Focus stratégique n° 44

Cyberguerre

En quête d'une stratégie

Michel Baud

Mai 2013

ifri
Laboratoire
de Recherche
sur la Défense

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901).
Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale. Avec son antenne de Bruxelles (Ifri-Bruxelles), l'Ifri s'impose comme un des rares *think tanks* français à se positionner au cœur même du débat européen.

Les opinions exprimées dans ce texte n'engagent que la responsabilité de l'auteur.

ISBN : 978-2-36567-168-2

Ifri
27 rue de la Procession
75740 Paris Cedex 15 – FRANCE
Tel : +33 (0)1 40 61 60 00
Fax : +33 (0)1 40 61 60 60
Email : ifri@ifri.org

Ifri-Bruxelles
Rue Marie-Thérèse, 21
1000 – Bruxelles – BELGIQUE
Tel : +32 (0)2 238 51 10
Fax : +32 (0)2 238 51 15
Email : info.bruxelles@ifri.org

Site Internet : www.ifri.org

« Focus stratégique »

Les questions de sécurité exigent désormais une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection **« Focus stratégique »**, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, **« Focus stratégique »** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

L'auteur

Officier de l'armée de Terre, le chef de bataillon (TA) Michel Baud appartient à l'arme des transmissions. Diplômé de l'enseignement militaire supérieur, du Cours Supérieur d'Etat-Major ainsi que de l'Ecole de Guerre, il est détaché comme chercheur au sein du LRD de l'Ifri.

Comment citer cet article

Michel Baud, « Cyberguerre. En quête d'une stratégie », *Focus stratégique*, n° 44, mai 2013.

Sommaire

Résumé

Domaine complexe, le cyberespace a révolutionné la conduite de la guerre. Ce nouveau champ d'action désormais incontournable représente à la fois un défi et un avantage stratégique majeur, à l'heure où les technologies de l'information affectent l'ensemble des relations au niveau mondial. Les Etats dans leur ensemble se trouvent déstabilisés par une dépendance croissante à l'égard du numérique exposant leur appareil de défense à de nouvelles vulnérabilités. Sur cet enjeu crucial, aucune stratégie de coopération internationale claire n'a encore été élaborée. Pourtant, s'il représente un indéniable facteur d'accroissement du potentiel militaire, le « cyber » reste une menace en l'absence de réponses adaptées. Asymétrie des acteurs, diversité des cyber-armes, absence de frontières, les caractéristiques de cet espace doivent donc faire l'objet d'une analyse critique. Celle-ci devra interroger les concepts approximatifs de « cyber-guerre » et de « cyber-dissuasion », et redéfinir les termes d'une « cyber-stratégie » cohérente et assumée au niveau national. Seules l'instauration d'une doctrine crédible et la consolidation d'unités spécialisées permettront de conduire des opérations efficaces.

* * *

Cyberspace, as a major but intricate field of action, represents both a challenge and a great strategic advantage. At a time when information technology affects all relationships at a global level, states are destabilized by growing dependence on computer data which puts their militaries at risk. No clear international strategy has yet been developed to face this critical issue. Though it could significantly increase military potential, "cyber" remains however a threat without appropriate solutions. Asymmetric actors, the diversity of cyber-weapons as well as the lack of borders are the main features of this space that should be assessed. This cyber-expertise should clarify among others concepts such as “cyber-warfare” and “cyber-deterrence”, as well as create a proper “cyber-strategy” at the national level. Only by establishing a credible doctrine, hiring and retaining a specialized staff, states could conduct cyber-operations.

Introduction

En 2010, la centrale nucléaire iranienne de Natanz est touchée par le virus Stuxnet qui cible les centrifugeuses chargées d'enrichir l'uranium au profit du programme nucléaire iranien[1]. Restées sourdes aux protestations et aux mesures de rétorsion de la communauté internationale, les autorités iraniennes auraient pu alternativement faire l'objet d'un bombardement stratégique de leurs installations nucléaires, au risque d'entraîner cependant une confrontation régionale. En provoquant des dégâts considérables en toute discrétion, cette cyberattaque atteste de l'émergence de ce nouveau champ d'action qu'est le cyber.

