensemble de capacités*** organisées pour se protéger contre des cyber-attaques, en atténuer les effets et revenir à l'état antérieur.

Ces définitions présentent l'avantage – mais aussi l'inconvénient – de rester très générales. De fait, elles couvrent des situations très variées qui peuvent concerner de nombreux systèmes ou cibles. A ce titre, elles ne permettent pas d'obtenir le niveau de différenciation indispensable pour élaborer finement un concept dissuasif adapté à l'espace numérique. Ainsi, le document de l'EWI qualifie de **cyber-guerre** « *des cyber-attaques autorisées par des acteurs étatiques contre des infrastructures dans le cyberespace, en conjonction avec une campagne gouvernementale* », quelle que soit l'intensité des opérations et leur impact réel sur les systèmes visés. Une telle définition peut conduire à considérer n'importe quelle cyber-attaque comme un acte de guerre[79].

Sans écarter définitivement les définitions proposées par l'EWI, nous préférons dans le cadre de cette étude utiliser celles, plus précises, proposées par le SGDSN[80] pour le cyberespace, la cyber-défense, la cyber-sécurité et la cybercriminalité (cf. infra).

Encadré 3 : Définitions dans le domaine cyber
(Défense et sécurité des systèmes d'information – Stratégie de la France – SGDSN 2011)

Cyberespace :

Espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques.

Cyber-sécurité :

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.

La cyber-sécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyber-défense.

Cybercriminalité :

Actes contrevenants 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.

Cyber-défense :

Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

[79] http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=WSJ_hp_LEFTTopStories

[80] « Défense et sécurité des systèmes d'information : La stratégie de la France », SGDSN, Février 2011.

Selon ces définitions, ***la cyber-dissuasion devrait appartenir au champ de la cyber-défense***, c'est-à-dire comprendre l'ensemble spécifique des mesures techniques et non techniques propres à dissuader les acteurs potentiels de chercher à porter atteint à la sécurité des systèmes d'information et de communication jugés essentiels.

Spécificités du cyberespace

Le cyberespace se distingue des autres milieux (terre, air, mer, espace) par plusieurs spécificités qui doivent être prises en compte afin de conduire une réflexion sur l'élaboration d'un concept de dissuasion qui lui serait propre.

A.– Extensivité et pervasivité de l'espace numérique

Les milieux habituels dans lesquels se déroulent les conflits armés (terre, air, mer et espace) ont leurs propres limites géographiques et sont généralement soumis à des règles et éléments de droit international. A l'inverse, le cyberespace n'a pas de délimitation géographique, même si son fonctionnement et son existence dépendent de systèmes physiques répartis sur l'ensemble du globe (routeurs, servers, câbles sous-marins..). En outre, il imprègne progressivement l'ensemble des activités humaines, même si de fortes disparités persistent entre les utilisateurs selon leur appartenance sociale, leurs secteurs d'activité ou encore leurs pays de résidence.

Enfin, il convient de souligner que le droit gouvernant les activités dans le cyberespace reste embryonnaire au regard de ceux régissant les activités dans les autres milieux, ou même le droit des conflits, et la nécessité de le développer demeure un sujet de débat[81].

B.– Convergence des systèmes de communication de données vers des protocoles uniques

Les protocoles utilisés pour gérer les flux de données numériques convergent rapidement vers la norme « *Internet Protocol* » qui tend à homogénéiser l'info-sphère et à intégrer progressivement l'ensemble des activités numériques dans Internet[82]. Cette homogénéisation est de nature à accroître les risques en matière de sécurité numérique[83].

Elle résulte toutefois d'une forte pression économique visant à réduire les coûts d'investissement aussi bien que ceux de fonctionnement. Il s'ensuit une interconnexion croissante des réseaux, des systèmes appartenant à des architectures numériques – en particulier les outils industriels ou des grands réseaux publics – et des acteurs privés ou publics qui les opèrent.

[81] « Perspectives for Cyber Strategists on law for cyberwar », Charles J. Dunlap Jr., Major General, USAF, Retired, voir aussi « Colloque INSEM – IDEST Les enjeux juridiques de la cyber-guerre », 16 juin 2011.

[82] http://en.wikipedia.org/wiki/Internet_Protocol

[83] Les risques résultant de la convergence sont détaillés plus loin.

C.– Absence de seuil technologique/opérationnel nécessaire à l'utilisation du cyberespace

Alors que la plupart des domaines technologiques nécessitent un certain degré d'expertise scientifique et la maîtrise d'outils techniques parfois complexes pour être utilisés à des fins offensives, l'espace numérique se distingue par la simplicité apparente de son utilisation.

Il suffit *a priori* d'acheter un ordinateur à quelques centaines d'euros, voire d'aller dans un cybercafé, pour accéder au cyberespace et y mener des actions potentiellement très agressives. Il n'est même pas nécessaire de savoir coder pour lancer un acte malveillant dans la mesure où de nombreux outils logiciels destinés à mener des actions offensives peuvent être acquis sur le marché noir lié à la criminalité numérique.

Ainsi, certains groupes criminels se sont spécialisés dans le développement et la vente de logiciels ou d'outils destinés à accéder et à pirater des réseaux distants voire à conduire des attaques massives contre des systèmes connectés à Internet. Ce marché noir, constitué au fil des années, est régi par la loi de l'offre et de la demande. Par exemple, une concurrence forte oppose les acteurs pour la maîtrise de réseaux de machines zombies. Selon le bulletin de juin 2009 sur la cyberdélinquance de la société Finjan[84], le coût d'« achat » de mille machines françaises infectées serait de 20 dollars. Cette étude détaille de façon didactique le marché des machines zombies en analysant une plate-forme existante : Golden Cash. Le prix de mille machines zombies varierait sur cette plate-forme de 5 dollars à 100 dollars en fonction du pays abritant les ordinateurs concernés. Des prix plus élevés peuvent, cependant, être pratiqués dans le cadre d'opérations ciblées et montées par des intermédiaires ayant acheté les machines au prix de gros.

L'absence de seuil technologique dans le domaine numérique a une conséquence majeure : il existe une unicité des moyens et outils techniques employés dans le cyberespace qui se traduit par une interopérabilité quasi-totale entre les systèmes. Ainsi, qu'il s'agisse des logiciels ou des systèmes physiques les plus élémentaires ou des plus performants, il apparait difficile si ce n'est impossible de séparer (*ségréger*) les activités numériques sur la base des niveaux technologiques, des utilisateurs concernés ou des modes opératoires.

D.– Les échanges de logiciels et moyens informatiques sont relativement mal encadrés par les accords et outils de contrôle des matériels sensibles

Alors qu'il existe de nombreux accords visant à maîtriser la dissémination des technologies, des composants et des matériels militaires, de ceux à caractère sensible ou ayant une application duale, les normes de non-prolifération et de contrôle des armements ne sont pas conçues pour contrôler la diffusion des moyens qui peuvent être employés pour des opérations offensives ou défensives dans l'espace numérique.

Il convient par exemple de noter que l'accord de Wassenaar ne prend pas en compte les logiciels du domaine public[85]. De fait, il revient à chaque État de définir les règles

[84] http://www.finjan.com/Pressrelease.aspx?id=2280&PressLan=2139&lan=3

[85] Arrangement de Wassenaar, « Note générale sur les logiciels ».

limitant l'acquisition ou la vente des logiciels et moyens informatiques qu'il considère comme sensible.

Par ailleurs, l'exemple des outils de cryptologie (cryptage et cryptanalyse) montre qu'il n'existe pas en la matière de consensus international sur le contrôle des technologies numériques. Ainsi, pour ce qui concerne la France, ces moyens ont été largement libéralisés à la fin des années 1990 et retirés de la liste des armes de guerre et des matériels assimilés.

Cette situation s'explique assez bien si l'on considère le caractère extrêmement dual des systèmes et logiciels concernés ainsi que le fait que, pour l'essentiel, les finalités d'utilisation sont pacifiques. De la même manière que l'espace extra-atmosphérique, les difficultés en termes de contrôle sont également liées au fait que le cyberespace est profondément transnational et que les mesures restrictives le concernant auraient des conséquences économiques majeures. Pour autant, comme en matière de gouvernance des activités numériques, il convient sans doute pour faciliter la lutte contre les risques numériques les plus graves de définir des règles internationales qui permettraient de responsabiliser les États et les principaux acteurs.

Quelles leçons peut-on tirer de l'exercice de la dissuasion dans le domaine nucléaire ?

Applicabilité des concepts de dissuasion nucléaire

La plupart des concepts de la dissuasion nucléaire sont théoriquement applicables au domaine cybernétique, parce que ce ne sont pas des concepts propres au domaine nucléaire.

En effet, il existe au fond assez peu de concepts spécifiques à la dissuasion nucléaire. La plupart de ces concepts sont en effet des adaptations au domaine nucléaire de concepts issus de la stratégie classique. Les notions de « dissuasion », de « représailles », « d'interdiction » font partie du vocabulaire stratégique depuis des siècles. Il en est de même pour certains des principaux concepts tels que par exemple le tir d'avertissement (le coup de semonce[86]), la notion d'escalade et ses dérivés (seuils et coupe-feux, maîtrise de l'escalade, etc.), l'idée de frappe à vocation « désarmante », et les divers raffinements qui ont été apportés aux politiques de ciblage (contre-C3, centres de pouvoir, etc.).

Les concepts sous-jacents aux expressions « représailles [ou riposte] massive[s] » et « riposte graduée » ne sont pas non plus fondamentalement des innovations de la stratégie nucléaire.[87] Dans le premier cas, il s'agit d'exercer contrer l'adversaire des représailles sans commune mesure avec l'enjeu du conflit – ce qui n'est aucunement une innovation historique.[88] Dans le second cas, il s'agit, dans son sens originel (document

[86] L'expression *« shot-across-the-bow »*, qui provient de la stratégie navale, était fréquemment employée au temps de la Guerre froide pour évoquer l'idée d'une frappe de démonstration ou d'avertissement.

[87] Dans une logique de dissuasion, l'expression « riposte massive » est une meilleure traduction de *« massive retaliation »* que celle de « représailles massives ».

[88] Même la notion de représailles massives contre les populations adverses ne date pas de l'ère nucléaire : le premier bombardement de Tokyo (18 avril 1942) relevait déjà d'une forme de représailles contre-citées réalisée

MC 14/3, 1968), de choisir, face à une agression, entre trois modes d'action possibles : soit de riposter au niveau de violence choisi par l'adversaire, soit de procéder à une escalade graduelle et contrôlée, soit de riposter massivement.

La « dissuasion élargie » applique au domaine nucléaire l'idée selon laquelle il est possible de décourager un agresseur de s'en prendre à un État faible en faisant savoir qu'il dispose d'un puissant protecteur – logique aussi ancienne que les alliances militaires.

Même l'expression « intérêts vitaux » peut être assimilée à celle des « œuvres vives » d'un navire (cette dernière expression était d'ailleurs fréquemment employée dans la réflexion stratégique française des années 1970).[89]

La dissuasion nucléaire a bien entendu innové, en donnant une résonance beaucoup plus forte à certains de ces concepts : c'est le cas notamment de la notion de « seuil » nucléaire, dont l'importance du franchissement a donné naissance au « non-emploi en premier »[90] ; et c'est également le cas des représailles massives, assimilées à la capacité de destruction quasi-instantanée des villes adverses, ou encore de la « dissuasion du faible au fort », qui n'a réellement de sens que dans le domaine nucléaire.

Mais ces concepts sont théoriquement applicables à d'autres domaines, dont, pourquoi pas, celui du cyberespace.

Obstacles et difficultés

Dans les faits, il existe de nombreux obstacles à l'application au domaine cybernétique des concepts de la dissuasion nucléaire – comme pour l'application d'autres concepts stratégiques.

A.– La question du dialogue dissuasif et de la menace de représailles

La dissuasion par menace de représailles est *a priori* difficilement applicable au domaine informatique. Les principales raisons sont bien connues et précisées dans le corps de cette étude.

Elles tiennent pour l'essentiel à cinq facteurs :

(1) La difficulté d'identifier l'adversaire avec certitude, qui à l'évidence pose problème pour la conduite même d'un « dialogue dissuasif ».[91] Elle rend particulièrement difficile une « dissuasion informatique élargie » : quel État s'engagerait pour un autre à prendre la responsabilité de la riposte sans certitude quant à l'origine de l'attaque ?

avec des moyens aériens. Les autres bombardements urbains de la Seconde Guerre mondiale (Londres, Dresde, Berlin, Tokyo…) relevaient de la coercition et non des représailles.

[89] De même l'expression « tous azimuts » provient-elle du vocabulaire des artilleurs.

[90] Même si l'on pouvait avoir un « non-emploi en premier de fait » (exemple des armes chimiques au cours de la Seconde Guerre mondiale).

[91] Selon un expert estonien, en 2011 les spécialistes occidentaux n'avaient toujours pas achevé la cartographie des attaques de 2007.

(2) La difficulté de maîtriser les effets des représailles. L'opérateur ne peut non plus avoir de certitude quant à la réussite de sa « frappe », ni au demeurant être certain que ses effets ont atteint ses objectifs.

(3) L'invisibilité des agents et l'absence d'effets physiques (au moins immédiats), qui empêchent, dans la plupart des cas, de conférer à l'arme informatique un caractère « effrayant ».

(4) Le très grand nombre des acteurs susceptibles d'être concernés, qui empêche d'envisager par avance une dissuasion « sur mesure ».[92]

(5) Le besoin de conserver une grande confidentialité sur l'existence même de certains des outils à la disposition du défenseur.[93]

De ce fait, l'exercice d'une menace crédible de représailles, de nature à être dissuasive, reste, sans être totalement impossible, très problématique.

B.– La question de l'escalade et de sa maîtrise

La définition d'un éventuel « seuil cybernétique » pose évidemment problème. Les moyens informatiques étant utilisés dans toutes les activités humaines, et *a fortiori* guerrières, il est impossible d'imaginer qu'un tel seuil puisse être aussi facilement identifiable et avoir la même valeur que le seuil nucléaire (ou que l'emploi d'autres moyens tels que les armes chimiques). Une norme de « non-emploi en premier » n'aurait donc guère de sens.

Tout au plus peut-on imaginer un accord implicite ou explicite entre deux adversaires pour ne pas avoir recours en premier à la lutte informatique offensive (même si l'un des deux protagonistes pourrait facilement rompre cet engagement en utilisant des intermédiaires ou des acteurs non étatiques). De même peut-on imaginer un accord sur le non-ciblage par des moyens informatiques de certaines installations civiles dont la perte de contrôle serait susceptible d'occasionner de nombreuses victimes ou des dommages importants au fonctionnement de l'État – barrages, contrôle aérien, centrales nucléaires, etc.[94] La même logique est applicable – par exemple dans le cas sino-américain – au domaine financier.[95]

Par ailleurs, l'invisibilité des agents (et de leurs effets dans de nombreux cas) rend peu crédible l'idée d'une escalade maîtrisée dans laquelle les intentions des protagonistes sont clairement compréhensibles. C'est pour cela, entre autres raisons (on peut y ajouter

[92] Sur ce dernier point voir Patrick Morgan, « Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm », National Academies of Science, Computer Science and Telecoms Board, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policies, 2010.

[93] Ceci peut également faire hésiter à employer certains moyens en riposte, de peur que leur utilisation ne compromette ensuite les capacités de renseignement du défenseur. Sur ce point voir Eric Sterner, « Deterrence in Cyberspace: Yes, No, Maybe? », in Returning to Fundamentals: Deterrence and US National Security in the 21st Century, The George C. Marshall Institute, 2011.

[94] Un parallèle pourrait être l'accord indo-pakistanais sur la sanctuarisation des installations nucléaires des deux pays.

[95] Aux dires de Richard Clarke, M. Bush avait d'ailleurs interdit le ciblage du système bancaire et financier, en raison du risque de perte de confiance des acteurs.

la grande rapidité de conception et de réalisation des agents, contrairement à ce qui se passe dans le domaine militaire), qu'il apparaît *a priori* difficile d'envisager une dissuasion purement « symétrique ».

Enfin, la distribution très large des compétences et des agents rend inapplicable un concept de « frappe contre-forces » à vocation désarmante. Notons que ceci implique, *ipso facto*, que tout État ayant des capacités importantes dans ce domaine disposerait par définition d'une aptitude à la « frappe en second ».

C.– La question de l'ascension aux extrêmes et de la « riposte massive »

La menace d'une « ascension aux extrêmes » a-t-elle un sens dans le domaine informatique ? Pour que ce soit le cas, il faut pouvoir imaginer qu'il est possible d'exercer des dommages inacceptables à un État à l'aide de tels moyens[96]. Or ceci ne semble pas crédible aujourd'hui.[97]

Encadré 4 : Dissuasion spatiale

Autre exemple de tentative d'application des concepts de dissuasion à un milieu spécifique, l'Espace se caractérise par le fait qu'il s'agit d'un domaine de souveraineté partagée entre les États. Il en découle que la seule reproduction des principes et schémas mis en place dans le domaine nucléaire n'est ni souhaitable, ni efficace.

Ainsi, Washington a articulé pour l'Espace un concept et une politique dans le domaine qui reposent sur quatre composantes[1] *:*

- Le développement de normes applicables aux « actions responsables » ;
- Le développement de partenariats internationaux conduisant à des accords de défense collective (une attaque contre un membre de l'accord sera interprétée comme une attaque contre l'ensemble des signataires) ;
- L'accroissement des niveaux de résilience (capacité de fonctionnement en mode dégradé et de retour au fonctionnement normal dans un délai raisonnable) ;
- Le maintien en état de préparation à des ripostes rapides en cas d'attaque contre les systèmes spatiaux, la riposte n'étant pas nécessairement limitée au domaine spatial.

[96] La mise hors d'état de fonctionner des infrastructures et des réseaux jugés critiques pourrait relever des « dommages inacceptables », en ce qu'elle affecterait sans doute gravement la souveraineté de l'État, qui fait traditionnellement partie des intérêts vitaux. Une autre hypothèse serait une série d'attaques massives sur des installations civiles occasionnant un très grand nombre de victimes civiles, à supposer qu'une telle option soit techniquement accessible (cf. infra.).

[97] Il existe peu d'exemples de piratage réussi d'infrastructures civiles majeures, ayant causé des dommages significatifs : outre Stuxnet, on peut mentionner le cas de la destruction d'un pipeline soviétique par une bombe logique (1982). L'un des cas les plus fréquemment cités est celui du barrage d'Itaipu (2009), mais outre le fait que cet incident n'a pas causé de victimes, il est loin d'être certain qu'il ait été dû à des attaques informatiques (Marcelo Soares, « Brazil Blackout Traced to Sooty Insulators, Not Hackers », *Wired*, 9 novembre 2009).

Réflexions sur les conditions d'application d'une dissuasion numérique

Plusieurs éléments rendent difficile l'exercice de la cyber-défense

Comme nous l'avons vu, l'espace numérique – y compris les moyens, systèmes et logiciels qui lui sont associés – se distingue des autres milieux par sa pervasivité[98], les difficultés liées à son contrôle, la facilité d'emploi des outils qui le composent et son caractère profondément transnational.

Si l'on considère l'activité de défense dans cet espace – et sa possible extension à des actions dissuasives à caractère offensif – quelques éléments viennent rendre plus difficile le traitement des incidents ou des attaques menées depuis ou vers le cyberespace.

A.– Difficultés liées à l'identification des auteurs et des acteurs impliqués

Alors que face à une action offensive sur terre, sur mer, dans l'air ou dans l'espace – en particulier dans le cas du tir d'un missile balistique –, les moyens d'observation et les capteurs de renseignement peuvent permettre de localiser presque immédiatement l'origine géographique de l'action et assez rapidement, dans la mesure où les capteurs de renseignement sont efficaces, d'établir l'identité des acteurs, ce processus est rendu complexe par la nature même de l'espace numérique.