Ce n'est pourtant pas le cyber en lui-même qui a métamorphosé la conduite de la guerre, mais bien la révolution des technologies de l'information et la numérisation de l'espace de bataille. La dépendance croissante des armées vis-à-vis des données informatiques a introduit de nouvelles vulnérabilités suscitant une véritable aubaine pour le cyberattaquant. En ce sens, ce domaine est incontournable parce qu'il peut considérablement accroître le potentiel militaire d'un Etat, en créant une rupture stratégique vis-à-vis de pays qui n'investiraient pas suffisamment ce champ d'action.

L'exemple iranien est particulièrement intéressant de par la réponse apportée par ce pays à cet événement. Peu après cette attaque, « le régime iranien a lourdement investi à la fois dans des capacités défensives et offensive dans le cyberespace[2]. Désormais, « l'Iran considère la cyberguerre, au même titre que d'autres tactiques asymétriques comme le terrorisme et la guérilla, comme un outil efficace pour infliger des pertes significatives sur le territoire de son ennemi… »[3]. En 2012, les Iraniens auraient ainsi financé un projet gouvernemental d'un milliard de dollars pour développer leurs capacités cyber par l'acquisition de nouvelles technologies, par la recherche d'une meilleure expertise en cyberdéfense et par la création d'un corps de cyber-experts. Militairement, cette volonté se traduit également par l'intégration de ce champ d'action dans les entraînements. Au cours d'une manœuvre navale dans le détroit d'Ormuz, le contre-amiral iranien Amir Rastgari, porte-parole militaire, apprend à la

[1] James P. Farwell et Rafal Rohozinski, « Stuxnet and the Future of Cyberwar », *Survival: Global Politics and Strategy*, vol. 53, n° 1, 2011, pp. 23-40.
[2] Ilan Berman, « The Iranian cyber threat to US homeland », *Pundicity Informed Opinion & Review*, 26 avril 2012, accessible à l'adresse : http://www.ilanberman.com/11611/the-iranian-cyber-threat-to-the-us-homeland.
[3] Gabi Siboni et Sami Kronenfeld, « Iran and Cyber Warfare », *Military and Strategic Affairs*, vol. 4, n° 3, décembre 2012, p. 79.

presse qu'une unité de cyberdéfense de la marine a « lancé une attaque contre le réseau informatique des forces défensives avec l'objectif d'infiltrer ce réseau pour y pirater des informations et y introduire des virus »[4].

De nombreux pays menacés par des cyberattaques tentent aujourd'hui de développer une réponse adaptée à ce nouveau défi. Mais définir une cyberstratégie n'est pas chose aisée. Tantôt considéré par certains comme un nouvel espace de liberté, tantôt comme un nouveau champ de bataille, le cyber est un domaine complexe qui remet en cause nombre de certitudes. Les difficultés d'attribution, l'asymétrie potentielle des acteurs, la fréquence des cyberattaques, leur diversité et leur instantanéité sont autant de facteurs qui altèrent profondément la réflexion stratégique.

Afin de bien saisir les enjeux auxquels sont confrontées les armées, il est indispensable de pouvoir analyser les différentes caractéristiques du cyberespace, de comprendre comment on est capable d'y intervenir. Les actions menées doivent répondre à des règles clairement définies comme à une stratégie d'ensemble. Enfin, cette « cyberstratégie » doit être mise en application via une doctrine et une organisation adaptées à la conduite d'opérations dans ce nouvel espace de bataille.

[4] « First-ever cyber drills planned », *Iran Daily*, 25 octobre 2012, p. 3.