En effet, l'identification permise par les capteurs techniques porte sur les ordinateurs d'où sont issus les données incriminées. Or, de multiples rebonds d'une machine à une autre peuvent être mis en place pour dissimuler l'origine réelle d'une agression. Au-delà du deuxième rebond, il devient très difficile de remonter jusqu'à l'ordinateur source. Le délai nécessaire à l'identification constitue également un facteur important, surtout lorsque les attaques sont transfrontières et nécessitent le concours des autorités locales pour mener l'enquête sur la ou les personnes responsables.

Même dans le cas d'événements analysés en détail dans la durée, il reste parfois difficile de démontrer le rôle précis de certains acteurs alors qu'il existe de fortes présomptions sur leur implication. Ce fût, par exemple, le cas du groupe de hackers russes « *Nashi* » dans le cas de l'attaque contre l'Estonie en 2007.

Enfin, il est fréquent que des groupes d'origines différentes et situés dans des zones géographiques distantes participent – de façon coordonnée ou pas – à une même opération. Cela peut inclure des militants politiques, des spécialistes travaillant pour des organisations criminelles ou des groupes paragouvernementaux, comme dans le conflit Géorgie-Russie en 2008[99].

[98] Sa présence est permanente dans tous les domaines de l'activité humaine. http://fr.wiktionary.org/wiki/pervasif

[99] Voir aussi Alexandre Klimburg, « Mobilizing Cyber Power », *Survival*, January 2011, sur le rôle de groupes de hackers russes et chinois dans des actions de soutien à la politique de leur gouvernement.

B.– Les conséquences réelles et de long terme d'un acte malveillant sont devenues complexes à estimer, tout comme il est difficile d'établir précisément a posteriori le mécanisme d'une attaque et sa finalité

L'effet immédiat mais également les conséquences à long terme d'une action hostile dans le cyberespace sont souvent difficiles à évaluer. De nombreux logiciels malveillants sont spécifiquement conçus pour ne pas être décelés (chevaux de Troie, *keyloggers*, *spywares*). Leur fonctionnement consiste à mettre en place des mécanismes qui auront un effet décalé dans le temps ou des moyens destinés à capter et à transmettre vers le pirate des données transitant ou stockées sur la machine concernée.

La compromission d'un système pour l'intégrer dans un réseau d'ordinateurs zombies (*botnet*) se fait le plus souvent à l'insu de son propriétaire. L'emploi de ces ordinateurs zombies dans des actions offensives ou pour participer à des opérations de type *phishing* peut d'ailleurs ne pas être détecté par ce dernier. D'une manière générale, dans le cyberespace, la furtivité est devenue la règle alors que l'action immédiatement destructrice s'avère être une exception.

Même lorsqu'elles sont volontairement ciblées, les cyber-attaques utilisant une faille donnée peuvent induire des effets collatéraux partout où cette vulnérabilité est présente. Ce fût, par exemple, le cas de Stuxnet et de ses conséquences sur le fonctionnement des machines-outils Siemens en Chine. La compromission de quelques ordinateurs dans un parc informatique oblige à vérifier toutes les machines du parc avant de pouvoir procéder à une évaluation générale d'impact.

Une ambigüité existe aussi souvent dans l'appréciation de l'évolution des moyens utilisés pour les attaques numériques. Bien que les types d'outils malveillants (ver, virus, *spyware*, keylogger, chevaux de Troie…) soient en nombre limité – ils ne se renouvellent d'ailleurs que peu depuis une dizaine d'années – la connaissance des chemins d'attaque utilisés et des moyens employés pour permettre la diffusion de ces logiciels demande la plupart du temps une enquête poussée, complexe techniquement et lente. Les résultats de ces efforts techniques sont incertains et ne permettent parfois pas de démonter totalement le mécanisme d'attaque. Une attaque réussie ne laisse souvent pas suffisamment de traces numériques pour, si elles sont exploitées, permettre de reconstituer fidèlement l'enchaînement des événements.

La finalité d'une action hostile se déduit le plus souvent de l'identification des auteurs et de l'évaluation des conséquences. Dans certains cas, les attaques font l'objet de revendications explicites. Les deux premiers éléments étant le plus souvent difficiles à établir, il reste la revendication, qui peut parfois avoir été conçue pour brouiller les pistes menant aux malfaiteurs. Dans le cas de la compromission de systèmes informatiques du ministère français de l'Économie et des finances fin 2010, les investigations n'avaient, par exemple, pas permis de déterminer la finalité de l'attaque.

C.– D'autres obstacles techniques et opérationnels propre au cyberespace sont susceptibles de réduire la crédibilité d'une dissuasion numérique

Dans un dialogue dissuasif, non seulement il faut disposer de capacités défensives, offensives et d'attribution, mais il faut également établir leur réalité et leur fiabilité. Il s'agit en somme d'établir une « crédibilité dissuasive ».

Problème particulièrement complexe dans le cyberespace marqué par l'ambigüité et par le doute sur l'origine et la finalité des attaques, quand celles-ci sont avérées. Le virus Conficker en est un bon exemple : de 2008 à 2009, il a démontré une remarquable capacité de dissémination (changement de configuration) au point d'affecter plusieurs millions d'ordinateurs. Mais sa source n'a pas été identifiée et aucun pays (mais était-ce un pays ?) ne peut se prévaloir d'avoir acquis cette capacité particulière.

La structure actuelle de l'Internet et des systèmes d'information fait obstacle à toute espèce de démonstration en grandeur réelle d'une capacité offensive. Lancer ouvertement une attaque contre un système d'information particulier – un système propriétaire par exemple – à des fins de démonstration permet *a priori* d'apporter des preuves convaincantes de l'efficacité des capacités offensives et défensives de celui qui conduit un tel exercice mais peut entraîner des dommages collatéraux importants dont il faudra assumer la responsabilité. Une démonstration en réseau fermé n'est pas de nature à convaincre de la même efficacité en réseau ouvert.

En outre, alors que revendiquer une capacité d'attaque sans apporter de preuve nuirait à la crédibilité d'un outil à vocation dissuasif, apporter des preuves précises et détaillées de la crédibilité de cette capacité dévoile le savoir-faire utilisé – avec la possibilité pour les acteurs concernés d'élaborer des moyens de protection – et fait courir le risque d'être suspecté si des attaques du même type son perpétrées.

Dans le cas du ver Stuxnet, par exemple, l'analyse détaillée du code et des traces laissées par l'attaque démontre le haut niveau de technicité et suggère des auteurs potentiels[100], mais ne fournit pas de preuve définitive de l'implication de tel ou tel acteur. Et même une déclaration personnelle[101] allant dans le même sens ne constitue pas une preuve suffisamment solide pour justifier des représailles.

Le cas de Stuxnet soulève d'autres questions : pourquoi le même niveau de technicité n'a-t-il pas été utilisé pour dissimuler les traces, voire pour détruire le ver (son code) une fois l'attaque exécutée afin d'empêcher la prolifération du savoir-faire utilisé ? Mais en supprimant les traces, l'auteur réduit les possibilités de pouvoir s'attribuer le bénéfice de cette capacité offensive. Ce qui s'est passé avec Stuxnet participe peut-être de la recherche d'une solution médiane : démontrer sa technicité quitte à la laisser disséminer (ce qui peut suggérer qu'on en a bien plus en réserve) et fournir des indices suffisamment nombreux et concordants pour que les personnes averties sachent à quoi s'en tenir…

Un autre volet de l'élaboration de cette « crédibilité dissuasive » tient à la fiabilité des déclarations que l'on peut faire : il faut prendre garde – dans un espace caractérisé par un fort degré de transparence et une vitesse importante de circulation des informations – à ne pas être démenti par les faits, car alors non seulement la dissuasion n'a pas fonctionné mais la crédibilité de l'auteur peut être durablement remise en cause. ***La perte de « réputation » dans l'espace numérique est de nature à réduire les bénéfices potentiels d'une posture dissuasive.***

[100] Discussion personnelle avec des responsables de la DGA en matière de Lutte informatique (note d'Alain Esterle).

[101] Le général israélien Gabi Ashkenazi a affirmé, lors de son départ à la retraite, être le père du ver Stuxnet.

La société américaine HBGary de technologie en logiciels sécurité a, par exemple, indiqué en 2010 pouvoir identifier des pirates grâce à ses outils d'analyse des informations véhiculées par les réseaux sociaux. Début 2011, elle annonce en outre avoir infiltré le groupe *Anonymous* et disposer d'une liste de ses membres qu'elle s'apprête à fournir au FBI. En réponse, le groupe *Anonymous* attaque le site d'HBGary et met en ligne des dizaines de milliers de mails échangés entre HBGary et ses clients, notamment des banques, montrant leurs intentions de mener une « sale campagne » contre *Wikileaks* sur la base de faux documents, de campagnes de désinformation, et d'actions d'espionnage. Simultanément, *Anonymous* indique que les personnes désignées par HBGary ne sont pas membres du groupe et que les méthodes d'identification utilisées par HBGary s'avèrent techniquement douteuses. A la suite de ces révélations, les clients d'HBGary prennent leurs distances vis-à-vis de la société et le gouvernement américain engage des enquêtes sur l'ensemble des contrats passés entre cette entreprise et les services américains de la défense.

Une situation analogue a mis aux prises l'OTAN et le même groupe *Anonymous*. Au printemps 2011, l'OTAN publie un rapport décrivant les enjeux des évolutions récentes en matière de cyber-activisme, et portant notamment sur les opérations de *Wikileaks* et sur celles du groupe de hackers *Anonymous*[102]. Le rapport suppose que, confronté à de nouvelles parades et à des opérations de police le visant, le groupe *Anonymous* ne pourra pas poursuivre ses activités à long terme, et que ces membres seront poursuivis. En réponse, *Anonymous* a accentué ses attaques contre des sites officiels, notamment le FBI. Fin juillet 2011, le groupe a fait savoir qu'il avait pénétré les sites de l'OTAN et subtilisé l'équivalent d'1 gigaoctet de documents dont quelques uns ont été mis en ligne à titre de preuve, accompagnés un message tournant l'Alliance en ridicule[103].

On peut remarquer que cette action, sans s'intégrer dans le cadre d'une démarche dissuasive, peut sans doute être assimilée à une tentative d'escalade dans le contexte d'un conflit de longue durée entre les États et un groupe pratiquant des activités illégales[104]. De fait, si le milieu concerné est spécifique (le cyberespace plutôt que le milieu terrestre), ce type de confrontation – et les méthodes employées – ne sont pas sans rappeler la lutte contre les organisations criminelles transnationales ou nationales.

L'absence d'exemple documenté de confrontation entre États dans le cyberespace ne signifie pas que ce type de conflit n'existe pas. En revanche, il montre que les actions offensives interétatiques restent, pour un certain nombre de raisons – on peut citer en vrac la volonté de ne pas dévoiler ses capacités, celle d'éviter des représailles physiques ou économiques ou encore d'entretenir le doute sur les auteurs –, discrètes. Plus sans doute que dans les autres milieux, les actions des spécialistes du renseignement et des agents des services d'espionnage prennent une place prépondérante dès lors qu'il s'agit d'actions offensives dans le cyberespace. Cette réalité doit être prise en compte dans la perspective de la mise en place d'un discours et d'une posture de dissuasion.

---

[102] http://www.nato-pa.int/default.asp?CAT2=2391&CAT1=16&CAT0=2&COM=2443&MOD=0&SMD=0&SSMD =0& STA=&ID=0&PAR=0&LNG=1

[103] « Yes, we haz more of your delicious data. You wonder where from. No hints, your turn. You call it war; we laugh at your battleships. »

[104] Fin juillet la FBI a aussi déclaré avoir arrêté 14 membres d'*Anonymous* responsables de l'attaque contre le site de paiement en ligne PayPal en Décembre 2010. Ce qui, à supposer que la culpabilité des auteurs soit confirmée, donne une idée du délai nécessaire à l'attribution d'une attaque ayant un caractère purement national.

Elle a des conséquences notamment en matière d'organisation dans le registre défensif comme dans celui des moyens offensifs. Deux principales alternatives se dégagent en la matière :

- Conformément au *Livre Blanc sur la Défense et la Sécurité Nationale*[105], la France a choisi de séparer les deux fonctions : l'Agence Nationale de la Sécurité des Systèmes d'Information pour la partie défensive, et le ministère de la Défense et la DGSE pour la partie offensive.

- A l'inverse, les États-Unis ont préféré confier les deux fonctions au même organisme (c'est-à-dire la National Security Agency).

Notons enfin que les interdépendances industrielles existantes dans le domaine informatique ainsi que le fait que des coopérations internationales paraissent indispensables afin de rendre plus efficaces les fonctions d'alerte, d'attribution et de riposte à des attaques devraient également avoir des conséquences pour la construction du discours dissuasif et la mise en place d'une posture correspondante.

Réflexions politiques et stratégiques sur la mise en place d'un concept de dissuasion dans le milieu numérique

Le principe de dissuasion, dans la mesure où il peut concerner un spectre large de menaces, s'applique aussi bien au domaine judiciaire qu'à celui des affaires militaires ou stratégiques. De fait, dans le domaine numérique, il ne peut être proposé que dans la mesure où les risques qui peuvent se concrétiser sont susceptibles d'avoir un impact important sur la sécurité – voire sur la survie – de la Nation. Il doit donc lever, d'une façon ou d'une autre, les difficultés identifiées précédemment.

Les problèmes qui existent pour identifier l'auteur (ou les auteurs) d'une attaque, évaluer les impacts subis, reconstituer en détail les événements et en établir les finalités sous-jacentes, le tout dans un contexte d'interconnexion générale des réseaux et des acteurs, distinguent le cyberespace des autres milieux dans lesquels des démarches de dissuasion ont pu être élaborées. La démarche dissuasive dans le cyberespace, si elle est possible, ne peut se construire uniquement par référence à des démarches existantes[106] : elle doit se bâtir *sui generis*.

Ainsi en va-t-il de l'exercice de la domination et du pouvoir dans le cyberespace. En suivant Daniel T. Kuel, on peut dire que le pouvoir se fonde ici sur « *la capacité à utiliser le cyberespace pour prendre un avantage et influencer les événements dans d'autres environnements opérationnels et à travers des instruments de pouvoir* »[107]. Le point important est que le seuil d'entrée dans le cyberespace est si bas que, contrairement aux autres domaines classiques (terre, mer, air, espace), n'importe quel pays, organisation, groupe social ou même individu peut prétendre à venir y jouer un rôle non négligeable. Dans les domaines classiques, les conflits s'arrêtent souvent par épuisement des ressources de l'un des adversaires, alors que la plupart des actions hostiles

[105] « Défense et Sécurité Nationale – Le Livre Blanc », Ed. Odile Jacob, juin 2008, pp. 182 et 207.

[106] Comme le dit Martin C. Libicki dans le rapport de la Rand « Cyberdeterrence and cyberwar » : « Attemps to transfer policy constructs from other forms of warfare will not only fail but also hinder policy and planning. »

[107] Daniel T. Kuehl, « From cyberspace to cyberpower: Defining the problem », in Franklin D. Kramer, Stuart Starr & Larry K. Wentz, « Cyuberpower and National Security (Washington, D.C.: National Defense UP, 2009).

dans le cyberespace sont à coût quasiment nul. Il s'ensuit que, selon Joseph S. Nye Jr., le pouvoir dans le cyberespace est par nature diffus, partagé entre de multiples acteurs[108].

A.– Quelles options possibles

La définition d'une doctrine de dissuasion informatique peut s'inspirer des réponses apportées à de telles difficultés dans d'autres domaines.

En effet, la dissuasion vis-à-vis d'une agression cybernétique présente les mêmes difficultés que d'autres formes de dissuasion. Le caractère particulièrement problématique de la question de l'identification rappelle la difficulté de dissuader le terrorisme nucléaire. Et celui de la maîtrise des effets n'est pas sans analogie avec l'utilisation des armes biologiques (ce n'est pas pour rien que l'on parle de « virus » et « d'infection »). L'invisibilité, dans de nombreux cas, des armes informatiques, est une autre analogie possible avec le domaine biologique.[109]

On peut donc imaginer de s'inspirer des réponses qui ont été apportées face aux difficultés méthodologiques de la dissuasion dans ces domaines : face à la menace terroriste, la dissuasion par interdiction et la dissuasion « indirecte » ; face à la menace biologique, la dissuasion « asymétrique ».

- La ***dissuasion par interdiction*** semble assez bien adaptée à la menace cybernétique. Elle consiste à faire savoir à l'adversaire (en l'espèce, « à qui de droit ») que le pays cible dispose de moyens de défenses actives et passives de nature à l'empêcher d'atteindre ses objectifs. Si la « communication » de l'état de ces défenses n'irait pas de soi, on peut imaginer que l'adversaire serait renseigné sur cet état du fait d'éventuelles tentatives d'intrusion de sa part.

- Une ***dissuasion « indirecte »*** consisterait à menacer l'État qui aurait organisé, sponsorisé ou facilité une attaque informatique, à condition bien sûr de pouvoir retracer l'origine de l'attaque. C'est ici que, comme dans le domaine du terrorisme nucléaire, la mise en avant d'éventuels progrès dans le domaine de l'attribution peut être un élément significatif de la dissuasion.

- Elle serait complétée par l'exercice d'une ***dissuasion envers les exécutants*** ou relais de l'attaque (à condition que ceux-ci soient accessibles – ce qui ne serait évidemment pas toujours le cas).[110] Contrairement au cas du terrorisme extrémiste, on suppose que la peur des représailles (judiciaires ou autres) pourrait être efficace envers un individu ou un groupe exécutant une attaque informatique massive.

- Comme face à la menace biologique, une ***dissuasion « asymétrique »*** est envisageable : dans l'hypothèse d'une attaque massive dont l'agresseur serait bien identi-

[108] Joseph S. Nye Jr, « CyberPower », Harvard Kennedy School, May 2010.

[109] Outre le fait, bien sûr, qui n'est pas pertinent ici, que l'arme biologique soit interdite par une convention internationale, ce qui interdit un mode d'exercice « symétrique » de la dissuasion.

[110] On s'inspire ici de ce que les États-Unis avaient fait en 2003, pour des raisons différentes, face à l'hypothèse d'une menace chimique ou biologique irakienne.

fié, et afin de maîtriser au mieux les effets de la riposte, il serait logique d'envisager une réponse « cinétique » (représailles conventionnelles).[111]

➡ A l'extrême, si l'on veut bien admettre que les intérêts vitaux d'un pays pourraient être mis en cause par des moyens informatiques, la ***dissuasion nucléaire*** elle-même pourrait être pertinente.[112] Il faut pour cela admettre qu'il est possible soit de causer des dommages massifs à des infrastructures civiles (avec des conséquences majeures pour les populations), soit de paralyser des infrastructures étatiques (avec des conséquences majeures pour le fonctionnement de l'État et l'exercice de sa souveraineté). Ceci reste à démontrer.

Dans les cas où la dissuasion « symétrique » (arme informatique contre arme informatique) pourrait fonctionner, il pourrait être fécond de s'inspirer de ce qui reste aujourd'hui l'un des concepts stratégiques les plus aboutis : le MC 14/3 de l'OTAN (1968), qui comme il a été rappelé plus haut comprend trois niveaux possibles de riposte : (a) la défense directe au niveau choisi par l'adversaire, (b) l'escalade délibérée, et (c) la riposte massive. En d'autres termes, il s'agirait pour un État disposant de capacités reconnues dans le domaine cybernétique de faire savoir, tout comme l'OTAN le faisait dans les années 1970 et 1980, qu'en cas d'attaque informatique, il se réserverait la possibilité, soit de riposter au niveau choisi par l'agresseur, soit – au vu des enjeux du conflit et des intentions présumées de l'adversaire – de procéder à une escalade délibérée (symétrique ou asymétrique), soit d'exercer d'emblée des dommages majeurs à l'agresseur.

B.– Il paraît essentiel de supposer que la cyber-dissuasion s'appuie *a priori* sur des mesures de rétorsion de même nature que les actes malveillants contre lesquels elle est censée agir de façon à mieux contrôler les risques d'escalade

Dans l'exercice de la dissuasion numérique, il paraît nécessaire d'écarter *a priori* l'utilisation physique de la force comme réponse appropriée à un acte numérique malveillant[113]. Ceci est d'autant plus important que le spectre des acteurs qui pourraient subir les mesures de rétorsion est extrêmement varié allant d'État jusqu'à des individus plus ou moins isolés.

En effet, il apparaît évident que des mesures de rétorsion qui seraient adaptées pour punir un État responsable d'un acte numérique malveillant contre un des groupes d'intérêts jugés critiques, ***pourraient être disproportionnées voire, dans certaines circonstances***[114]***, inadéquates pour répondre aux actions d'une personne, d'un groupe criminel ou d'une organisation terroriste*** et, ainsi, éviter une nouvelle attaque ou des actes de représailles conduisant à une escalade.

---

[111] C'est d'ailleurs, comme on le sait, ce qu'envisagent désormais les États-Unis.

[112] A cet égard, le concept français dans sa formulation traditionnelle (riposte nucléaire si les intérêts vitaux sont atteints « quels que soient les moyens adoptés » par l'adversaire) apparaît particulièrement bien adapté.

[113] En dernier ressort toutefois, il faut considérer que certaines atteintes aux intérêts vitaux peuvent conduire à une riposte « disproportionnée ». Cf. §1.2.3.

[114] Par exemple, si le groupe concerné ne possède pas de structures vulnérables ou dont la perte aurait des conséquences existentielles.

La ***symétrie complète des moyens utilisés et des effets recherchés*** est envisageable conceptuellement si l'on considère que les développements d'Internet et des outils numériques et de communication se poursuivront de façon relativement homogène au niveau mondial et, *a fortiori*, au sein des administrations et des entreprises du secteur privé.

En effet, cette hypothèse semble globalement devoir se vérifier, dans la mesure où :

- Les bénéfices (au moins économiques) du développement des technologies numériques sont largement supérieurs aux risques encourus par leur utilisation. En particulier, dans une économie mondialisée à l'extrême, la déconnexion volontaire aura un coup élevé en termes d'accès aux marchés, de facilité financière, d'échanges commerciaux, scientifiques ou même culturels…

- De nombreux outils/objets (y compris des moyens lourds de production ou de transport) devraient à l'avenir fonctionner soit sur la base d'une connexion fonctionnelle avec un réseau de communication adossée à internet, soit, *a minima*, avec des systèmes d'exploitation commerciaux. Le cas des machines-outils infectées par Stuxnet montre que la numérisation des processus industriels laisse peu de place à la liberté de détenir des moyens autonomes utilisant des systèmes numériques uniques de conception locale.

Toutefois, si la dépendance des États envers les outils numériques semble établie, il n'en va pas de même de celle **des autres acteurs susceptibles d'utiliser des moyens malveillants contre des systèmes numériques** et, à ce titre, justiciables de l'emploi des moyens de dissuasion numérique. Les groupes de hackers qui louent/vendent leur savoir-faire et/ou leurs réseaux de machines infectées pour conduire des attaques de type déni de service, pour programmer des malwares ou des spywares ou encore pour découvrir des failles de sécurité dans des systèmes d'exploitation, n'ont le plus souvent besoin que de quelques ordinateurs (puissants) et d'une connexion à internet. Il se pose donc la question de savoir s'il est seulement possible de les dissuader par la menace de rétorsion uniquement numérique.

La nécessité d'obtenir une forme de proportionnalité entre l'acte et la réponse et d'établir l'efficacité de cette dernière soulève finalement la question de la capacité à garantir l'effet des représailles et à répéter celui-ci autant de fois que nécessaire. Comme le soulignent certains auteurs, à la différence de mesures de rétorsion (physiques) qui neutralisent (plus ou moins) définitivement l'adversaire, ***la cyber-dissuasion peut perturber celui-ci ou temporairement lui ôter la capacité de nuire mais aucun moyen numérique ne peut obtenir la neutralisation définitive de la menace***[115].

Dans ces circonstances, **la dissuasion numérique ne peut pas écarter totalement l'emploi ponctuel de représailles « asymétriques »**[116]**.** Le recours à des réponses policières/judiciaires – y compris des actions visant les ressources financières des auteurs – doit par exemple être considéré contre des groupes criminels pour lesquels la recherche

[115] Martin C. Libicki, « Cyberdeterrence and Cyberwar », RAND Project Air Force, 2009, p. 31.

[116] Le *Wall Street Journal* confirmait le 31 mai 2011 que le Pentagone avait décidé de considérer les cyber-attaques comme des actes de guerre, ouvrant la voie à l'application de la force physique comme représailles à une attaque numérique. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=WSJ_hp_ LEFTTopStories

du profit est un intérêt à caractère existentiel[117]. De la même façon, l'utilisation de représailles militaires contre des acteurs malveillants pourrait s'envisager dans le cas où ces derniers ont un niveau faible de dépendance envers les technologies de l'information.

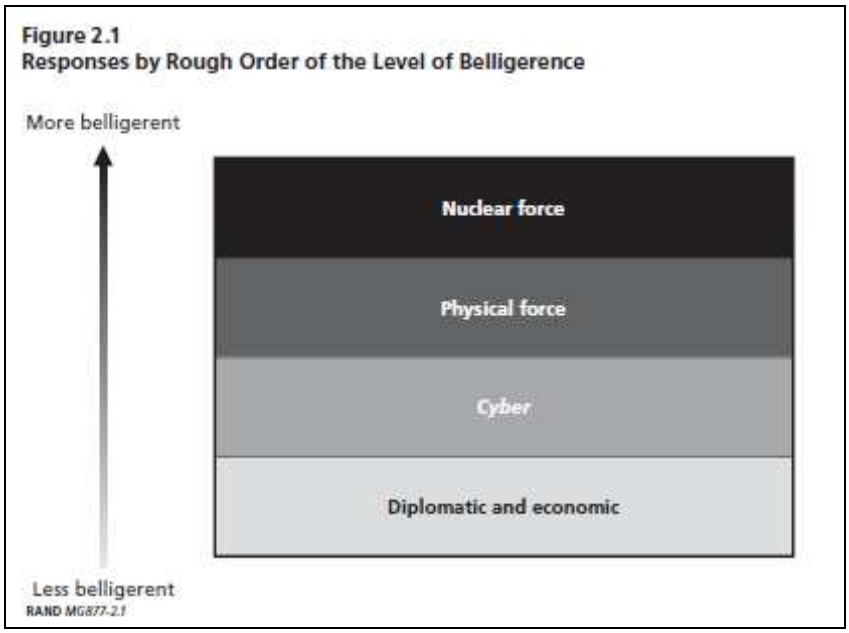


Figure 11 : Échelle des réponses possibles à un acte malveillant ou à une agression (source : RAND)

C.– Il faut déterminer avec précision le degré de transparence qui doit être appliqué à l'engagement de mesures de rétorsion contre un acteur qui serait tenu pour responsable d'un acte ou d'une série d'actes malveillants

Il s'agit *in fine* de définir la posture publique qu'il convient d'adopter en matière de dissuasion numérique. Dans cette perspective, plusieurs facteurs doivent être pris en compte :

⇒ ***La fonction de communication fait intégralement partie de la manœuvre de dissuasion*** : elle a pour rôle *a minima* de convaincre les agresseurs potentiels qu'ils prennent des risques démesurés s'ils sont pris en train d'attaquer les intérêts couverts par la dissuasion[118]. L'idée de conduire l'ensemble de la manœuvre de dissuasion numérique de façon secrète ou confidentielle paraît absurde au regard du rôle préventif que doit jouer le système. Dans cette perspective, il convient de souligner que les actions de rétorsion doivent être visibles/ perceptibles au moins pour l'État, l'organisation ou la personne visée. Si possible les effets d'une action de rétorsion doivent avoir une visibilité publique suffisante (et des effets assez impressionnants) pour dissuader d'autres agresseurs de conduire leurs opérations.

[117] Le FBI estime que le chiffre d'affaires global des organisations criminelles s'élève à un trillion de dollars soit schématiquement 10 % du volume financier représenté par les échanges économiques mondiaux.

[118] Matthew D. Crosston, « How « Mutually Assured Debilitation » Is the Best Hope for Cyber Deterrence », *Strategic Studies Quaterly*, Spring 2011, p. 111.

⇒ Dans la mesure où l'attaque est attribuée à un ou plusieurs acteurs, il peut s'avérer nécessaire de fournir à la communauté internationale des éléments pour justifier l'emploi de moyens de rétorsion. Sur ce point, il n'est pas forcément indispensable d'amener publiquement la preuve « juridique » de la responsabilité mais il semble nécessaire de chercher à obtenir un minimum de soutien pour des actions de rétorsion dont les conséquences seraient visibles et pourraient être exploitées diplomatiquement et publiquement pour envoyer un message (sur l'efficacité des moyens utilisés par exemple) aux futurs agresseurs.

⇒ Il est nécessaire de conserver un niveau de confidentialité suffisant sur les moyens pour limiter les possibilités de voir se développer des parades. Il est également indispensable, pour les mêmes raisons, de protéger les informations portant sur les cibles potentielles. Cela est d'autant plus nécessaire que les cibles possibles peuvent évoluer assez rapidement en fonction des découvertes techniques ou logicielles sur les failles informatiques ou les vulnérabilités des systèmes.

De la même façon, les cibles qui ont déjà été attaquées seront souvent beaucoup plus difficiles à atteindre une deuxième fois dans la mesure où les vulnérabilités ou les failles exploitées pour y parvenir devraient être prises en compte et couvertes par les administrateurs systèmes concernés. Comme corollaire, la préparation opérationnelle et technique des attaques doit faire l'objet de mesures de confidentialité très marquées pour éviter d'alerter les défenseurs ou de fournir des informations critiques sur les vulnérabilités exploitées (en particulier s'il s'agit de « *0 day exploit* », mais même pour l'utilisation de virus très performants[119]).

La problématique du degré de transparence qui doit être appliqué aux opérations de rétorsion se complique au-delà du seul aspect politique si l'on considère la spécificité de la dimension numérique.

Il existe en effet des cas de figure dans lesquels les incertitudes sur l'agresseur ou encore le risque de publicité sur des vulnérabilités critiques sont tellement importants que les actions de rétorsion ne feront pas l'objet de communication publique.[120] L'opération de rétorsion doit toutefois apparaître suffisamment transparente aux yeux de l'agresseur pour que celui-ci comprenne qu'il a été détecté et ainsi que s'applique un effet dissuasif. De la même façon, il ne peut être question d'agir systématiquement de façon secrète au risque de réduire à néant la finalité des représailles.

Le fonctionnement de cet édifice de communication, qui doit finalement être très flexible afin de prendre en compte le contexte de l'attaque et la difficulté spécifique de l'attribution (cf. infra), repose d'une certaine manière sur une certaine forme de dialectique entre les acteurs impliqués. La stratégie de communication doit également prendre en compte le risque de « dégâts collatéraux » si la cible des actions de représailles n'est pas le responsable de l'attaque initiale. En la matière, il est difficile de proposer une formule qui s'applique à tous les cas de figure, toutefois quelques lignes directrices peuvent être imaginées :

[119] Martin C. Libicki, « Cyberdeterrence and Cyberwar », RAND Project Air Force, 2009, pp. 57-58.

[120] Ibid, pp. 94-96.

- Si les effets d'une attaque sont ressentis par la population ou si les médias apprennent l'existence d'une agression, il apparaît nécessaire de communiquer sur les mesures prises pour y répondre. Il peut s'agir dans un premier temps d'indiquer que les services compétents cherchent à trouver le ou les responsables et d'informer le public sur les mesures correctives prises pour le protéger et éviter une reproduction de l'attaque. Selon les résultats obtenus dans la phase d'attribution, la communication publique doit couvrir les initiatives prises pour punir les responsables et leurs résultats, ne serait-ce que pour faire passer un message dissuasif vers d'autres acteurs qui seraient susceptibles de mener des actions similaires. La communication publique peut également permettre de réduire le prestige numérique de l'adversaire et par là même sa propre capacité à communiquer positivement sur ses actions. Dans le cas d'États, l'exposition de leurs actions malveillantes présente un intérêt pour éventuellement les conduire à négocier les conditions d'une sortie de crise ou d'une cessation des attaques.

- Si les informations recueillies permettent d'identifier l'agresseur avec un niveau de confiance élevé[121], les représailles doivent faire l'objet d'actions de communication à la fois vers le ou les responsables identifiés (ou leur commanditaires). La difficulté peut venir alors du choix des canaux employés pour faire passer les messages en particulier si les acteurs directement concernés ne sont pas des États. On peut imaginer des cas de figure dans lesquels il est nécessaire de communiquer à la fois vers les agresseurs identifiés mais également vers les pays depuis lesquels ils agissent[122].

- Il peut exister des scénarios dans lesquels les représailles ne sont pas souhaitables – par exemple parce qu'elles viennent trop tard après l'attaque ou qu'elles sont irréalisables ou trop complexes à mettre en œuvre – mais pour lesquels l'État concerné peut avoir intérêt à communiquer vers l'agresseur dans une logique dissuasive. Cela peut consister simplement à faire savoir à ce dernier qu'il a été identifié et ainsi le prévenir des conséquences qui pourraient découler d'une nouvelle attaque.

Enfin, il faut prendre en compte dans la construction d'une stratégie de communication – qui s'appliquerait de façon générale à la cyber-défense et plus spécifiquement à la cyber-dissuasion – le fait que plusieurs éléments rendent le dialogue avec les agresseurs relativement compliqué par rapport à ce que l'on connait dans les autres milieux. Le simple fait que certains agresseurs peuvent ne pas être des États implique de disposer d'une gamme d'outils relativement large pour faire passer des messages. Il faut également prendre en compte la possibilité que les auteurs agissent pour le compte de commanditaires. Dans ce cas, la stratégie de communication pour contribuer à dissuader tous les acteurs impliqués doit s'étendre des voix diplomatiques à des solutions plus artisanales ou créatives.

[121] Il est difficile de définir précisément ce que ce niveau doit être. On peut toutefois imaginer qu'il dépendra d'un choix effectué par les responsables politiques prenant en compte : le contexte, la discussion avec les services et éventuellement celle avec les alliés.

[122] Ces derniers pouvant être des commanditaires ou alors des États ne disposant pas des outils juridiques et policiers capables de dissuader des auteurs criminels de commettre des attaques numériques. Cf. infra.

L'attribution de l'acte reste au cœur de l'application du concept de dissuasion dans l'espace numérique

Si ***l'attribution*** d'un acte (ou d'une série d'actes) malveillant à un acteur spécifique paraît *ex nihilo* compliquée du fait de la nature même de l'espace numérique, plusieurs éléments doivent cependant permettre l'exercice de la cyber-dissuasion[123] :

⇒ ***Le contexte géostratégique mais également celui qui prévaut en termes techniques peut faciliter l'attribution d'une série d'actes malveillants :*** pour prendre un exemple, dans le cas estonien, il apparaît que la Russie porte une part importante de responsabilité même si les services officiels russes n'ont pas forcément menés directement les opérations visant à neutraliser les serveurs estoniens. Pour autant, cela ne peut pas être le seul facteur déterminant pour attribuer une attaque, ce d'autant que dans certaines circonstances plusieurs acteurs peuvent avoir intérêt à la commettre et il peut arriver que des acteurs conduisent des attaques numériques en cherchant à en rendre responsable un tiers[124]. Il faut toutefois considérer que les États pourraient vouloir prendre la responsabilité d'attaques numériques menées contre leurs adversaires, par exemple dans une logique de dissuasion.

⇒ La responsabilité de l'État abritant les infrastructures et les moyens techniques utilisés pour conduire l'action malveillante pourrait être engagée dans certaines circonstances[125]. Ainsi, dans les pays ne disposant d'aucun cadre juridique – ou de législations peu contraignantes – visant les acteurs numériques malveillants ou criminalisant, certains comportements pourraient être considérés comme (co)-responsables d'une action émanant de machines situées sur leur territoire. La responsabilisation des États, tout comme d'ailleurs celle des fournisseurs de service abritant des pirates ou facilitant leurs opérations[126], est imaginable.

De la même façon, les États refusant de coopérer dans le cadre d'enquêtes criminelles concernant des actes commis depuis leur territoire pourraient être tenus comme partiellement responsables d'une attaque menée depuis leur territoire. Le recours à des individus ou des organismes comme proxy n'altère pas le fait que, sans la participation, le soutien ou même seulement l'accord tacite ou encore l'absence de mesures correctives/dissuasives mises en place par les États, certains actes malveillants ne pourraient avoir lieu.

Comme le souligne d'ailleurs quelques auteurs, ***les groupes de pirates capables de produire les effets les plus importants*** en termes de durée comme de conséquences – donc ceux considérés comme vitaux qui seraient pris en compte par le système de dissuasion numérique – ***disposent vraisemblablement d'une assistance technique assez importante de la part d'États*** : même s'ils ne sont

[123] Eric Sterner, « Retaliatory Deterrence in Cyberspace », *Strategic Studies Quarterly*, Spring 2011, pp. 73-75.

[124] Martin C. Libicki, « Cyberdeterrence and Cyberwar », RAND Project Air Force, 2009, p. 44.

[125] Les États restent responsables physiquement des infrastructures qu'ils abritent comme juridiquement des organisations qui agissent sur leurs territoires. Voir Joseph S. Nye Jr, « CyberPower », Harvard Kennedy School, May 2010, p. 11.

[126] Voir sur cette question, Noah Schchtman, « Pirates of the ISPs: Tactics for Turning Online Crooks Into International Pariahs », Brookings China Center, Cyber Security #1, July 2011.

pas institutionnalisés, leurs actes peuvent donc légitimement être considérés comme émanant des pays qui les soutiennent[127]. On pourrait dès lors avancer en première analyse dans le cadre de ce raisonnement que seuls les États sont les acteurs susceptibles de soutenir et de conduire des cyber-attaques qui s'avèreraient justiciables de l'emploi de représailles. A ce titre ils se qualifient également pour des mesures de rétorsion symétriques visant leurs infrastructures ou leurs systèmes informatiques critiques.

Cependant, ces arguments restent difficiles à manier du fait de ***l'absence d'une convention contraignante en matière de cybercriminalité s'appliquant de façon universelle***[128]. Par ailleurs, les différences entre les approches juridiques nationales – par exemple, l'existence de lois protégeant les données numériques des citoyens – peuvent conduire certains États à refuser de coopérer au nom de la protection de leurs citoyens. Enfin, on ne peut pas écarter totalement la possibilité de fausses alarmes : qu'il s'agisse de disfonctionnements (logiciels notamment) produisant des effets comparables à une attaque ou pannes mécaniques ou logiques. On ne peut pas plus ignorer le fait que certains hackers particulièrement doués, géniaux ou chanceux pourraient être en mesure de produire des effets allant au-delà de leurs espérances ou de leur niveau de savoir-faire.

⇒ ***L'évolution et le développement des outils techniques pourraient faciliter le travail d'enquête et d'investigation*** suivant une attaque. Les capacités des États à tracer – éventuellement en temps réel – les points d'origine, à cerner (et éventuellement à recopier) les modes opératoires, à décortiquer les codes et logiciels utilisés pour une action ou une série d'actes devraient continuer à augmenter tout comme la disponibilité de ressources humaines et techniques plus importantes (notamment en termes de **puissance de calcul disponible** ou de savoir-faire technologique).

Même si l'on peut craindre que les groupes de pirates voient également leur potentiel de nuisance augmenter au fur et à mesure du développement des technologies, l'avantage technique et humain appartient potentiellement aux puissances publiques que sont les États[129]. A condition que ces derniers parviennent à exploiter cet avantage, il pourrait devenir de plus en plus difficile pour une partie des acteurs malveillants de conduire des attaques (d'ampleur) sans risque d'attribution.

[127] Dans une logique comparable de celle qui prévaut pour les organisations terroristes en gardant à l'esprit que certains actes techniques (la création de logiciels, la découverte de « *0 day exploit* » c'est-à-dire de vulnérabilités qui n'ont jamais été exploitées) demandent des moyens techniques et de recherche plus importants que ceux minimaux dont disposent certains réseaux de hackers (en anglais « *ring* » c'est-à-dire des organisations informelles).