L'enjeu cyber

De « l'Internet champ de bataille »[5] aux « cyber offensives »[6], le vocabulaire militaire semble être utilisé à outrance dans la presse pour décrire l'ensemble des menaces qui pèsent sur les réseaux informatiques, sur ce que l'on nomme le cyber. Même si la presse spécialisée parle de plus en plus de « militarisation du cyberespace », ce n'est pas pour autant que ce domaine relève dans son intégralité de la sphère militaire[7]. Il convient donc tout d'abord de délimiter ce nouvel espace de bataille. En se plaçant volontairement sur le haut du spectre, il faut mener un effort d'analyse du cyberespace pour savoir comment agir dans ce milieu conflictuel et comment discriminer les différents événements cyber.

Nature du cyberespace

La définition du cyberespace communément admise est celle d'un espace virtuel rassemblant la communauté des internautes et des ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs. L'émergence de ces nouvelles capacités s'associe logiquement à l'apparition d'un nouveau milieu générateur de tensions et même de conflits entre les différents acteurs, publics ou privés, qui l'investissent. Ce « milieu » a ceci de particulier qu'il traverse (ou est transverse à) tous les autres. Son domaine est relativement vaste, et si aujourd'hui tous les domaines deviennent peu ou prou cyber (cyber-guerre, cyber-attaque, cyber-crime…), il est important de différencier plusieurs niveaux d'analyse. Traditionnellement, on distingue trois niveaux dans les systèmes d'information[8].

Un premier niveau, appelé la couche physique, est constitué par le matériel et les infrastructures de réseau. Il comprend les ordinateurs, les routeurs, les serveurs, les câbles et fibres optiques, soit l'ensemble des moyens physiques qui permettent le déploiement des réseaux. Vulnérables

---

[5] Emmanuel Le Bohec, « Internet, champ de bataille des temps modernes ? », *Les Echos.fr*, 16 février 2012, accessible à l'adresse : http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221143516/internet-champ-bataille-temps-modernes.

[6] « Des milliers de clients d'EDF visés par une vague de faux emails », *Le Monde.fr*, 31 janvier 2013, accessible à l'adresse : http://www.lemonde.fr/technologies/article/2013/01/31/edf-cible-d-une-cyberattaque-d-ampleur_1825096_651865.html

[7] « Rapport Clusif: le cyberespace se « militarise » de plus en plus », *01.net*, 18 janvier 2013, accessible à l'adresse : http://www.01net.com/editorial/584645/rapport-clusif-le-cyberespace-se-militarise-de-plus-en-plus/.

[8] Bertrand Boyer, *Cyberstratégie l'art de la guerre numérique*, Paris, Nuvis, 2012, pp. 62-63.

aux attaques, ces installations peuvent cependant être protégées physiquement par des mesures de sécurité. C'est sans doute la couche dont la protection est la plus conventionnelle et la plus facilement réglementée, du fait de sa réalité matérielle et de sa présence physique sur un territoire soumis au droit. Les Etats sont aujourd'hui largement conscients des besoins de protection de ces infrastructures informatiques, en particulier au sein des Organismes d'Intérêt Vital (OIV). Comme le rappelle le Contre-amiral Arnaud Coustillière : « attaquer globalement un OIV, c'est peut-être très compliqué […] il faut bien prendre conscience de la logique du maillon faible »[9] ; de fait, la sécurité d'un réseau présente toujours une faille, plus ou moins difficilement identifiable, qui peut être exploitée lors d'une attaque.

Le second niveau est la couche logique. Ce sont les différents logiciels qui permettent d'exploiter les capacités physiques des réseaux, d'adresser des requêtes, d'obtenir des services et d'organiser le transfert des flux d'information. C'est en quelque sorte le niveau de mise en œuvre, à la jonction entre les deux autres et qui permet l'utilisation effective du cyberespace. Ce niveau peut être différencié en fonction du type de dialogue : celui lié au dialogue homme-machine, le codage, et celui lié au dialogue entre machines, le protocole[10]. C'est là que se concentre le plus grand nombre d'attaques informatiques.

Enfin, le dernier niveau est celui de la couche cognitive, encore appelée couche sémantique ou informationnelle. C'est la couche haute où se mêlent les perceptions de la réalité et les capacités de gestion de la connaissance[11]. Cette couche traite du contenu des informations dont il faut protéger l'intégrité.