[128] La convention sur la cybercriminalité de novembre 2001 n'a été ratifiée que par 14 États, dont la France. Elle prévoit toutefois la mise en place de coopérations internationales spécifiques pour répondre à des crimes numériques. http://fr.wikipedia.org/wiki/Cybercrime

[129] L'idée qu'une agression détectée puisse conduire à une riposte immédiate et automatique contre les machines qui en sont à l'origine pourrait être envisagée. Joseph S. Nye Jr, « Cyber Power », Harvard Kennedy School, May 2010, p. 16.

L'attribution partielle d'une attaque numérique est un moyen envisageable pour exercer une forme de dissuasion sur certains acteurs

Même lorsqu'il est possible de rassembler beaucoup d'indices sur l'implication de certains acteurs, il reste généralement très difficile d'apporter suffisamment de preuves pour établir formellement qu'ils sont les auteurs d'une attaque. Cette incertitude rend finalement délicat le recours à des représailles « de destruction » dans le cadre d'une logique dissuasive.

La mise en place d'un système de réaction multinational peut suppléer cette difficulté. Il s'agirait alors :

- D'accroître les capacités d'analyses et d'enquête en exploitant les synergies entre les moyens techniques des États et les coopérations judiciaires et policières ;
- D'obtenir une condamnation commune d'un acte et de son auteur présumé – qu'il s'agisse d'un État ou de groupes non étatiques – en établissant une conviction partagée reposant sur des données analysées en commun à défaut de preuves.

Cette solution peut offrir un certain niveau de dissuasion contre des attaques numériques aux États et aux organisations impliquées dans un système multinational à caractère coopératif. Son aspect dissuasif pourrait être renforcé si ce système était investi par les participants de l'autorité nécessaire pour prendre des mesures coercitives ou punitives dépassant la seule condamnation de l'acte.

Cette dimension particulière de la dissuasion numérique a été identifiée dans son étude sur le « Cyber Power »[130] par Joseph S. Nye Jr : « *Finally, to the extent that false flags are imperfect, and rumors of the source of an attack are widely deemed credible (though not probative in a court of law) reputational damage to an attacker's soft power may contribute to deterrence*.».

Il est vrai que dans l'espace numérique, ***la réputation d'un acteur possède une valeur spécifique bien plus importante que dans les autres milieux***. De fait, de nombreux acteurs du réseau mondial sont lus et suivis par les internautes du fait de leur réputation : intégrité, compétence, accès à des informations fiables, indépendance, etc. Les opinions qu'ils formulent, les analyses qu'ils dispensent ou les informations qu'ils fournissent sont d'autant plus ou moins crédibles qu'ils disposent d'une bonne ou d'une mauvaise réputation.

La réputation sur internet des personnes physiques, des États, comme des personnes morales constitue une véritable identité numérique, différente de celle qui résulte des interactions classiques. la réputation numérique des organisations est de nature plus dynamique et volatile qu'elle ne l'est dans l'espace réel.

Les entreprises, par exemple, se trouvent confrontées à des acteurs – souvent mal identifiés – qui peuvent produire du contenu, diffusé de façon universelle, concernant leur marque, leurs produits, leurs collaborateurs, au moyen d'outils simples[131].

[130] Joseph S. Nye, Jr, « Cyber Power », Harvard Kennedy School, Belfer Center for Science and International Affairs, may 2010, p. 17.

[131] Digimind, « White paper: Réputation internet », juin 2008, p. 5.

De fait, la mise en cause de la réputation numérique est une problématique sérieuse pour les acteurs concernés. Dès lors, sa remise en cause potentielle peut devenir un outil dissuasif important de participer à une action malveillante, d'autant que cette dernière sera contraire à l'image que l'acteur concerné souhaite donner de lui-même.

Ébauche d'une doctrine en matière de dissuasion numérique : difficultés technico-opérationnelles et comparaisons internationales

Le besoin de développer une posture dissuasive paraît établi : du fait de l'évolution des technologies informatiques et de communications, de la généralisation de l'usage d'Internet pour un nombre grandissant d'applications quotidiennes, il paraît nécessaire de compléter la posture défensive en matière numérique, qui se trouve confrontée à l'asymétrie grandissante entre l'attaque et la défense, pour considérer l'ensemble des options disponibles. La question du seuil de déclenchement de la riposte numérique se pose légitimement si l'on considère que les mesures de rétorsion peuvent avoir des conséquences graves (même si elles ne sont pas forcément existentielles) sur la cible concernée.

L'analyse des différents éléments et capacités qui se rattachent au concept général de dissuasion a mis en lumière certaines spécificités particulières du cyberespace :

- ***Le caractère asymétrique des capacités défensive/offensive***, les moyens de protection sont plus coûteux et long à développer et à mettre en œuvre que les systèmes permettant de conduire des attaques logiques ou physiques contre des systèmes d'information.

- ***La difficulté à attribuer rapidement une action offensive malveillante*** à un pays ou à un groupe d'acteurs particulier. Nous avons toutefois mis en lumière le fait que les États-Unis disposent de moyens techniques qui pourraient être suffisants pour y parvenir. Il en découle ***un besoin d'établir une coopération technique et opérationnelle*** avec nos alliés et nos partenaires pour renforcer nos capacités de défense et de protection.

- ***Les problèmes inhérents à la démonstration de la crédibilité des capacités défensives et offensives*** dont on dispose : le risque existe de provoquer des effets collatéraux sur des systèmes amis et/ou de rendre accessible aux adversaires potentiels des informations clefs sur les moyens utilisés.

En 1998, un texte de quelques pages de Joseph S. Nye Jr indiquait que la maîtrise totale de l'information (« *information dominance* ») était susceptible de devenir le nouvel axe de la politique internationale des États-Unis en lieu et place de la capacité nucléaire militaire[132]. Il s'appuyait sur un parallèle très simple : une maîtrise totale de l'information devrait permettre de connaître les actions préparées par un adversaire et de le dissuader de les entreprendre en lui faisant savoir que les défenses et les représailles étaient prêtes ; de leur côté, les alliés, quels qu'ils soient, auraient besoin de recueillir auprès des États-Unis les confirmations ou compléments d'informations nécessaires à la réalisation de leurs objectifs de sécurité.

[132] Document de travail fourni dans le cadre de la formation de « responsable senior en sécurité nationale et internationale » ; texte non publié.

Le concept d'« *information dominance* » a été remplacé par ceux de cyber-sécurité, de cyber-défense ou encore de cyber-dissuasion. Pour autant, aucun texte officiel américain spécifique ne décrit l'application par les États-Unis d'une doctrine de cyber-dissuasion mais le concept est exposé ou évoqué dans plusieurs documents récents.

Le texte américain le plus explicite en la matière a été publié par la Maison blanche en 2010. Il s'agit de la « Stratégie internationale pour le cyberespace »[133]. Ce document s'appuie sur une vision future du cyberespace qui serait ouvert et interopérable, sûr et fiable mais surtout stabilisé par des normes de comportement fondées sur des principes reconnus par tous : libertés fondamentales, respect de la propriété, valeur de la vie privée, protection contre le crime et droit à l'autodéfense. Il s'agit là d'un enjeu collectif qui suppose un comportement « acceptable » et « responsable » des différents pays conformément à ces normes. Pour parvenir à l'établissement de telles normes, les États-Unis envisagent de combiner des outils diplomatiques et des moyens de défense afin de développer un contexte « prospère et sécurisé » bénéficiant à l'ensemble des utilisateurs des technologies de l'information.

C'est au sein de la composante « défense » que sont avancées les deux idées de « *dissuasion* » et « *deterrence* » :

- « *Dissuasion* » par une capacité de résister à des attaques, tant au plan national qu'à l'étranger, sur la base de coopérations étroites en matière d'alerte, de réponse et de récupération.

- « *Deterrence* » vue comme une capacité de réponse, en application du principe d'autodéfense reconnue par la Charte des Nations Unies, à des actions malveillantes dirigées contre les intérêts numériques américains. L'accent est mis là encore sur la nécessité de coopération avec le plus grand nombre possible de partenaires étrangers, même si les États-Unis se réservent le droit de « *répondre à des actes hostiles dans le cyberespace de la même manière qu'ils le feraient vis-à-vis de tout autre type de menace contre le pays* ».

Parmi les priorités politiques américaines, le développement d'un volet militaire offensif est proposé pour préparer les États-Unis aux défis de la sécurité du XXI^{ème} siècle. Outre le besoin de disposer de réseaux militaires sûrs et fiables, et de coopérer avec les alliés et autres partenaires internationaux et nationaux pour accroître la sécurité collective, le document propose de *« renforcer les alliances militaires pour faire face aux menaces potentielles dans le cyberespace* ». C'est dans ce cadre que les États-Unis continueront à « *travailler avec les contreparties militaires et civiles de leurs alliés … à développer les moyens et les méthodes d'une autodéfense collective dans le cyberespace. De tels partenariats et alliances militaires renforceront nos capacités de dissuasion collective et de défendre les États-Unis contre des acteurs étatiques ou non étatiques* ».

Les menaces numériques d'origine étatique sont donc bien prises en compte et les États-Unis se préparent à y répondre. L'approche ne semble toutefois pas procéder d'une vision unilatérale, comme elle aurait pu l'être sous les administrations précédentes, alors même que les capacités américaines actuelles sont uniques, notamment en matière

[133] White House, « International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World », May 2011.

d'attribution d'actes malveillants et de moyens offensifs. Au contraire, le discours des États-Unis sur la cyber-dissuasion insiste sur sa nature collective et sur le besoin de coopération étroite avec leurs alliés.

Cette démarche est confirmée dans le rapport publié par le Pentagone sur sa stratégie pour opérer dans le cyberespace. L'initiative stratégique n° 4 (construire des relations robustes avec les alliés des États-Unis) prévoit en effet que « *le Département de la Défense étendra ses coopérations formelles et informelles dans le cyberespace à un ensemble élargi d'alliés et de partenaires militaires pour développer une autodéfense collective et accroître une dissuasion collective* »[134].

Éléments d'organisation d'une capacité nationale initiale de cyber-dissuasion à finalité défensive

Des responsables américains ont récemment indiqué à leurs homologues français[135] qu'il serait souhaitable que la France améliore son niveau de sécurité des systèmes d'information[136].

Outre le fait que cette déclaration met en lumière les vulnérabilités – connues par les services américains – des dispositifs de chiffrement utilisés par la France, elle montre que les États-Unis attendent de leurs alliés un certain niveau de compétences et de capacités autonomes en matière de cyber-défense.

Ainsi, le schéma américain de dissuasion collective décrit dans la « Stratégie internationale pour le cyberespace » classe les États dans trois catégories distinctes :

- Ceux ayant un comportement « inacceptable » ou « irresponsable » (adversaires potentiels) avec qui il n'est pas possible de coopérer ;
- Les États ayant un comportement « acceptable » et « responsable » mais ne possédant ni compétences ni moyens efficaces en matière de défense numérique, avec lesquels il est possible d'entretenir de bonnes relations mais qui seront une charge en termes de sécurité pour les États-Unis ;
- Les États ayant un comportement « acceptable » et « responsable », capables d'assurer par eux-mêmes la sécurité de leurs systèmes d'information et avec qui il est possible de pleinement coopérer.

Paris devra vraisemblablement poursuivre ses investissements en matière de sécurité numérique pour parvenir à disposer d'un système autonome permettant de conduire seul des opérations de représailles dans l'espace numérique.

Par contre le schéma américain, tel qu'interprété précédemment, offrirait une réponse au dilemme souveraineté/dépendance en permettant à la France d'engager et de conduire les réformes et programmes nécessaires à l'élaboration progressive d'une cyber-

[134] « Department of Defense Strategy for Operating in Cyberspace », July 2011, p. 10.

[135] Discussion personnelle avec des responsables de la DGA en matière de Lutte informatique (note d'Alain Esterle).

[136] On peut rappeler qu'il a fallu trois ans de discussions et d'aménagements pour faire valider à l'OTAN le chiffreur gouvernemental français *Echinops*.

dissuasion. En s'affirmant comme une nation majeure en termes de sécurité des systèmes d'information et de cyber-défense, la France peut être un partenaire respecté dans le cadre d'une ***cyber-dissuasion collective***, à condition de concéder aux États-Unis la direction de cet outil commun.

La doctrine française pourrait alors s'appuyer sur trois piliers :

- Être exemplaire en matière de SSI, avec une définition claire et une application rigoureuse de politiques en SSI, tant pour les actions de sensibilisation que pour la mise en œuvre et la maintenance des outils de sécurité classiques (anti-virus, chiffreurs, pare-feux…) ;
- Établir et maintenir les bases d'une cyber-défense efficace et l'appliquer à un champ englobant :
  - ✓ les réseaux très sensibles ;
  - ✓ l'agrément des produits de sécurité (à renouveler régulièrement) ;
  - ✓ l'analyse d'attaques numériques ;
  - ✓ les procédures et moyens permettant de garantir la continuité d'activité en modes dégradés et le retour à la normale ;
- Développer des coopérations avec les partenaires étrangers en matière d'échange de données, d'alerte, d'analyse des attaques, d'exercices et d'actions opérationnelles destinées à répondre à des attaques à plus ou moins grande échelle.

De fait, ces éléments s'avèrent être cohérents avec les objectifs stratégiques en sécurité des systèmes d'information tels que récemment fixés par le SGDSN[137]. Ils ne constituent pas en soi une doctrine de cyber-dissuasion mais, en y adjoignant une capacité offensive autonome, ils peuvent permettre de participer à une cyber-dissuasion collective en tant que partenaire de premier plan, c'est-à-dire participant à la décision et à la mise en œuvre d'actions éventuelles de représailles suite à une attaque.

Deux obstacles majeurs se présentent néanmoins dans la mise en œuvre du schéma proposé du point de vue des capacités industrielles et des partenariats avec les opérateurs privés :

- ***Les chaînes d'approvisionnement fiables en France sont limitées à quelques produits de sécurité développés pour des industriels de confiance*** – souvent du domaine de la défense – et agréés par l'ANSSI pour couvrir les besoins des activités dites « de souveraineté » (défense/armement, diplomatie). Or, le champ de la cyber-défense doit englober l'ensemble des « systèmes d'information jugés essentiels », au-delà de ces seules activités, en particulier les infrastructures et réseaux critiques (production/distribution d'eau ou d'électricité, communications, transports...). Il faut donc prévoir d'étendre les procédures d'agrément aux produits destinés à de plus

[137] « Défense et sécurité des systèmes d'information – Stratégie de la France », ANSSI, février 2011.

nombreux secteurs d'activités, ce qui représente une contrainte forte en matière de gestion des appels d'offres[138].

➥ ***En réalité, une telle évolution doit conduire progressivement à l'intégration des opérateurs d'infrastructures vitales dans le champ des activités de souveraineté en matière de sécurité numérique***. Une telle opération suppose non seulement la fiabilisation des produits utilisés par ces acteurs mais également l'extension à ces derniers des procédures en matière d'habilitation et d'organisation. Il s'agit également de les associer aux exercices conduits en matière de cyber-sécurité. Une refonte complète du schéma actuel de partenariat public-privé et de la Directive Nationale de Sécurité (DNS) paraît nécessaire pour y parvenir.

Éléments d'architecture pour une future capacité nationale de cyber-dissuasion (volet offensif)

A la lumière des éléments exposés précédemment, quelques principes semblent devoir guider l'élaboration d'une éventuelle future capacité offensive dans le domaine numérique :

➥ ***Les représailles numériques devront être généralement symétriques et proportionnelles, mais il ne faut pas exclure l'emploi dans certaines circonstances de moyens asymétriques :*** la dissuasion numérique s'applique uniquement dans la mesure où les agresseurs présentent des dépendances importantes envers des systèmes ou des réseaux informatiques. Les États ou les entreprises légales, dont on considère qu'ils auront développé un niveau de dépendance globalement comparables, sont donc les plus à même d'être sensibles à une manœuvre dissuasive dans le domaine numérique. *A contrario*, les organisations criminelles ou terroristes et les personnes physiques sont assez peu susceptibles d'être dissuadés par la menace de rétorsion symétrique. Sur ce point, les actions à caractère légal (poursuites criminelles) ou encore les sanctions économiques ou financières pourraient s'avérer plus dissuasives. En dernière extrémité, le recours à des représailles physiques peut être envisagé si (1) les conséquences de l'attaque sont suffisamment graves et les effets durables et (2) l'acte peut être attribué au-delà du doute raisonnable. Nous avons enfin montré que les États peuvent être tenus en partie responsables des activités criminelles qui se développent sur leur territoire en exploitant les failles légales nationales dans la mesure où celles-ci ont été officiellement dénoncées comme facilitant les activités hostiles.

➥ ***Il sera indispensable de suivre un processus d'attribution avant toute utilisation des outils de représailles*** : l'attribution d'un acte numérique malveillant (ou d'une série d'actions) s'avère complexe : c'est un processus à la fois long et dont l'issue est incertaine. De fait, il parait possible de prendre des mesures de rétorsion sur la base des informations de contexte, des données techniques recueillies lors des attaques et en se fondant sur la politique des États ou des entreprises en matière de guerre numérique. Dans certains cas, les responsables (et leurs sponsors) peuvent même ouvertement revendiquer leurs actions pour des raisons politiques d'affichage. Les risques d'erreur étant importants, le maniement de la rétorsion mérite un

[138] A noter que même dans le cadre de l'approvisionnement des forces, le choix de produits agréés n'est pas évident pour les forces françaises depuis la réintégration complète dans l'OTAN.

examen politique de fond. En tout état de cause, il est difficile d'imaginer de renoncer à l'effort d'attribution qui s'avère consubstantiel de la manœuvre de dissuasion et qui doit prendre une forme publique (ou diplomatique) suffisante pour renforcer la posture de l'État qui l'exerce.

➥ ***La manœuvre de dissuasion numérique nécessitera une communication maîtrisée et pourrait s'appuyer sur une coopération internationale renforcée*** : comme pour l'attribution, la manœuvre de dissuasion ne peut s'opérer sans un minimum de communication vers l'extérieur comme vers l'intérieur : cette dernière doit concerner les agresseurs potentiels, les alliés et partenaires internationaux mais également les parties prenantes au niveau national. Cette communication doit être maîtrisée, c'est-à-dire que la confidentialité de certaines informations, systèmes et données doit être assurée pour éviter de réduire l'efficacité des mesures de rétorsion. En matière de coopération, il semble nécessaire de reconnaître qu'il est urgent de mettre en œuvre un cadre juridique international qui fixerait quelques règles de comportement, notamment en matière de crime numérique afin de permettre, par exemple, de développer l'entraide judiciaire sur les actes les plus graves[139].

Une éventuelle dissuasion numérique devra ***s'appuyer sur trois fonctions opérationnelles et organisationnelles*** : commandement, développement des moyens et outils, mise en œuvre.

Chaque fonction peut à son tour se décomposer en sous-fonctions qui participent pleinement à l'exercice de la dissuasion ou à la conduite des opérations offensives engagées pour répondre à une attaque d'ampleur suffisante. La dissuasion numérique doit de plus s'intégrer dans un système complet de cyber-défense qui englobe les activités de protection, de surveillance et d'alerte et d'action offensive. La figure suivante offre des éléments de structuration de ces fonctions et sous-fonctions.

[139] Joseph S. Nye Jr, « Cyber Power », Harvard Kennedy School, May 2010, pp. 17-18. Il faut également considérer à plus long terme la possibilité de voir émerger un modèle de régulation des conflits numériques qui ne serait pas sans lien avec les conventions sur le droit de la Guerre et la protection des populations civiles (Genève et La Haye).

Figure 12 : Organisation générale possible d'une architecture de cyber-dissuasion

Pour fonctionner, cette organisation devra vraisemblablement ***s'adosser à l'architecture de sécurité des systèmes d'information et de cyber-défense***. Elle doit en effet pouvoir capitaliser autant que possible sur les mesures de protection et de défense déjà mises en place. En particulier, l'organisation devrait utiliser l'ensemble des moyens de détection et de traçage des actes malveillants. Elle doit également pouvoir mobiliser les ressources techniques et humaines permettant de connaître intimement la composante technique des menaces et l'état de l'art en matière de logiciels malveillants. Mais ces ressources techniques et humaines devront être enrichies pour faciliter la découverte et l'exploitation de vulnérabilités et de failles de sécurité dans les principaux systèmes informatiques. Ce pilier technique serait chargé de l'élaboration de logiciels ou de codes et participerait à la définition de dossiers d'objectifs complets sur les principaux acteurs malveillants connus[140] et susceptibles d'être sensibles à la manœuvre de dissuasion. Enfin, il aura pour tâche de fournir les données d'alerte et de conduire les efforts destinés à permettre l'identification d'éventuels agresseurs.

La mise en œuvre des armes logiques et la gestion de la « bataille numérique » reviendraient à une structure de forces qui pourrait s'appuyer sur un État-major[141].

[140] Dans ce domaine, il sera probablement nécessaire de prendre en compte le fait que la neutralisation ou la disruption des systèmes visés auront des conséquences sur l'environnement de la cible et pas seulement uniquement sur cette dernière. Karl Frederick Rauscher & Andrey Korotkov, « Working Towards Rules for Governing Cyber Conflict », East-West Institute, January 2011, p. 18.

[141] C'est du reste la solution retenue par les États-Unis au travers de la création d'un US CyberCom – sous l'autorité de STRATCOM –, et chargé d'unifier les approches des différents services du DoD en matière de lutte informatique offensive et défensive. Voir Department of Defense, « Strategy for Operating in Cyberspace », July 2011, p. 11.

Également autorité de commandement, ce dernier pourrait être chargé d'une part des travaux préparatoires des opérations (définir les besoins opérationnels, les concepts d'emploi, élaborer les dossiers d'objectifs, planifier et préparer les opérations) et d'autre part de missions à caractère opérationnel (veille et alerte, renseignement, articulation C2 avec l'échelon politique). L'autre composante de la force numérique consisterait en unités opérationnelles chargées de la mise en œuvre des moyens de rétorsion – y compris si nécessaire, l'introduction physique de logiciels dans des systèmes isolés –, de la gestion des engagements (coordination des actions, évaluation des effets) et des phases de formation/entraînement y compris les exercices de retour sur expérience. Cette force opérationnelle pourrait également être responsable de la coordination des mesures de défense et de protection numériques aux niveaux national et international, y compris dans le domaine de la résilience – l'ensemble de ces mesures et des plans associés participant pleinement à la manœuvre dissuasive[142]. Dans ce cadre, elle devrait être en mesure de renforcer le lien avec le secteur privé, en particulier les opérateurs d'infrastructures sensibles ou critiques.

Enfin, troisième pilier de cette triade, une organisation à vocation politico-militaire pourrait être mise en place. Son rôle serait de participer à l'exercice de la diplomatie (publique et entre États) et de la communication dans le cadre de la capacité de cyberdéfense (y compris les aspects liés à la protection et à la veille). Parmi ses principales missions, devrait apparaître la fonction de renseignement, et ce en complément des travaux de la composante technico-industrielle sur les aspects techniques de la menace. Enfin, elle pourrait être chargée des aspects internationaux et juridiques : coopérations, dialogues stratégiques, négociations internationales, évolutions du cadre juridique national (étude des options, rédaction de propositions de textes, etc.).

[142] Harry D. Raduege, « Fighting Weapons of Mass Disruption: Why America Needs a « Cyber Triad » », East-West Institute, Global Cyber Deterrence, April 2010.

Les moyens existants pourraient permettre d'établir les prémisses d'une cyberdissuasion

De nombreux outils, systèmes, procédures et moyens ont été mis en place dans le domaine défensif

Mettre en place des mesures techniques et non techniques permettant d'assurer la sécurité des systèmes d'information est au cœur même de la cyber-sécurité depuis que le concept existe. Mais pour être efficaces, ces mesures doivent concerner **toutes les menaces et vulnérabilités** possibles, alors qu'**une seule faille** correctement exploitée peut suffire à assurer le succès d'une attaque.

L'impossibilité à établir un registre exhaustif et détaillé des menaces et vulnérabilités, en particulier compte tenu du facteur humain, rend le schéma attaque/défense dans le cyberespace fondamentalement asymétrique, même si certains chercheurs envisagent qu'à partir d'un certain niveau d'engagement, et donc de capacité de défense, l'impact marginal des attaques fléchisse ou, ce qui est équivalent, que leur coût pour en conserver l'efficacité augmente considérablement.

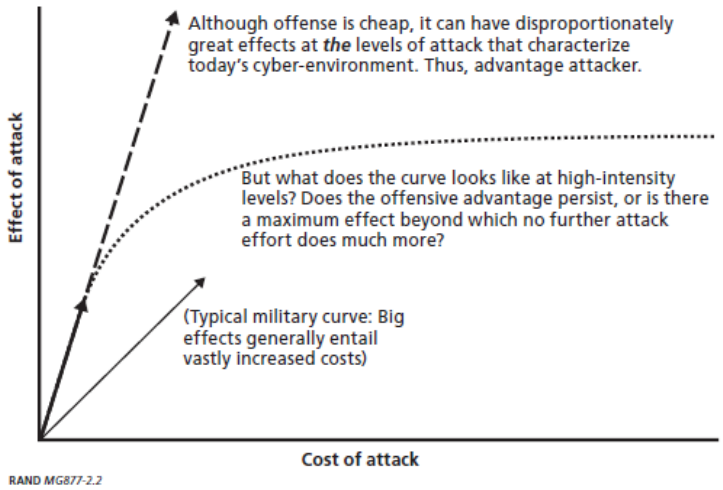


Figure 13 : Il pourrait exister des situations de conflit dans lesquelles l'asymétrie entre attaque numérique et défense s'estompe (source RAND 2009)

D'une manière générale, les capacités défensives s'appuient sur une combinaison de méthodes de gestion des risques, de produits fiables, de compétences et d'organisation. Leur apport au volet protection d'un système de dissuasion numérique mérite d'être mis en lumière afin de déterminer les marges de progrès existantes.

Méthodes et procédures

L'analyse et la gestion des risques sont au cœur de la démarche de sécurité des systèmes d'information. Il n'existe en effet aucune défense efficace qui ne parte d'une analyse complète des risques encourus et d'un choix des priorités à accorder à telle ou telle mesure défensive.

Il existe maintenant des standards ISO en matière de gestion des risques en général (ISO-IEC 31000-2009) et de gestion des risques numériques en particulier (ISO-IEC

27005-2008). Les différentes méthodes et outils proposés s'appuient sur une approche séquentielle[143] :

- Expression des besoins de sécurité ;
- Analyse des vulnérabilités et des menaces ;
- Analyse des contraintes environnementales (juridiques, budgétaires, opérationnelles…) ;
- Analyse et évaluation des risques (taux d'occurrence, impact et conséquences) ;
- Identification et évaluation des choix dans le traitement des risques (y compris identification des risques résiduels) ;
- Établissement d'un plan de traitement des risques avec conditions de mise en œuvre.

Le plan de traitement des risques combine l'acquisition et l'entretien d'équipements particuliers (produits de sécurité) et de compétences (sensibilisation, formation, exercices) ainsi que la mise en place d'un schéma organisationnel et d'un cycle récurent d'évaluation et de correction de l'efficacité de ces traitements (audits, mesures correctives).

Les risques numériques peuvent faire l'objet de plusieurs approches différentes :

- L'élimination des vulnérabilités ou des failles connues via la mise à jour des logiciels concernés et la correction des failles qui peuvent être exploitées.
- La réduction des risques par l'utilisation de logiciels tiers capables de détecter et d'empêcher des intrusions, des accès non autorisés, ou des tentatives de modifications de programmes protégés (pare-feu, antivirus, etc.).
- Le transfert du risque à un tiers, par exemple par le biais d'une police d'assurance.
- L'acceptation des risques considérés comme résiduels[144].

A ce jour, les méthodes de gestion des risques n'incluent pas un mode de traitement fondé sur des actes de représailles visant à dissuader un attaquant potentiel. Cela est compréhensible dans la mesure où la gestion des risques se concentre sur le volet défensif sans vraiment aborder les questions d'identification d'agresseurs éventuels et de capacité de riposte. Néanmoins, si une démarche dissuasive devait être envisagée, il faudrait prévoir d'inclure la dissuasion dans les mesures de traitement des risques, notamment pour les systèmes d'information jugés sensibles tels que, par exemple, les infrastructures critiques.

[143] Voir par exemple la méthode EBIOS mise au point et promue par l'ANSSI http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

[144] Tous les experts s'accordent à considérer que la réduction totale du risque est impossible. Dès lors, les responsables de sécurité des systèmes d'information peuvent être amenés à accepter des risques pour lesquels les solutions de protection sont soit trop coûteuses, soit reconnues comme inefficaces.

Produits de sécurité

En matière de cyber-sécurité, il existe trois types de produits : les produits commerciaux sans garantie particulière, les produits bénéficiant d'une certification (par exemple selon les critères européens communs) et les produits développés sous contrôle (en France les produits agréés par l'ANSSI après une évaluation technique complète).

Les pays avancés en matière de sécurité des systèmes d'information disposent de ces trois types de produits, y compris la troisième catégorie développée par des industriels accrédités. En France, les produits agréés équipent les réseaux de la défense et les réseaux de communication des hautes autorités. Plus onéreux et moins diffusés que les autres, ce sont les seuls qui proviennent d'une chaîne d'approvisionnement contrôlée et fiable.

Afin de bâtir un dialogue dissuasif crédible, les capacités défensives doivent couvrir l'ensemble des réseaux et infrastructures qui ont été inclus dans le champ de cette dissuasion. Or, ce n'est pas le cas pour les infrastructures critiques dont les politiques de sécurité sont validées par le SGDSN mais dont les opérateurs ne sont pas tenus de s'équiper en produits agréés par les laboratoires de l'agence nationale de sécurité des systèmes d'information[145].

Pour être certain que la capacité défensive soit pleinement crédible, il faut aussi s'assurer que les industriels accrédités sont à même de garantir un approvisionnement stable et sûr de l'ensemble des produits et des composants nécessaires à l'équipement des réseaux concernés[146].

Le développement en Europe et en France des compétences dans le domaine de la sécurité numérique est indispensable dans une perspective d'établissement d'une politique de cyber-dissuasion

Le renforcement des capacités défensives suppose également la mise en place d'efforts spécifiques destinés à sensibiliser les responsables de l'administration et de l'usage des réseaux, au niveau national et, si possible, européen. Il s'avère effectivement indispensable d'entraîner et de former le personnel qui serait amené à intervenir en cas d'incident numérique comme les personnes dont la mission est d'assurer la protection des infrastructures et des systèmes critiques pour le fonctionnement des réseaux numériques.

Pour la gestion des incidents, surtout dans le cas d'attaques de grande ampleur, l'expérience a en effet montré l'importance de la coordination entre les équipes impliquées, notamment l'implication des *Computer Emergency Reponse Teams* (CERTs) et des cellules de gestion de crise.

Depuis 2007 – date de l'attaque contre l'Estonie et année de création du centre d'excellence de l'OTAN à Tallin –, la coopération européenne et transatlantique s'est intensifiée. Elle a conduit notamment à la mise en œuvre d'exercices communs et de travaux

[145] A l'heure actuelle, le Référentiel Général de Sécurité (RGS) produit par ANSSI identifie des produits qualifiés (1, 2 ou 3 étoiles) et ne s'adresse qu'aux administrations.

[146] Avec les difficultés que nous avons évoquées précédemment.

d'ordre juridique entre experts permettant de répondre plus efficacement à des attaques de grande ampleur. Ainsi, la création d'un CERT institutionnel européen, décidée en juin 2011, doit permettre à l'Union de disposer d'une équipe d'experts capables d'intervenir en soutien d'une institution ou agence européenne qui serait confrontée à un incident de sécurité majeur[147].

L'année 2011 sera également marquée par la tenue de trois exercices de réponse à des cyber-attaques à l'échelle européenne :

- Eurocybex impliquant la France, la Hongrie et l'Espagne sous supervision ENISA, (une vingtaine d'États membres ont souhaité être observateurs) ;
- Cyber Europe impliquant l'ensemble des pays européens (pilotage ENISA) ;
- Un exercice de coordination impliquant l'UE et les États-Unis. Il est prévu que tous ces exercices contribuent à la mise au point de protocoles communs d'échange de données et de coordination.

Il faut cependant noter que, bien que les promoteurs soient d'accord sur le principe, ces exercices n'impliquent pas encore le secteur privé, notamment les opérateurs d'infra-structure critiques. Ce point devra être corrigé si l'ambition est de démontrer une capacité à réagir rapidement, efficacement et de façon coordonnée à des cyber-attaques dans le cadre d'une capacité de défense propre à consolider une démarche dissuasive crédible pour protéger ces cibles essentielles en termes de sécurité.

L'évolution des partenariats public-privé constitue une priorité en matière de sécurité numérique

Les problématiques liées à la sécurité numérique – pas seulement la sécurité physique des réseaux, mais aussi les questions de réputation numérique, de protection des informations privées comme publiques, la protection des futures infrastructures dédiées par exemple à la gestion de l'internet des objets – reçoivent une attention grandissante de la part des autorités nationales, transnationales[148] mais également des grands groupes industriels ou de service.

Ainsi, les principaux acteurs de l'économie numérique qui ont investi lourdement pour le développement de leurs offres de *Cloud Computing* ou de solutions d'externalisation et/ou de « virtualisation » – c'est le cas de Google, de Microsoft ou encore d'IBM – de même que les industries qui sont conduites à engager des coopérations internationales pour leur développement – cas, par exemple, d'AREVA –, développent de plus en plus la dimension "sécurité numérique" de leur activité. Microsoft édite bi-annuellement un rapport sur la sécurité numérique de ses outils mais également de programmes tiers qui comprend, notamment, une analyse des risques[149] par pays.

[147] Commission européenne, « Cybersécurité : l'UE se prépare à mettre en place une équipe d'intervention pour les institutions européennes », 10 juin 2011.

[148] Voir, par exemple, le rapport de l'ENISA sur la sécurité dans l'informatique en nuage. ENISA, « Cloud Computing: Benefits, Risks and Recommandations for Information Security », November 2009.

[149] Microsoft, « Microsoft Security Intelligence Report Volume 8 (July through December 2009) », December 2009.

Des travaux ont également été réalisés par certaines agences ou organismes officiels américains ainsi que dans le cadre de *think-tanks* sur la question de la cyber-sécurité. Ainsi, fin 2008, le CSIS publie un rapport issu de la commission réunie par ses soins sur cette question, qui appelle notamment à réinventer le partenariat public-privé et, de façon générale, la relation entre les agences et les sociétés en matière opérationnelle[150].

Enfin, la question de la gouvernance et de la sécurité de l'espace numérique spécifique que constitue Internet fait également l'objet d'intenses réflexions, aux États-Unis comme en Europe, comme en témoigne le récent rapport du *Government Accountability Office* (GAO)[151]. De fait, avec 90 % des infrastructures critiques du secteur de la sécurité nationale (défense, agences...) sous la responsabilité d'opérateurs privés, les États-Unis se trouvent en pointe dans les réflexions sur cette question[152]. ***L'implication du secteur privé – des grandes entreprises aux plus petites sociétés – y est considérée comme l'une des conditions clefs du succès de l'ensemble des démarches dans ce domaine autant que dans celui de la sécurité des systèmes d'information.*** En particulier, les responsables américains considèrent qu'il reste beaucoup à faire en matière de connaissance commune des menaces et de détection d'incident ou d'attaque. Ainsi dans le document de stratégie publié en juillet 2011, le Pentagone souligne la nécessité de renforcer les partenariats public-privé dans cette perspective.

> 2007. Building upon this program, DoD is also establishing a pilot public-private sector partnership intended to demonstrate the feasibility and benefits of voluntarily opting into increased sharing of information about malicious or unauthorized cyber activity and protective cybersecurity measures.

Extrait du « Department of Defense Strategy for Operating in Cyberspace, July 2011

Du point de vue de la mise en place d'une capacité défensive crédible à l'échelle nationale, l'analyse a également montré que la participation des opérateurs d'infrastructures critiques pèche au moins sur quatre plans :

- L'absence d'accès aux informations concernant les menaces d'origine étatique ;
- Le manque de choix coordonné en matière de traitement des risques, notamment pour le choix des risques résiduels et des mesures qui contribueraient à une démarche dissuasive ;
- L'absence d'une démarche d'acquisition de produits agréés ;
- Pas de participation à des exercices organisés par les États en matière de réponse à des attaques sur Internet.

[150] Center for Strategic and International Studies, « Securing Cyberspace for the 44th Presidency », A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, December 2008, p. 2. Le rapport appelle également à la mise en place aux États-Unis de capacités offensives dans le domaine numérique.

[151] GAO, « United States Faces Challenges in Addressing Global Cybersecurity and Governance », July 2010.

[152] The Hague Center for Strategic Studies & TNO, « The future of cybersecurity », Strategy and Change, Paper No 2011•04, p. 19.

Dans les pays avancés dans le domaine de la sécurité numérique, la question de la protection des infrastructures vitales est gérée dans le cadre de Partenariats Public-Privé (PPP). Ces PPP ont des structures variables selon les pays : organisés de façon plutôt pyramidale en France (tradition/culture de pouvoir centralisé), ils prennent une forme de concertation plus équilibrée entre partenaires dans les pays anglo-saxons.

Toutefois, si ces derniers considèrent que l'amélioration des capacités de sécurité du secteur privé – en particulier pour ce qui concerne les opérateurs d'infrastructures critiques – passe par une démarche volontaire des entreprises concernées, ils reconnaissent qu'il peut exister un besoin à les inciter à entreprendre des mesures de sécurité, y compris par l'établissement d'un cadre juridique contraignant.

La notion de partenariat public-privé dans le domaine de la sécurité numérique soulève à cet égard un problème épineux au niveau national comme à l'étranger. En effet, les attentes du secteur privé vis-à-vis des services publics sont à la fois d'obtenir plus d'implication – notamment au niveau technique comme par exemple sur la qualification du software et du *firmware* en matière de sécurité – mais également de ne pas accroître outre-mesure les contraintes, en particulier légales ou réglementaires, pesant sur le développement de leurs produits et la conduite de leurs opérations.

Par ailleurs, les divers acteurs du monde numérique sont confrontés à des contraintes de plus en plus pesantes en matière de recueil et de conservation des données personnelles, de protection de l'identité numérique et de gestion/sécurisation de l'information. Ces contraintes s'appliquent notamment aux échanges qui peuvent avoir lieu entre les sphères publique et privée dans le cadre de partenariats de sécurité. Elles ne feront que s'aggraver au fur et à mesure de la généralisation des solutions numériques pour des applications de la vie quotidienne[153]. Dès lors, la convergence public-privé n'est pas une évidence sur le fond et les solutions à adopter méritent également une analyse objective et détaillée.

Quoi qu'il en soit, une capacité défensive crédible ne pourra pas être bâtie sans revenir en profondeur sur les schémas de partenariat public-privé en place.

Certaines capacités offensives pourraient être utilisées dans le cadre d'un système de dissuasion numérique

Il paraît nécessaire de considérer que les attaques les plus courantes qui conduisent à des perturbations, voire des interruptions momentanées de trafic – qu'il s'agisse de dénis de service, de défigurations de pages web, d'opérations de *phishing*[154] ou de détournements d'adresses –, ne sont pas susceptibles de faire partie d'un dialogue dissuasif au niveau des États. Pour qu'une capacité offensive puisse participer d'une dissuasion étatique, elle doit effectivement pouvoir ***affecter profondément*** et, dans la mesure du possible, ***dans la durée, le fonctionnement des réseaux jugés sensibles voire critiques de l'adversaire.***

[153] Voir, par exemple, Guillaume Desgens-Pasanau et Eric Freyssinet, « L'identité à l'ère numérique », Dalloz/Presaj, 2009.

[154] http://en.wikipedia.org/wiki/Phishing

Deux types de capacités semblent pouvoir répondre à ces critères : les attaques informatiques par *malware* (attaques dites logiques) et les attaques physiques sur des réseaux ou des machines assurant les communications entre les États, les continents ou les régions (e.g. câbles sous-marins).