Tout mode d'action dans le cyberespace agit au départ sur le second niveau, la couche logique, et peut avoir des répercussions sur les autres. Une attaque par déni de service qui vise la couche logique en saturant un serveur, et donc en le rendant inaccessible, aura un impact sur la couche cognitive. Le serveur qui en est victime se met hors service, ne peut plus répondre aux requêtes et mettre en ligne les informations disponibles. Un virus comme *Shamoon* utilisé lors des attaques contre l'entreprise pétrolière Saudi Aramco et le producteur qatarien de gaz RasGas à l'été 2012 s'est attaqué à la couche logique et a eu des répercussions sur la couche physique[12]. Après avoir copié les données des différents ordinateurs et les avoir envoyées, ce virus a réécrit le *Master Boot Record* (MBR : le secteur d'amorçage du disque dur), ce qui empêche par la suite tout redémarrage du disque dur[13]. Les trois couches

[9] Contre-Amiral Arnaud Coustillière, officier général à la cyberdéfense de l'état-major des armées, « Ministère de la défense : Opérer en sécurité dans le cyberespace », *Cybercercle défense & stratégie*, 24 octobre 2012.
[10] Olivier Kempf, *Introduction à la cyberstratégie*, Paris, Economica, 2012, p. 13.
[11] Bertrand Boyer, *op. cit.*, p. 63.
[12] Abdelghani Henni, « Middle East Attacks Raise Cyber Security Questions », *Journal of Petroleum Technology*, octobre 2012, pp. 68-69.
[13] Christopher Bronk et Eneken Tikk-Ringas, « The Cyber Attack on Saudi Aramco », *Survival: Global Politics and Strategy*, vol. 55, n° 2, avril 2013, pp. 81-96.

informationnelles du cyberespace sont donc intimement liées et interdépendantes les unes des autres. C'est sur la couche logique que l'action initiale se porte.

L'éventail des cyberarmes

Dans le cyberespace, plusieurs modes d'action sont envisageables. On parle désormais de cyberarmes. Certains pays comme les Etats-Unis développent un véritable arsenal, en partenariat avec des industriels comme General Dynamics et Lockheed Martin. Le but de cette collaboration est de constituer des cyberarmes pour assurer la défense des réseaux du département de la Défense, et attaquer d'autres réseaux sur la planète[14]. Il n'existe pas actuellement de définition d'une cyberarme reconnue au niveau international. On peut cependant relever la définition de Thomas Rid et Peter McBurney : « une cyberarme est vue comme un sous-ensemble d'armes et plus généralement : un code informatique qui est utilisé, ou conçu pour être utilisé, avec le but de menacer ou de causer des dommages physiques, fonctionnels ou psychologiques aux structures, systèmes ou organismes vivants »[15]. Dans cette définition, on retrouve une vision particulière de ce sujet, qui considère qu'une certaine forme de violence est indissociable des cyberarmes. Si tel devait être le cas, toutes les attaques informatiques ne pourraient être regardées comme ayant employé des cyberarmes, et l'exemple d'un virus comme *Win 32 Conficker* ne serait alors pas considéré comme une cyberarme, ce qui reste discutable[16]. Une autre définition de Kevin Coleman peut apporter un éclairage différent sur la nature de cet outil, en n'incluant pas nécessairement la notion de violence. La cyberarme serait une capacité destinée à perturber les systèmes informatiques et les réseaux. Cela inclut tout objet ou instrument qui peut causer des dommages à un ordinateur, à un réseau ou à un appareil électronique contenant des logiciels[17]. Plus simplement, dès lors qu'une arme peut être définie comme « un élément ou équipement complet servant à mettre un adversaire hors de combat »[18], une cyberarme pourrait être définie comme un élément logique (un code) servant à mettre le système d'information d'un adversaire, ou tout équipement qui en est doté (système d'arme, infrastructure critique) hors de combat.