Attaques logiques

Les logiciels malveillants conçus pour attaquer des serveurs ou des applications comprennent couramment deux éléments : un vecteur servant à pénétrer un réseau, à s'y implanter, se dupliquer et se propager ; une charge utile porteuse de la partie réellement offensive capable par exemple de copier, modifier ou détruire de l'information ou une fonctionnalité.

Les *malwares* les plus efficaces utilisent généralement un « *zero-day exploit* », c'est-à-dire une vulnérabilité qui n'a pas été préalablement identifiée et pour laquelle aucun correctif n'a encore pu être publié. Le vecteur doit en outre être codé de façon suffisamment originale pour ne pas être reconnu par les défenses en place (anti-virus par exemple). L'utilisation de « *zero day exploit* » s'avère extrêmement rare : sur plusieurs millions de nouveaux *malwares* détectés annuellement, une dizaine exploitent ce type de vulnérabilité[155]. En effet, la détection/découverte de failles nouvelles dans la programmation de systèmes d'exploitation exige des compétences informatiques pointues : il faut être capable d'analyser des millions de lignes de code pour y parvenir.

A titre d'exemple, Confiker est un *malware* de type virus qui a affecté de très nombreux ordinateurs à travers le monde en 2008-2009 mais sans créer de dommage notable. Tout s'est passé comme s'il s'agissait d'un vecteur sans charge utile. A ce titre, ce virus s'apparenterait selon certains experts à une démonstration d'une capacité ou à la qualification d'un nouveau système[156]. L'extrême complexité du logiciel semble montrer que sa conception dépasse largement les compétences des principaux pirates opérant à cette période et serait le résultat d'une coopération entre des spécialistes de divers horizons.

A l'inverse, le *malware* Stuxnet de type ver, qui a frappé des installations nucléaires iraniennes à l'été 2010, était équipé à lui seul de quatre « *zero-day exploit* » pour assurer une efficacité maximum, là où Conficker n'en utilisait qu'un. En termes offensifs, il était doté de deux charges utiles très sophistiquées : la première pour dérégler la vitesse de rotation des centrifugeuses et ainsi progressivement causer leur détérioration, l'autre pour neutraliser les systèmes numériques d'alerte, d'affichage et d'arrêt qui contrôlent les centrifugeuses.

Ainsi, le niveau de sophistication de Stuxnet le classe au-dessus des *malwares* vus jusque-là, y compris Conficker. Il était le produit de compétences de très haut niveau et est vraisemblablement le précurseur d'une nouvelle catégorie de capacités offensives. Pourtant de telles capacités, aussi sophistiquées soient-elles, ont aussi leurs inconvénients.

[155] Kim Zetter, « How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History », Wired, 11 July 2011.

[156] Entretiens B. Gruselle, 2009.

D'une part, l'analyse de l'attaque permet de connaître les vulnérabilités utilisées et d'établir (en général rapidement) des correctifs : ces vulnérabilités ne pourront donc plus être utilisées pour une attaque ultérieure. Plus généralement, l'analyse du code révèle les éléments originaux du codage conduisant à une sorte de « prolifération » *de facto* ; le code de Stuxnet a été aujourd'hui mis en ligne et peut maintenant être utilisé tel quel ou, éventuellement, amélioré.

D'autre part, si les vulnérabilités employées sont choisies pour atteindre certaines fonctions de la cible visée – logiciels Siemens dans le cas de Stuxnet –, elles peuvent être aussi présentes dans des systèmes *a priori* sans rapport direct avec l'objectif – tous les équipements Siemens en Chine dans le cas de Stuxnet –, voire chez l'utilisateur de la capacité offensive. ***Pour parvenir à un ciblage précis des attaques permettant de mieux diriger les effets, il faudrait pour le moins disposer d'une cartographie détaillée et temps réel des réseaux constamment remise à jour grâce à des « robots fureteurs ».*** La mondialisation croissante du marché des technologies de l'information devrait rendre cette tâche de plus en plus difficile.

Attaques physiques contre des systèmes informatiques ou de communication

Les télécommunications entre les États dépendent physiquement de supports satellitaires (segments spatial et sol) et terrestres (câbles sous-marins en fibre optiques). A l'heure actuelle, 99 % du trafic Internet entre les pays circule via des câbles sous-marins, et une attaque physique les ciblant serait de nature à perturber durablement le trafic Internet des pays connectés.

A titre d'exemple, fin mars 2008, quatre coupures de câbles sous-marins ont eu lieu dans la région du Moyen-Orient[157] causant la perte de 70 % des connexions égyptiennes et de près de 30 % des services fournis par son industrie de centres d'appels[158]. Or, de telles concordances temporelle et spatiale sont rares et une des coupures est intervenue dans une zone stratégique (le « goulot » au nord d'Alexandrie où convergent les lignes de Méditerranée) interdite à la navigation...

Il existe une grande disparité mondiale dans la distribution des câbles sous-marins. Les liaisons câblées transatlantiques et à travers le Pacifique sont très denses et offrent beaucoup de redondances. Il s'ensuit que l'Europe et les États-Unis sont, de loin, moins vulnérables à des ruptures que la région du Moyen-Orient qui ne dispose que de trois câbles majeurs, ou l'Afrique qui est encore desservie par un seul (cf. infra).

[157] Deux coupures intervinrent en Méditerranée, près d'Alexandrie et près de Marseille, et touchèrent les réseaux indiens, pakistanais, égyptiens, qataris, saoudiens, bahreinis et des Émirats Arabes Unis. Les deux autres affectèrent le câble reliant Oman aux Émirats et celui reliant le Qatar aux Émirats Arabes Unis.

[158] Mais avec un impact minime en Iran, au cas où ce pays aurait été la cible de cet acte malveillant.

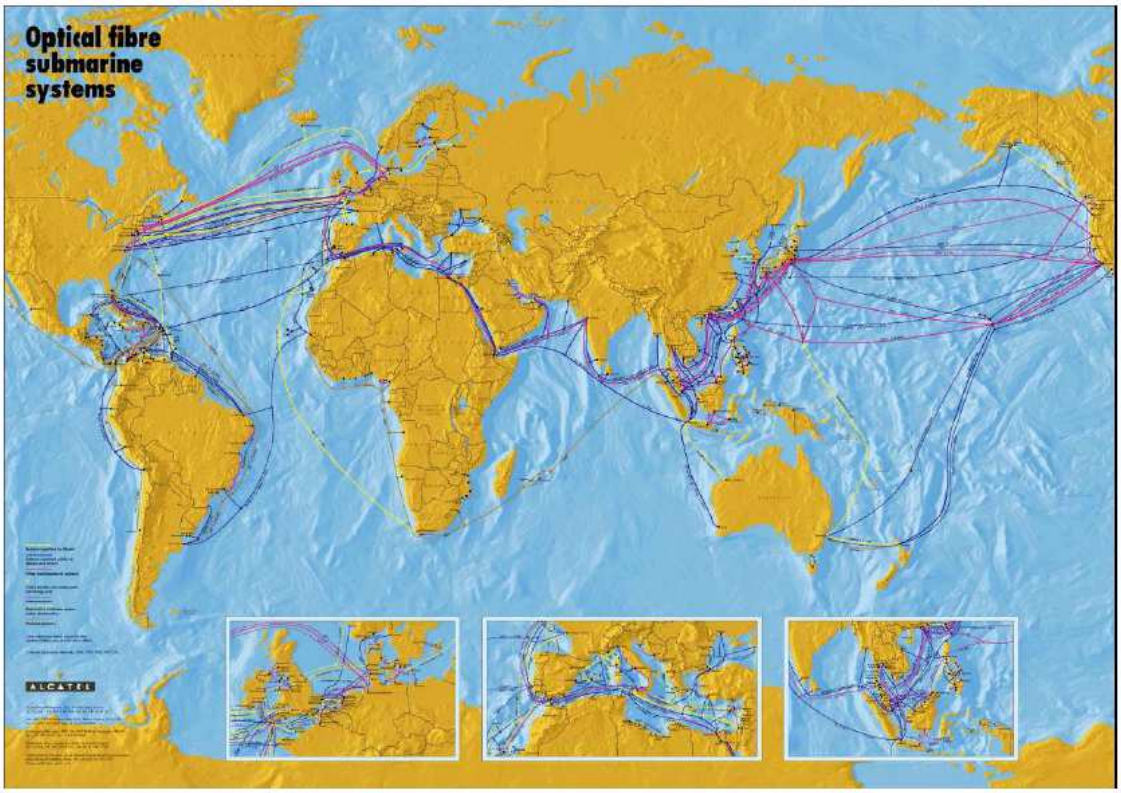


Figure 14 : Réseau des câbles sous-marins à fibres optiques

Selon John Borland, une première coupure peut limiter les connexions, tandis qu'une seconde les paralyseraient complètement[159]. Si une coupure accidentelle peut avoir des effets désastreux à l'échelle d'un pays, c'est uniquement parce qu'il était situé en bout de chaîne du réseau de fibres optiques[160]. En revanche, les risques sont infimes en France dans la mesure où le pays bénéficie d'une irrigation très dense et de nombreuses lignes secondaires qui seraient amenées à palier à la coupure de certains câbles.

Le sabotage de câbles sous-marins serait donc une arme s'appuyant sur les différences de développement dans le domaine des technologies de communication entre les régions. Au-delà des considérations de développement, les pays géographiquement contraints à une localisation en bout de chaîne sont également vulnérables : Islande, Nouvelle Zélande, îles du Pacifique, Madagascar…

Ce type de capacité offensive s'avère donc la plus efficace vis-à-vis de pays câblés de manière particulière. Dès lors, l'augmentation des dessertes devrait conduire à réduire l'intérêt d'exploiter ce type de solution à des fins offensives (cf. infra).

On peut aussi noter que les liaisons satellites pourraient être une cible possible, surtout si les liaisons Internet satellitaires se développent. Toutefois, dans la mesure où les

[159] John Borland, « Analyzing the Internet Collapse: Multiple fiber cuts to undersea cables show the fragility of the Internet at its choke points », *Technology review*, February 5, 2008. http://www.technologyreview.com/Infotech/ 20152/?nlid=854&a=f

[160] Benjamin Ferran, « Comment une grand-mère a pu couper l'Internet d'un pays », *Le Figaro*, 8 avril 2011. Peut être trouvé à http://www.lefigaro.fr/hightech/2011/04/08/01007-20110408ARTFIG00418-comment-une-grand-mere-a-pu-couper-l-Internet-d-un-pays.php

satellites dédiés à ce genre d'emploi sont majoritairement gérés par des opérateurs privés qui optimisent leur emploi selon les demandes des clients, leur neutralisation aurait vraisemblablement des conséquences au-delà de la cible visée. Ainsi, neutraliser un satellite (ou ses répéteurs) pourrait créer plus d'effets collatéraux sur des pays tiers que de dégâts à la cible.

Il existe des moyens et des procédures qui pourraient être utilisées pour faciliter l'attribution d'attaques numériques

Une fois une attaque informatique reconnue comme telle, l'identification des auteurs, à commencer par les adresses Internet[161] à l'origine des flux de données ayant contribué à l'agression, peut être d'une grande complexité. L'abondance des données qui peuvent être à l'origine de l'infection et les possibilités de rebond dans l'adressage brouillent efficacement les pistes qui permettraient de remonter à un auteur spécifique.

De plus, même si les adresses d'origine ont pu être identifiées sans ambigüité, l'établissement de l'identité des personnes et de leurs intentions requiert la capacité d'analyser d'autres sources d'information à grande échelle (ex : communications téléphoniques), voire celle d'enquêter physiquement sur l'utilisation des ordinateurs concernés.

La capacité d'attribution dépend donc (1) de la capacité à collecter massivement les messages circulant sur les réseaux et à analyser rapidement un volume colossal de données collectées et (2) de la possibilité de compléter le traitement numérique par d'autres actions de recueil de renseignement ou d'enquête.

Collecte des données

Il s'agit d'intercepter là où circule le plus grand nombre de messages, c'est-à-dire sur les réseaux à plus haut débit possible. Là encore les systèmes satellitaires et les câbles sous-marins sont des cibles de choix.

Côté spatial, la collecte peut se faire par des satellites de renseignement (COMINT, ELINT) ou des systèmes d'écoute installés dans des satellites civils de communication développés par l'industrie. Les États-Unis sont particulièrement bien placés dans ce domaine, tant pour ce qui est de la flotte de satellites d'écoute en orbite, que pour les capacités industrielles de construction de satellites à l'exportation. En matière d'écoute, ils s'appuient physiquement sur le programme Echelon et son réseau mondial de stations d'écoute implantées dans le cadre de la coopération dans le domaine du renseignement avec le Royaume-Uni, le Canada, l'Australie et la Nouvelle Zélande. Côté sous-marin, le problème est plus complexe car les fibres-optiques n'émettent pas de radiation électromagnétique.

[161] Le protocole IP fixe à chaque ordinateur/serveur connecté à Internet une série unique de chiffres qui constitue son adresse. http://en.wikipedia.org/wiki/Internet_Protocol

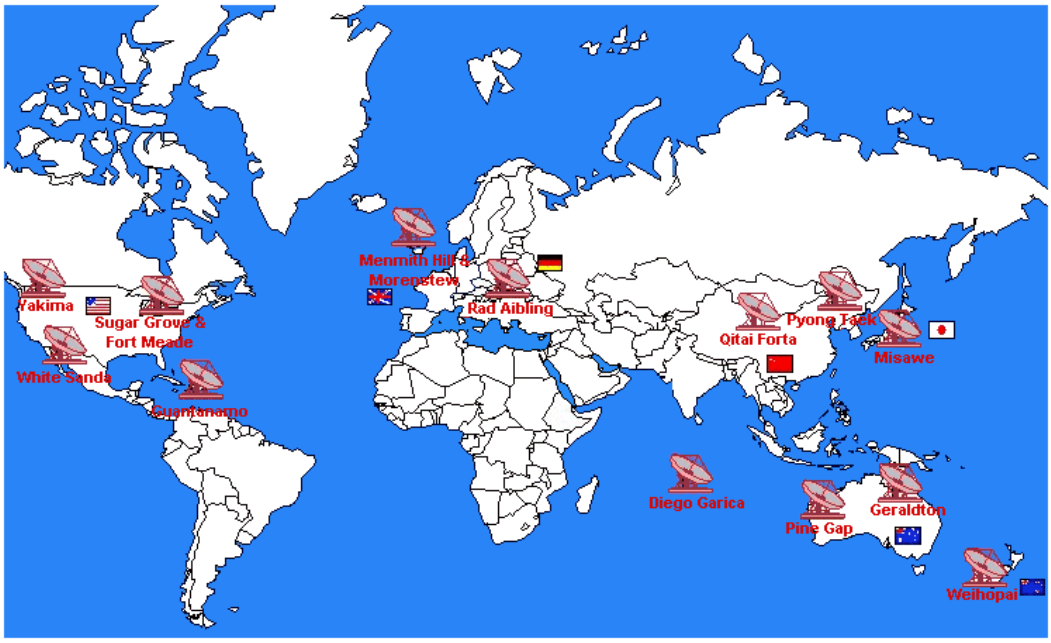
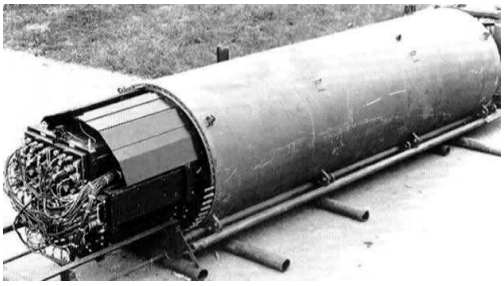


Figure 15 : Réseau de stations sol Echelon

Encadré 5 : Interception de données dans les fibres optiques[162]



En supposant résolu l'accès au câble dans des conditions suffisantes de sécurité et de discrétion, les données lumineuses peuvent être récupérées de trois manières. La première mise sur la perte de signal et la nécessité de le ré-amplifier. Un branchement par induction (grâce à un pod ou « cloche d'écoute » tel que celui présenté sur la photo) est donc possible au niveau de ces « amplificateurs » ou « répéteurs » intermédiaires qui transforment le signal optique en signal électrique, l'amplifient et le retransforment en signal optique. Ces « amplificateurs » s'échelonnent tous les 100 km environ. Cette solution est rendue partiellement obsolète par le développement en 1995 de la technique EDFA (améliorée en 2000) qui permet l'amplification optique par un dopage à l'erbium et, par voie de conséquence, rendrait les amplificateurs tout à fait inutiles ; pour autant, des « amplificateurs » sont toujours présents bien que plus rares. Les deux autres solutions recommandent soit de plier la fibre pour laisser échapper quelques rayons de lumière qui sont alors récupérés pour reconstituer le message complet, soit d'implanter une dérivation. La dernière solution semble la plus facile à réaliser, mais elle implique une coupure momentanée (voire une altération) du signal, ce qui n'échappera en aucune façon aux instruments de télémesure des câbles opérateurs (à moins d'obtenir sa complicité), si brève soit-elle. Des incidents récents intervenus sur des câbles sous-marins montrent que, dans le meilleur des cas, les flux sont « re-routés » vers des routes secondaires éventuellement « contrôlées », c'est-à-dire mises préalablement sous écoute.

[162] Contribution de Sébastien Urbieta-Martin en Master de Sécurité Internationale, thème « Conflits et coopérations dans le cyberespace », Sciences Po Paris, 2011.

Quoi qu'il en soit, les interceptions sur les câbles sont relativement plus faciles à effectuer sur terre, notamment dans les stations dîtes d'« atterrissement », surtout s'il est possible d'établir une coopération avec l'opérateur propriétaire du câble.

La carte des câbles sous-marins révèle que la plupart de ceux situés dans l'Atlantique et dans le Pacifique sont accessibles via les stations d'atterrissement situées sur des territoires membres du réseau Echelon. A l'inverse, les câbles qui alimentent l'Asie en connectant le Japon, la Chine, Singapour, l'Indonésie, l'Inde et les Pays du Golfe, ainsi que le réseau reliant l'Europe au Maghreb et au Moyen-Orient sont physiquement isolés des moyens d'écoute du réseau Echelon.

Les États-Unis ont démontré durant la Guerre froide leur capacité à pratiquer des interceptions sur câble, notamment grâce au sous-marin *Halibut* chargé de l'opération « *Ivy Bells* » pour intercepter les données transitant en mer d'Okhotsk, puis à l'USS Parche pour l'écoute des communications au large de Mourmansk. Par la suite les opérations se sont étendues aux câbles reliant l'Europe à l'Afrique de l'Ouest.

Comme le rapporte le site officiel du réseau Echelon, les interceptions sous-marines se sont poursuivies après la Guerre froide : « *Nor has the end of the Cold War led to the termination of ship-based signals intelligence collection or submarine reconnaissance operations – including operations to tap undersea cables* »[163]. Au cours de la dernière décennie, le sous-marin *Jimmy Carter* a inauguré, entre autres, de nouvelles techniques d'interception grâce à une chambre sous-marine similaire à celles utilisées par les entreprises réparant les câbles sous-marins, détachable du sous-marin et alimentée par lui en oxygène et en électricité.

Tri et analyse des données recueillies

Plus le volume de données recueillies est important, plus il est difficile de les trier et analyser pour identifier rapidement les informations pertinentes, par exemple relatives à une attaque informatique donnée. La « fouille de données » se fait par étapes en réduisant progressivement le volume de messages potentiellement intéressants. Sans une bonne caractérisation préalable de l'incident – malgré une montée en puissance des outils de traitement automatique des paquets de données[164] –, le tri ne peut qu'être grossier, la quantité de messages à traiter importante et l'analyse fine longue.

Les données issues des différentes capacités de collecte des États-Unis convergent vers les « fermes de serveurs » de la *National Security Agency* (NSA) à Fort Meade (Maryland) et au Texas. Les messages cryptés – on estime que 10 à 20 % des messages mondiaux sont chiffrés – sont déchiffrés, qu'ils soient commerciaux – avec un niveau de cryptage moindre – ou bénéficiant de moyens de chiffrement plus puissants.