Il est indispensable de distinguer ce qui est une cyberarme de ce qui ne l'est pas, même si la différence est subtile. De cette différenciation

---

[14] David Francis, « Pentagon Readies a Cyber Arsenal to Fight Attackers », *The Fiscal Times*, 18 février 2013, accessible à l'adresse : http://www.thefiscaltimes.com/Articles/2013/02/18/Pentagon-Readies-a-Cyber-Arsenal-to-Fight-Attackers.aspx#page1.

[15] Thomas Rid & Peter McBurney, « Cyber-Weapons", *The RUSI Journal*, vol. 157, n° 1, p. 7, accessible à l'adresse : http://www.tandfonline.com/doi/full/10.1080/03071847.2012.664354#tabModule.

[16] Début 2009, ce virus infecta un grand nombre d'ordinateurs dont ceux du ministère de la Défense français. Par mesure de sécurité certains avions restèrent cloués au sol, le temps que le virus soit éradiqué des ordinateurs qui devaient planifier les plans de vol. A aucun moment ce virus n'a eu de forme violente.

[17] Kevin Coleman, « Cyber warfare doctrine », *The Technolytics Institute*, Analysis, 1er juin 2008, p. 2.

[18] Trésor de la langue française informatisé, définition du mot « arme », accessible à l'adresse : http://atilf.atilf.fr/dendien/scripts/tlfiv5/advanced.exe?8;s=2590341255.

découle une réponse appropriée, qui n'est pas du même niveau en fonction de la gravité de l'attaque et qui évite l'écueil de l'automaticité d'une réponse disproportionnée. Pour Thomas Rid et Peter McBurney, délimiter cette frontière est important pour trois raisons. D'une part à cause de ses conséquences sur la sécurité – si un outil n'a pas le potentiel pour être utilisé comme une cyberarme, il est tout simplement moins dangereux. D'autre part parce que tracer une frontière a des conséquences politiques – une intrusion non armée est politiquement moins grave qu'une intrusion armée. Enfin parce que cette frontière a des conséquences légales : identifier une capacité comme un moyen armé doit, du moins en principe, placer sous le coup de la loi et donc rendre condamnable celui qui la développe, la possède ou l'utilise[19].

Trois composants sont nécessaires pour la conception d'une cyberarme offensive : un vecteur (page web, courriel, logiciel, programme, clé USB…), un composant capable de pénétrer un système informatique malgré la sécurité mise en place, et une charge utile, c'est-à-dire un code malveillant[20]. Par exemple, pour le logiciel espion *Flame*, le vecteur est la clé USB ou l'accès au réseau local, le composant pénétrant a utilisé une faille du système d'exploitation Windows, et la charge a permis de dérober et d'envoyer des informations, d'allumer le micro de l'ordinateur, d'utiliser le *bluetooth* pour scanner les appareils à proximité, d'effectuer des captures d'écran… On peut regrouper les types d'attaques dans le cyberespace dans les grandes catégories qui suivent.

Un premier type est l'attaque par déni de service (*Denial of Service* ; DOS). Cette attaque peut avoir lieu par saturation du serveur en envoyant un nombre de requêtes instantanées supérieur à ses capacités de traitement, ou par exploitation des vulnérabilités de ce même serveur. L'équipement est rapidement inaccessible et se met hors service. Plus récemment est apparue l'attaque par Déni de services distribués (*Distributed Denial of Service* ; DDOS). Ce mode d'action à peu près similaire utilise un plus grand nombre d'ordinateurs qui participent tous à la même attaque. On parle alors de *Botnets*, des réseaux de robots ou réseaux de machines « zombies », qui après avoir été infectés participent au DDOS, sans que leur propriétaire en soit nécessairement conscient.