Il est difficile de savoir dans quelle mesure la masse d'information systématiquement collectée et les capacités de traitement informatique de la *National Security Agency* permettent d'identifier l'origine informatique des cyber-attaques portées à la connaissance des responsables américains. Le 7 juillet 2001, le *Wall Street Journal* a rapporté

[163] « Desperately seeking signals » by Jeffrey Richelson : http://echelononline.free.fr/documents/bulletin.htm

[164] Les logiciels de *Deep Packet Inspection* (DPI) permettent de filtrer et de traiter automatiquement des paquets de données interceptés en identifiant des éléments selon des critères d'alerte prédéfinis (un mot, un protocole..). http://en.wikipedia.org/wiki/Deep_packet_inspection

que la NSA était parvenue à percer et extraire des informations des câbles à fibres optiques[165]. Au cours de l'interview donnée au quotidien, le lieutenant général Michael Hayden, directeur de la NSA, suggère toutefois que ce n'est pas l'accès au câble qui représente le problème majeur, mais plutôt la diversité, la vitesse et le volume incommensurable d'informations qui transitent : « *There's simply too much out there, and it's too hard to understand* ». Plus récemment, il faut noter que les services américains n'ont pas été en mesure, au moins à ce jour, d'identifier tous les informateurs de *Wikileaks*.

Malgré les succès limités et les obstacles à un traitement systématique à l'échelle mondiale de l'ensemble des communications numériques, les États-Unis s'avèrent être le pays le plus avancé en matière de capacités d'interception de traitement de données.

Les États-Unis ont progressé vers une coordination des actions de cyber-défense et de cyber-sécurité même si la mise en place d'une stratégie nationale cohérente de protection et de dissuasion reste encore lointaine

En plaçant dès son élection la sécurité numérique au cœur des priorités de son administration, le Président Obama a engagé une réforme historique des efforts américains dans les domaines de la cyber-sécurité et de la cyber-défense. Il a pu capitaliser sur les efforts des gouvernements précédents qui ont également lancé des programmes et des initiatives visant à renforcer les capacités des services et des agences dans ces deux domaines.

La première brique posée par le gouvernement actuel afin de renforcer l'organisation en matière de sécurité numérique correspond au lancement puis à la publication dès 2009 d'une revue stratégique sur le cyberespace. D'autres documents portant sur des aspects spécifiques du développement du domaine informatique – en particulier sur la question de la protection des identités ou du développement de l'informatique en nuage – ont été publiés depuis mais c'est cette initiative qui a abouti à quelques conclusions clefs qui ont structuré les projets américains depuis :

- Plusieurs services et agences au sein des divers ministères sont impliqués pour leurs sphères respectives de compétences et à des degrés divers en matière de sécurité et de défense numérique. Dès 2003, l'administration précédente, ayant constaté le morcellement des efforts, avait donné au directeur du *Department of Homeland Security* (DHS) la responsabilité de superviser toutes les activités de cyber-sécurité et de coordonner les efforts de toutes les agences pour la protection des infrastructures gouvernementales et publiques[166].

  En janvier 2008, la *Comprehensive National Cybersecurity Initiative* (CNCI) entreprend d'élargir le spectre de coordination des efforts en incluant les aspects relevant du renseignement et la dimension offensive. Fin 2009, le DHS est chargé d'établir un centre commun national de suivi et de surveillance des activités numériques gouvernementales (le *National Cybersecurity and Communication*

[165] G. Fouchard, « Blind Mans's Bluff ou le piratage des câbles en 1975», *Bulletin de l'Association des Amis des Câbles Sous-marins*, n°26, Le N/C Ampere dans les glaces de Terre Neuve, Juin 2004.

[166] The White House, « The Cyberspace Policy Review », January 2009, p. 4. Le DHS est directement chargé de l'administration et de la protection des passerelles internet avec des noms de domaine en « .gov ».

Integration Center) qui doit fournir une image opérationnelle commune de l'état du cyberespace à l'ensemble des services fédéraux. L'ensemble des parties prenantes, y compris le Pentagone, la *National Security Agency* (NSA) ou encore le *Federal Bureau of Investigation* (FBI), participe à l'armement de ce centre opérationnel permanent. Sa mise en place a également été rendue possible par la signature d'un *Memorandum of Agreement* entre le DHS et le DoD qui permet l'intégration d'une équipe de la NSA dans l'organisation.

Après la publication de la revue stratégique de 2009, le Président nomme un coordinateur national placé au niveau de l'exécutif et dont la tâche consiste à la fois à faciliter le développement d'une stratégie cohérente au niveau des ministères, des agences et des services mais également à renforcer les partenariats avec le secteur privé en matière de sécurité numérique.

- Les aspects internationaux font partie des priorités mises en avant par l'administration Obama dans le domaine de la cybersécurité. La revue de 2009 propose ainsi la mise en place d'une stratégie internationale visant à la fois au développement d'un cadre juridique et au renforcement des coopérations avec les alliés. Elle avance également le besoin d'améliorer le dialogue avec les Economies émergentes afin de développer une norme multilatérale et des moyens de répondre à la nature souvent transnationale des risques numériques. L'*International Strategy for Cyberspace*, publiée en mai 2011, distingue plusieurs axes concernant la mise en place de règles qui pourraient permettre de régir l'attitude des États dans le cadre de conflit dans le cyberespace. Deux méritent en particulier que l'on s'y attarde. Conformément à la Charte des Nations Unies, Washington considère que les États doivent pouvoir exercer leur droit à l'autodéfense. Par ailleurs, les États-Unis indiquent que les gouvernements doivent être tenus pour responsables de la sécurité des infrastructures cyber en tant que bien commun mais également de la sécurisation des systèmes nationaux face aux risques de mauvais usages[167]. La question se pose toutefois de savoir quelles agressions – tant en termes de nature, d'intensité, de fréquence et de cible – peuvent être qualifiées en tant qu'actes de guerre. Le risque relevé par certains experts serait de réduire la crédibilité d'une posture dissuasive en fixant des « lignes rouges » qui pourraient être franchies de façon trop fréquente ou trop facilement[168]. Une telle situation abaissant le seuil de riposte à une agression créerait en particulier le risque de rendre difficile la gestion de l'escalade avec les attaquants potentiels.

- La coopération avec l'ensemble des acteurs nationaux du domaine est essentielle mais elle n'exonère pas l'Administration de ses responsabilités en matière de sécurité. De fait, si la revue de 2009 souligne sans réserve le besoin de développer de nouveaux liens avec le secteur privé et associatif, elle rappelle également qu'en cas d'incident significatif, c'est à la Maison Blanche que revient la responsabilité de coordonner et de conduire la réponse.[169]

Au sein du département de la Défense, des travaux destinés à mieux coordonner les initiatives des armées et des services et à mettre en place un cadre stratégique pour les

[167] The White House, « International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World », May 2011, pp. 9-10.

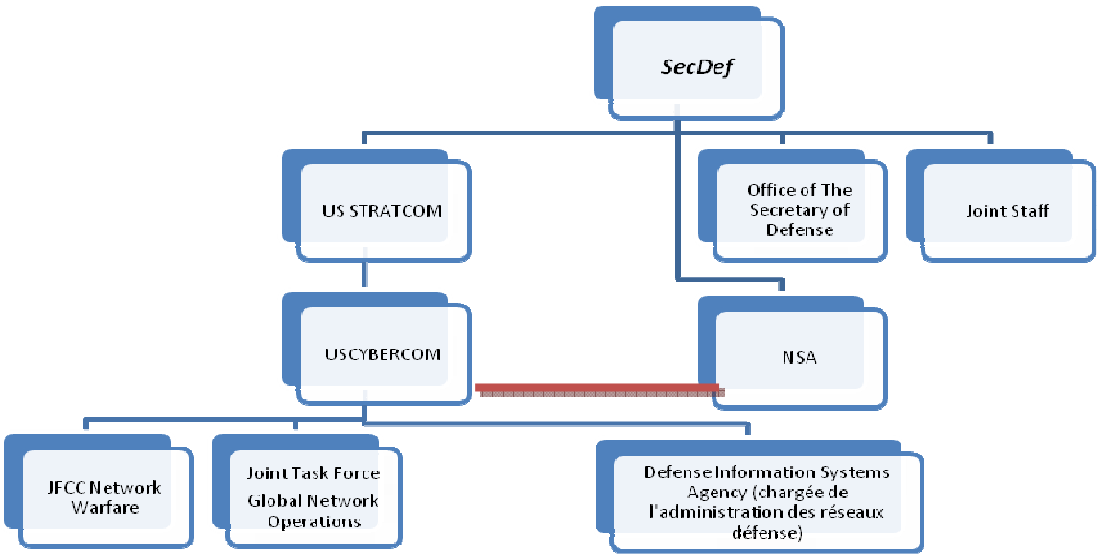
[168] Entretiens de l'auteur, Washington, octobre 2011.

[169] The White House, « The Cyberspace Policy Review », January 2009, p. 23.

opérations militaires dans le cyberespace ont accompagné les réflexions nationales. Ainsi, en 2008, STRATCOM publie un concept d'opération consacré au domaine numérique[170]. La revue de défense de 2010 (QDR2010) inscrit finalement la capacité à opérer dans l'espace numérique comme priorité du département et des forces, qu'il s'agisse de protéger les moyens et les systèmes appartenant à la Défense ou de surclasser un adversaire dans ce domaine spécifique.[171]

La mise en place du commandement cyber des forces, à partir de mai 2010, doit permettre au Pentagone d'unifier les efforts des services dans le domaine. Elle répond à une attaque de grande ampleur conduite en 2008 contre le réseau protégé du département de la Défense et qui aurait permis à un service étranger de voler des milliards d'octets de données, y compris des informations confidentielles portant sur des programmes d'armement en cours de développement[172]. CYBERCOM intègre les unités créées par les armées[173] pour gérer à la fois les aspects de protection des infrastructures numériques – et notamment la surveillance des réseaux de la Défense et des passerelles existantes avec internet, c'est-à-dire les domaines en « .mil » dont la gestion revient au Pentagone – mais également les aspects de guerre numérique (« *netwar* »). Le commandement doit en effet développer la gestion du domaine numérique afin d'en faire la cinquième dimension des opérations militaires américaines.

CYBERCOM se trouve sous le commandement du directeur de la *National Security Agency*[174] qui s'avère être l'un des services du Pentagone les plus avancés dans le domaine de la sécurité et de la défense numériques.



[170] Government Accountability Office, « Defense Department Cyber Efforts », July 2011, p. 11.

[171] Department of Defense, « Quadrennial Defense Review, 2010 », February 2010, p. 38.

[172] http://www.lemondeinformatique.fr/actualites/lire-les-systemes-informatiques-du-pentagone-attaques-par-une-clef-usb-31468.html

[173] L'Air Force, la Marine, les *Marines* et l'Army ont centralisé au sein de leurs commandements leurs efforts en matière cyber depuis 2010. Voir Center for New American Security, « America's Cyber Future: Security and Prosperity in the Information Age », Edited by Kirstin Lord & Travis Sharp, June 2011, pp. 32-33.

[174] Actuellement le Général Keith Alexander (*US Army*).

Figure 16 : Organisation du DoD en matière de cybersécurité et de cyberdéfense

Malgré l'existence de cette organisation, les responsabilités en matière de défense dans le domaine numérique s'avèrent encore très atomisées au sein du Pentagone. En matière de définition des aspects stratégiques et politiques, plusieurs acteurs au sein de l'*Office of the Secretary of Defense* sont chargés de superviser les divers aspects relatifs à la lutte informatique défensive comme offensive et des programmes d'armement liés[175]. Dans le domaine opérationnel également d'autres acteurs au sein de l'État-major travaillent à la fois sur les aspects stratégiques et sur les questions de doctrine et de concept d'emploi.

Ainsi, il apparaît encore trop tôt pour juger des bénéfices réels que le département de la Défense tirera de l'effort de réorganisation qu'il a engagé à partir de 2009, même si le rattachement des commandements interarmées (JFCC *Network Warfare* et JTF *Global Network Operation*) à CYBERCOM paraît offrir quelques garanties d'un meilleur fonctionnement d'ensemble.

A contrario, le renforcement des capacités et de la cohérence d'ensemble du volet militaire met en exergue les faiblesses qui existent encore sur la partie civile en matière de sécurité numérique. Le département de la Sécurité du territoire (DHS) semble en effet souffrir à la fois d'un certain retard d'expertise vis-à-vis de la défense mais également de difficultés spécifiques d'organisation qui n'ont pas encore été surmontées. En outre, la concurrence qui existe entre DHS et DoD – auxquels il faut sans doute ajouter le département de la Justice et plus particulièrement le FBI qui se trouve en première ligne pour la gestion de la criminalité – sur les questions de sécurité numérique sont de nature à renforcer les difficultés de coordination alors même qu'il semble subsister un manque de direction politique/stratégique au niveau de l'exécutif[176].

D'un point de vue budgétaire, les États-Unis investissent lourdement en matière de sécurité numérique. En 2010, 12 milliards de dollars auraient été dépensés par l'ensemble des services et agences dans le domaine[177]. En flux annuel, environ 15 % des budgets dédiés aux technologies de l'information seraient consacrés à la sécurité. Le département de la Défense représente le plus fort investissement avec un montant moyen de 3 milliards de dollars (3,2 milliards prévus pour 2012) qui couvre à la fois les investissements matériels mais également la formation et l'entraînement des personnes intervenant dans le domaine[178]. Le DHS est le deuxième plus gros investisseur avec des budgets compris entre 500 millions et 1 milliard de dollars par an (936 millions demandés en 2012). Une partie importante de cette somme est consacrée au CERT américain (391 millions de dollars pour 2012[179]).

[175] Government Accountability Office, « Defense Department Cyber Efforts », July 2011, pp. 19-20.

[176] David Hollis, « USCYBERCOM: The Need for a Combatant Command versus a Subunified Command », National Defense University, Joint Force Quaterly, issue 58, 3rd Quarter 2010, p. 51.

[177] Center for New American Security, « America's Cyber Future: Security and Prosperity in the Information Age », Edited by Kirstin Lord & Travis Sharp, June 2011, p. 34.

[178] Hors black programs.

[179] Ibid.

Parmi les projets financés par le budget du Pentagone, le programme de création d'un cyber-polygone de tir (*National Cyber Range* – NCR) mérite d'être présenté tant il est susceptible de jouer un rôle clef pour permettre l'essai des armes numériques qui pourraient être utilisées dans le cadre de la montée en puissance d'une dissuasion numérique. Le programme piloté par la DARPA et confié à Lockheed Martin – pour le développement comme pour la gestion – a débuté en 2009 afin de créer un système capable de simuler le fonctionnement d'un réseau informatique de type Internet et de permettre d'essayer en grandeur réelle et de mesurer les effets de l'utilisation de logiciels[180]. Le projet qui doit aboutir en 2012, a un budget estimé de 130 millions de dollars[181].

Malgré les coupes qui devraient affecter pour la décennie à venir les budgets des principaux ministères et agences américains, la sécurité numérique semble à l'heure actuelle non seulement épargnée mais sera vraisemblablement un des seuls axes de la politique américaine qui fera l'objet d'un financement en hausse[182].

Même si les montants investis ne peuvent pas conduire à supposer que l'organisation américaine de cybersécurité et de cyberdéfense se montre efficace, ils donnent toutefois quelques éléments d'éclairage sur le décalage qui semble exister aujourd'hui entre les États-Unis et les autres pays occidentaux dans ces domaines. Ainsi, le budget de l'ANSSI devrait atteindre environ 100 millions d'euros en 2012[183]. Côté britannique, le *General Communication Headquarters* (GCHQ en charge des aspects défensifs) devrait obtenir, sur une période de quatre ans, 650 millions de livres supplémentaires[184] pour le financement du développement d'une capacité offensive[185].

[180] DARPA, « The National Cyber Range: A National Testbed for Critical Security Research ». Consulté à http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf

[181] Julius Motal, « Pentagon to Prep for Battle Via 'National Cyber Range' », PCMag.com, June 20, 2011.

[182] Seung Min Kim, « Leon Panetta: Don't Gut our Defense », Politico, 1 November, 2011.

[183] http://www.itespresso.fr/la-france-se-dote-dune-vraie-agence-gouvernementale-de-cyber-securite-30404.html

[184] Pour un budget total de cybersécurité de 1 milliard de livres sur cette période.

[185] Nick Hopkins, « UK developing cyber-weapons programme to counter cyber war threat », *The Guardian*, 30 May 2011.

Conclusion

La mise en place d'une dissuasion numérique pourrait constituer l'une des solutions pour répondre à l'aggravation des risques créés par la montée en puissance d'acteurs malveillants utilisant les outils du cyberespace pour leur profit personnel ou pour conduire des attaques à finalité destructrice contre des infrastructures importantes pour les États et les populations. Avec l'apparition d'applications numériques de plus en plus omniprésentes dans la vie sociale, économique et, de façon générale, dans la plupart des activités humaines, les vulnérabilités informatiques devraient se multiplier à moyen et long termes.

Ainsi, les derniers cas de tentative d'intrusion connus – en particulier les révélations sur l'étendue et la nature du programme chinois d'espionnage « *Shady RAT* » visant plusieurs dizaines d'entreprises, de services gouvernementaux et d'organisations internationales[186] – montrent que le cyberespace est devenu le champ de conflits d'une ampleur suffisamment importante pour soulever la problématique de l'utilisation d'actions offensives fondées sur la logique de légitime défense.

Dans cette perspective, il semble utile de considérer les moyens d'une dissuasion numérique visant à exercer sur les acteurs malveillants une menace de représailles suffisamment crédible pour réduire leur intérêt à conduire les actes affectant de façon significative le fonctionnement et l'intégrité des systèmes d'information et des réseaux jugés comme les plus sensibles non seulement pour la sécurité nationale mais, éventuellement, pour le fonctionnement de la société et de l'économie.

Il ressort de l'étude que le concept de dissuasion pourrait être utilisé dans le cyberespace mais que son application n'est envisageable que sous des formes et dans des conditions différentes de celles de la dissuasion nucléaire. De fait, on ne peut que constater que les spécificités du cyberespace, des systèmes d'information et des attaques qui sont menées contre eux doivent conduire à proposer des solutions spécifiques. Plusieurs problématiques particulières se posent particulièrement pour la mise en œuvre d'une dissuasion numérique :

- En premier lieu, l'identification des responsables d'une attaque significative ou d'une campagne comprenant plusieurs agressions s'avère en général difficile et longue. Dans certaines circonstances, il peut même s'avérer impossible de déterminer avec un niveau de certitude élevé[187] la responsabilité et l'implication de certains acteurs. De fait, la possibilité d'agir par procuration et l'utilisation des moyens techniques existants afin de cacher ses traces rendent dans les faits l'attribution incertaine pour les attaques qui ne sont pas revendiquées. Pour autant, il paraît dans certains cas possible, en utilisant l'ensemble des sources d'information et de renseignement disponibles, en analysant le contexte et la cible de l'attaque ainsi que les moyens utilisés, de finalement identifier le responsable. En outre, il convient de souligner que la question de la responsabilité des États dans le cas d'attaques menées depuis leur territoire et grâce à leurs infrastructures numériques semble aujourd'hui posée par certains pays occidentaux, en particulier les États-Unis. Ainsi, le document de stratégie internationale pour le cyberespace, publié par

[186] http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

[187] En tout cas suffisamment important pour permettre de publiquement accuser l'auteur présumé.

la Maison Blanche en mai 2011, souligne que la mise en place de normes internationales en matière de sécurité numérique doit inclure la reconnaissance de la responsabilité des États[188].

- Par ailleurs, alors que l'on doit supposer que l'exercice de la force dans une logique de représailles doit se faire avec des moyens de même nature que les attaques, la mise au point de logiciels susceptibles d'affecter suffisamment les adversaires pour permettre de les dissuader, mais également la démonstration de leur efficacité peuvent s'avérer problématiques. Ainsi, si des capacités offensives peuvent être développées par les États, la structure d'Internet, au moins sous sa forme actuelle, rend délicate toute forme de démonstration en vraie grandeur. Or, de telles démonstrations doivent être effectuées pour établir la crédibilité des moyens et des effets attendus.

- Des capacités défensives et d'attribution efficaces, donc crédibles, devraient être conçues dans le cadre d'une coopération étroite avec les pays partageant la même vision des réseaux informatiques et, singulièrement, d'Internet. Ces coopérations doivent inclure le respect de normes (standards et bonnes pratiques), des échanges d'informations, la coordination de systèmes d'alerte et d'identification des auteurs d'agressions, des exercices de réponses à des attaques, etc. Elles doivent *in fine* garantir que les États entreprennent en commun les démarches informatiques et physiques permettant d'établir l'identité des auteurs ou de leurs commanditaires. Pour être fonctionnelles, ces coopérations doivent également intégrer les opérateurs d'infrastructures jugées sensibles, qu'ils soient privés ou publics. En particulier, il paraît indispensable – et vraisemblablement urgent au vu de la montée en puissance des fournisseurs chinois – de traiter la question des chaînes d'approvisionnement pour les produits et services destinés aux systèmes d'information. L'idéal serait de recourir à des capacités industrielles – si possible françaises ou européennes – ayant fait l'objet d'une expertise de validation conduite par les autorités nationales.

- Les stratégies de communication qui doivent accompagner la manœuvre dissuasive dans l'espace numérique soulèvent des difficultés qui sont directement liées à celles de l'identification des agresseurs et de l'attribution des attaques. Il faut faire preuve de flexibilité dans la politique de communication afin de prendre en compte les différents niveaux de visibilité des attaques au niveau du public ainsi que la diversité des agresseurs potentiels. Ainsi, certains peuvent ne pas être directement accessibles à des démarches diplomatiques ou conduites par des représentants officiels. En revanche, l'utilisation de l'ensemble du spectre des outils de communication existants doit être envisagée.

- Si de façon générale, les moyens offensifs permettant d'organiser des représailles contre un acteur malveillant identifié doivent rester dans le registre numérique et leurs effets doivent demeurer proportionnés à l'attaque subie, il ne faut pas exclure l'emploi de moyens asymétriques pour répondre à certaines agressions. En particulier face aux acteurs dont les intérêts numériques sont limités, le recours à des mesures de rétorsion physiques, financières ou à des actions juridiques doit être envisagé.

[188] The White House, « International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World », May 2011, p. 10.

La prise en compte des spécificités de l'espace numérique appelle à une démarche de restructuration des efforts afin de permettre l'émergence d'une stratégie de dissuasion fondée à la fois sur des mesures défensives crédibles et sur des moyens permettant de faire peser sur les agresseurs potentiels une menace à caractère dissuasif.

En premier lieu, il convient sans doute de mettre en place au niveau de l'exécutif des moyens permettant de coordonner l'ensemble des initiatives et des programmes conduits par les administrations en matière de sécurité et de défense numériques. Il s'agit également d'assurer le pilotage stratégique et l'autorité politique nécessaire sur l'ensemble des outils défensifs et offensifs. Cet échelon doit participer à la définition des règles d'engagement et des conditions d'emploi des armes numériques et coordonner les activités de veille et d'alerte.

L'architecture de dissuasion numérique qui devrait intégrer les services et moyens déjà consacrés à la sécurité informatique au sein des ministères y compris ceux de l'ANSSI, devrait également comprendre une division opérationnelle chargée, pour la partie offensive, d'élaborer les dossiers d'objectif, de gérer l'engagement des armes numériques (y compris le choix des moyens à utiliser), mais également d'évaluer et de caractériser les effets. Au niveau de l'expertise technique, une division aurait pour fonction de développer les armes et d'identifier les vulnérabilités des systèmes des agresseurs potentiels. Elle serait également chargée, avec les services de renseignement compétents, de participer aux efforts destinés à attribuer les attaques significatives à des acteurs malveillants et, le cas échéant, à leurs commanditaires.

En termes techniques justement, le développement d'armes numériques ayant des effets significatifs sur les systèmes ou les réseaux adverses exige des efforts de recherche permettant d'identifier des failles de sécurité (si possible nouvelles de type « 0 day exploit ») dans les codes utilisés, les logiciels déployés et les protocoles employés par les adversaires potentiels. Ainsi, la dissuasion devra disposer d'un spectre d'« armes » (chevaux de Troie, vers, virus…) assez large pour affecter une gamme d'acteurs très large mais suffisamment spécifiques pour causer des dégâts significatifs à des agresseurs particuliers. Cette nécessité pose quelques difficultés. En premier lieu, la démonstration de leur efficacité de façon « publique » s'avère pratiquement infaisable : de fait, l'utilisation de ces armes permet en théorie l'identification des vulnérabilités et des failles qu'elles exploitent, ce qui par conséquent les rend caduques[189]. Par ailleurs, il existe un risque de voir une arme affecter un nombre plus important de systèmes ou de réseaux que celui ciblé initialement.

Le développement d'un mécanisme permettant de faciliter l'attribution des actes malveillants repose sur (1) la capacité à collecter massivement les messages circulant sur les réseaux et à analyser rapidement un volume colossal de données collectées et (2) la possibilité de compléter le traitement numérique par d'autres actions de recueil de renseignement ou d'enquête. En l'état, ***seuls les États-Unis disposent*** des moyens et des compétences permettant de détecter et, éventuellement, d'attribuer une attaque. La *National Security Agency* (NSA) qui supervise le commandement des opérations

[189] A son tour, cette situation rend plus coûteuses et complexes les campagnes permettant d'essayer les armes numériques mises au point.

« cyber » du Pentagone – CYBERCOM créée en 2010 –, grâce à son réseau d'interception Echelon et à ses capacités de traitement de données, s'avère être l'un des seuls organismes au monde capable d'analyser les données numériques transitant par le réseau à l'échelle mondial et donc de rapidement identifier l'ensemble des machines impliquées dans une attaque.

En définitive, alors que l'élaboration d'une dissuasion dans l'espace numérique paraît nécessaire pour répondre à l'évolution rapide des menaces, les difficultés liées à sa mise en place effective demeurent nombreuses. A l'heure actuelle, seuls les États-Unis paraissent disposer des moyens et des structures qui leur permettraient d'y parvenir. Toutefois, Washington ne peut pas espérer faire fonctionner un tel système totalement seul et souhaite développer des partenariats renforcés avec ses alliés afin, d'une part, de faciliter les efforts visant à identifier les responsables d'une attaque significative en capitalisant sur les moyens d'enquête des autres États et, d'autre part, de renforcer les mesures dissuasives que ses alliés peuvent prendre.

Annexe 1
Principales attaques numériques recensées depuis 2007

- Mai 2007 : les sites du gouvernement estonien font l'objet d'une attaque en déni de service revendiquée par une organisation non gouvernementale russe (« Nashi »). En rendant les services publics numérisés inaccessibles pour les utilisateurs, le groupe russe parvient à désorganiser l'ensemble de la société estonienne extrêmement dépendante des systèmes d'information en ligne.

- Septembre 2007 : des réseaux informatiques gouvernementaux en France, au Royaume Uni, aux États-Unis et en Allemagne font l'objet d'une attaque qui aurait été menée depuis des machines situées en Chine. L'Allemagne accuse les autorités chinoises d'avoir commandité cette opération[190].

- Octobre 2007 : le gouvernement chinois indique que les réseaux gouvernementaux, dont certains appartenant à la deuxième académie chinoise, ont fait l'objet d'une campagne d'intrusion[191]. Il accuse les États-Unis et Taiwan d'avoir commandité ces opérations.

- Mars 2008 : des responsables américains indiquent que de nombreuses sociétés américaines, européennes et japonaises sont victimes de vols de propriété intellectuelle et d'espionnage effectués depuis le cyberespace.

- Mai 2008 (?) : le Pentagone est infecté par un code malveillant (vraisemblablement un cheval de Troie) introduit sur le réseau protégé par le biais d'une clef USB et qui se serait répandu lors de l'utilisation de supports de ce type[192]. Le secrétaire adjoint à la Défense, William Lynn, révèle en 2010 que ce logiciel espion pourrait avoir permis à une agence étrangère d'accéder à plusieurs milliards d'octets d'information, y compris des données classifiées[193]. Cette attaque, longtemps passée sous silence par les États-Unis, aurait accéléré la création du CYBERCOM. Il convient de souligner que trois ans après cette attaque, le Pentagone continu à nettoyer son système d'information.

- Mai 2008 : selon la DCRI, environ 3 000 sociétés françaises auraient été victimes d'attaques numériques à des fins d'espionnage, de sabotage ou de déstabilisation entre 2006 et 2008[194].

---

[190] http://www.generation-nt.com/commenter/pentagone-piratage-chine-usa-etats-unis-attaque-informatique-actualite-44779.html

[191] http://www.generation-nt.com/commenter/espionnage-chine-gouvernement-attaques-informatiques-actualite-45084.html

[192] Security and Defense Agenda, « A conversation on Cybersecurity with William J. Lynn III », September 15th, 2010.

[193] http://www.lemondeinformatique.fr/actualites/lire-les-systemes-informatiques-du-pentagone-attaques-par-une-clef-usb-31468.html

[194] http://www.latribune.fr/actualites/economie/france/20090625trib000392170/exclusif-3.000-entreprises-francaises-victimes-d-espionnage-economique-en-trois-ans.html

- Août 2008 : alors que les forces russes s'apprêtent à envahir la Géorgie, les réseaux numériques du pays, en particulier les sites gouvernementaux, subissent plusieurs attaques (intrusions et déni de service).

- Janvier 2009 : le ver Conficker infecte plusieurs réseaux numériques basés sur des systèmes d'exploitation Microsoft (dont Windows XP). La Marine nationale voit son réseau informatique mis en quarantaine après avoir été infecté, causant des difficultés pour l'accès aux plans de vol des missions aéronavales[195].

- Mars 2009 : une étude canadienne met au jour l'existence d'un réseau de cyber-espionnage opéré depuis la Chine et qui accéderait régulièrement à des milliers de machines infectées par des logiciels espions, y compris au sein de systèmes gouvernementaux. Le réseau « *Ghostnet* » deviendra le premier exemple documenté des efforts d'espionnage numérique de la RPC[196].

- Avril 2009 : des pirates obtiennent l'accès au réseau de données utilisé pour le développement du *Joint Strike Fighter* (F-35 JSF). Le Pentagone ne fournit aucune information sur la quantité ou la nature des données dérobées[197].

- Juin 2009 : dans un rapport publié sur la sécurité en 2008, le ministère allemand de l'Intérieur accuse la Chine et la Russie de conduire des actions répétées d'espionnage industriel via l'utilisation de l'espace cyber[198].

- Août 2009 : Albert Gonzales est arrêté par la police fédérale américaine pour avoir, avec plusieurs complices entre 2006 et 2008, contrefait 130 millions de cartes de crédit après avoir volé les données d'identité nécessaires et pour s'être introduit dans les réseaux d'information de plusieurs entreprises américaines[199]. Il s'agit du crime numérique le plus grave (en volume) jamais poursuivi par les tribunaux.

- Janvier 2010 : Google indique que les services chinois ont tenté de pénétrer sur ses réseaux informatiques d'entreprise. 34 autres sociétés de hautes technologies auraient également fait l'objet de tentatives élaborées de pénétration[200]. Les attaques auraient particulièrement visé les comptes Gmail d'activistes chinois.

- Avril 2010 : un rapport de l'Université de Toronto fait état de l'existence d'un programme chinois – dénommé *Shadow Network* – destiné à pénétrer dans les réseaux du ministère de la Défense indien et à en voler des données, en particulier sur des projets d'armement[201].

---

[195] http://en.wikipedia.org/wiki/Conficker

[196] http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[197] http://online.wsj.com/article/SB124027491029837401.html

[198] Le rapport 2010 insiste à nouveau sur ce problème pour l'année 2009 :

http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=36556

[199] http://www.wired.com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/

[200] http://www.nytimes.com/2010/01/13/world/asia/13beijing.html?pagewanted=all

[201] http://articles.timesofindia.indiatimes.com/2010-04-06/china/28132106_1_hacking-activities-chinese-hackers-china

- Octobre 2010 : découverte dans plusieurs machines utilisant un système de contrôle industriel fabriqué par Siemens du ver Stuxnet. Il infecte notamment l'ensemble des centrifugeuses du programme iranien tout en transmettant des données erronées aux opérateurs.

- Janvier 2011 : des pirates parviennent à obtenir plus de 200 000 « crédits carbone » européens pour une somme estimé à 4 millions de dollars. Pour ce faire, ils ont hameçonné des employés de nombreuses sociétés et utilisés leurs données personnelles pour émettre des faux au nom de six sociétés[202].

- Mars 2011 : plusieurs systèmes d'information appartenant à des ministères « économiques et financiers » sont infectés par un cheval de Troie d'origine inconnue. L'ANSSI indique que l'objectif de l'attaque aurait été de voler des données économiques concernant la France[203].

- Juin 2011 : le FMI fait l'objet d'une attaque de son réseau informatique rendu vraisemblablement possible par des vols d'identité réalisés au moyen d'opérations ciblées d'hameçonnage[204].

- Août 2011 : McAfee publie un rapport décrivant l'organisation d'un réseau d'espionnage global par la Chine. Celui-ci aurait permis de voler des données à plusieurs dizaines de gouvernements, d'entreprises et d'organisations internationales[205].

- Septembre 2011 : une attaque qui permet d'émettre plusieurs centaines de certificats de sécurité frauduleux pour des liaisons sécurisées frappe une entreprise néerlandaise de certification DigiNotar. L'opération aurait été conduite pour piéger des centaines de milliers d'utilisateurs d'internet et, en particulier, d'intercepter des messages électroniques de la messagerie de Google Gmail[206],

- Octobre 2011 : le système d'information permettant le fonctionnement de la flotte de drones américains est infecté par un *keylogger*, c'est-à-dire un programme permettant d'enregistrer les éléments tapés au clavier et de les envoyer à des machines distantes[207].

- Octobre 2011 : l'entreprise japonaise Mitsubishi Heavy indique que son réseau informatique a fait l'objet d'une attaque visant à obtenir des données sur ses projets de recherche et de développement. Des informations concernant la conception et la tenue aux tremblements de terre des centrales nucléaires de sa fabrication auraient notamment été volées[208].

---

[202] http://www.wired.com/threatlevel/2010/02/hackers-steal-carbon-credits#ixzz0eafFpvUR

[203] http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/attaque-informatique-contre-les-ministeres- economique-et-financier.html

[204] http://www.pcworld.com/article/230157/imf_hacked_no_end_in_sight_to_security_horror_shows.html

[205] http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

[206] http://www.lemonde.fr/technologies/article/2011/09/06/internet-nous-accordons-une-confiance-totale-aux-certificats-de-securite_1568541_651865.html

[207] http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

[208] Agence France Presse, "Japan cyber attackers may have military info", 24 October 2011.

➡ Novembre 2011 : Duqu, un cheval de Troie présentant de nombreuses similarités (lignes de code) avec Stuxnet, est découvert par une université de Budapest. Comme Stuxnet, il infecte essentiellement des systèmes d'exploitation de machines mais sa finalité est avant tout de rassembler des informations et de les transmettre vers des machines distantes[209]. Selon le quotidien israélien Haaretz, le virus aurait infecté de nombreuses machines iraniennes.

[209] http://www.computerworld.com/s/article/9221817/FAQ_What_s_the_big_deal_about_Duqu_?taxonomyId=17

Annexe 2
Bibliographie Sommaire

Travaux sur la dissuasion numérique ou sur l'exercice de la puissance numérique

Martin C. Libicki, « Cyberdeterrence and Cyberwarfare », RAND Project Air Force, RAND, 2009.

« Perspectives for Cyber Strategists on law for cyberwar », Charles J. Dunlap Jr., Major General, USAF, Retired, 2011.

Patrick Morgan, « Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm », National Academies of Science, Computer Science and Telecoms Board, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policies, 2010.

Eric Sterner, « Deterrence in Cyberspace: Yes, No, Maybe? », in Returning to Fundamentals: Deterrence and US National Security in the 21st Century, The George C. Marshall Institute, 2011.

Matthew D. Crosston, « How « Mutually Assured Debilitation » Is the Best Hope for Cyber Deterrence », Strategic Studies Quaterly, Spring 2011.

Eric Sterner, « Retaliatory Deterrence in Cyberspace », *Strategic Studies Quarterly*, Spring 2011.

Harry D. Raduege, « Fighting Weapons of Mass Disruption: Why America Needs a « Cyber Triad » », East-West Institute, Global Cyber Deterrence, April 2010.

Daniel T. Kuehl, « From cyberspace to cyberpower: Defining the problem », in Franklin D. Kramer, Stuart Starr & Larry K. Wentz, « Cyberpower and National Security (Washington, D.C.: National Defense UP, 2009).

Joseph S. Nye Jr, « CyberPower », Harvard Kennedy School, May 2010.

Stratégie en matière de cyber-espace et sécurité numérique.

« Défense et Sécurité Nationale – Le Livre Blanc », Ed. Odile Jacob, juin 2008.

« Défense et sécurité des systèmes d'information : La stratégie de la France », SGDSN, Février 2011.

The White House, « International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World », May 2011.

The White House, « The Cyberspace Policy Review », January 2009.

Center for New American Security, « America's Cyber Future: Security and Prosperity in the Information Age », June 2011.

Center for Strategic and International Studies, « Securing Cyberspace for the 44th Presidency », A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, December 2008.

GAO, « United States Faces Challenges in Addressing Global Cybersecurity and Governance », July 2010.

Center for New American Security, « America's Cyber Future: Security and Prosperity in the Information Age », Edited by Kirstin Lord & Travis Sharp, June 2011.

Programmes et travaux du Département de la Défense américain.

William Lynn III, « Defending a New Domain », *Foreign Affairs*, Sep/Oct2010, Vol. 89, Issue 5.

Alexandre Klimburg, « Mobilizing Cyber-Power », *Survival*, Volume 53, Issue 1, January 2011.

Department of Defense, « Department of Defense Strategy for Operating in Cyberspace », July 2011.

Karl Frederick Rauscher & Andrey Korotkov, « Working Towards Rules for Governing Cyber Conflict », East-West Institute, January 2011.

David Hollis, « USCYBERCOM: The Need for a Combatant Command versus a Subunified Command », National Defense University, Joint Force Quaterly, issue 58, 3rd Quarter 2010.

Government Accountability Office, « Defense Department Cyber Efforts », July 2011.

DARPA, « The National Cyber Range: A National Testbed for Critical Security Research ». Consulté à http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf

Julius Motal, « Pentagon to Prep for Battle Via 'National Cyber Range' », PCMag.com, June 20, 2011.

Développement de la menace dans le cyberespace.

Dmitri Alperovitch, « Revealed: Operation Shady RAT », McAfee, August 2011.

US Cyber Consequences Unit, « Overview of the Cybercampaign against Georgia in August of 2008 », August 2009.

Magnus Hjortdal, « China's Use of Cyber Warfare: Espionnage meets Strategic Deterrence », *Journal of Strategic Security*, Volume IV Issue 2 2011.

Thérèse Delpech, « La guerre informatique a commencé », *Politique Internationale*, N°130, Hiver 2010-2011.

Kim Zetter, « How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History », Wired, 11 July 2011.

Noah Schchtman, « Pirates of the ISPs: Tactics for Turning Online Crooks Into International Pariahs », Brookings China Center, Cyber Security #1, July 2011.

European Commission Staff Working Document, « Early Challenges regarding the « Internet of Things » », 29 septembre 2008.

David Bradshaw, « Western European Software-as-a-Service Forecast, 2009–2013 », Apr 2009 – Doc # LT02R9, 2009. Cité par l'*European Network and Information Security Agency*.

European Network and Information Security Agency, « Cloud Computing: Benefits, risks and recommendations for information security », November 2009.

Syntec Numérique, « Livre Blanc sur la sécurité du Cloud Computing : analyse des risques, réponses et bonnes pratiques », 2010.

Digimind, « White paper: Réputation internet », juin 2008, p. 5.