Un deuxième mode d'action s'apparente à l'espionnage : les attaques par intrusion, ou attaques d'accès. L'objectif est d'accéder à une information protégée et confidentielle sans en avoir le droit. Plusieurs méthodes, utilisées seules ou de manière combinées, permettent de mener à bien cette attaque : tout d'abord par *sniffer*, ou renifleur de paquets, qui récupère des paquets de données qui circulent sur un réseau, puis par DPI[21] pour lire ces informations sensibles. Un autre mode d'intrusion est celui du logiciel espion, *spyware* ou *rootkit*, qui sont des programmes installés dans un ordinateur à l'insu de son propriétaire, et qui permettent

[19] Thomas Rid et Peter McBurney, *op. cit.*, p. 11.
[20] Kevin Coleman, « Cyber Warfare Doctrine », *The technolytics Institute*, 1er juin 2008, p. 2, accessible à l'adresse : http://www.docstoc.com/docs/21531063/Cyber-Warfare-Doctrine.
[21] DPI : Deep Packet Inspection, en français Inspection des Paquets en Profondeur.

de récupérer des données confidentielles. Il existe également des « chevaux de Troie », qui sont des programmes *a priori* anodins, capables de tromper les anti-virus et qui agissent par capture de données (mot de passe, coordonnées sécurisées, identifiants). Enfin, la *backdoor* ou porte dérobée est une fonctionnalité installée dans ou par un programme et qui permet à un individu d'accéder, en toute discrétion, à un ordinateur, à un serveur ou à un réseau sans que l'administrateur de celui-ci l'y ait autorisé. Cet accès peut permettre de prendre le contrôle total du système informatique. A la marge de cette catégorie, on trouve l'ingénierie sociale qui consiste non pas à s'attaquer à une éventuelle faille informatique, mais à exploiter les failles humaines, par abus de confiance et en profitant de la naïveté de l'utilisateur. On retrouve dans cette catégorie les attaques par *phishing* ou hameçonnage, dont le principe repose en général sur l'usurpation de l'identité d'une société pour obtenir de la victime des informations confidentielles (coordonnées bancaires…).

Existent également des attaques de modification, dont l'objectif est de modifier l'intégrité de l'information après avoir attaqué puis pénétré un système informatique. Plusieurs méthodes, utilisées seules ou combinées, permettent de mener à bien cette attaque, à commencer par les « virus » qui, en tant que programmes malveillants, ont besoin d'autres programmes dits « hôtes » pour se développer et se propager. Ils peuvent perturber gravement le fonctionnement du système sur lequel ils sont installés. Viennent ensuite les « vers », programmes autonomes qui peuvent détruire les informations classifiées, détourner des données ou entraîner des dysfonctionnements de l'ordinateur. Enfin, les « chevaux de Troie » peuvent, en plus de la capture de données, détruire des fichiers et déclencher des attaques ciblées.

En outre, et en dehors du domaine cyber au sens strict mais relevant en partie de la « guerre électronique », il faut encore citer les actions offensives visant la neutralisation physique de réseaux ou de moyens électroniques terminaux[22]. Dans ce domaine, de nouvelles armes spécialisées font leur apparition. C'est en particulier le cas du projet CHAMP : « Counter-electronics High-powered Microwave Advanced Missile Project » conduit par Boeing. Basé sur le principe de l'impulsion électromagnétique (IEM) neutralisant les équipements électroniques, un missile a été doté d'un canon à impulsion micro-ondes. Celui-ci est capable de créer une surtension dans les cibles électroniques et de les détruire[23].

Quel que soit le moyen d'attaque choisi, même s'il ne comporte pas à ce jour de capacité létale, certaines caractéristiques d'une arme demeurent, en ce sens qu'il s'agit bien de neutraliser des systèmes d'armes adverses (cf. *supra*). Il conserve également une dimension psychologique qui se traduit, pour la victime potentielle, par la crainte des risques encourus et l'incertitude quant à leur ampleur. Dans le cadre des

[22] Bertrand Boyer, *op. cit.*, p. 134.
[23] Pierluigi Paganini, « New weapons for cyber warfare. The CHAMP project », *blog Security Affairs*, 4 décembre 2012, accessible à l'adresse : http://securityaffairs.co/wordpress/10783/cyber-warfare-2/new-weapons-for-cyber-warfare-the-champ-project.html>.

cyberarmes, cette notion est constamment présente[24]. Cette dimension peut être renforcée si la cyberarme est utilisée comme une menace, c'est-à-dire lorsque son utilisation est annoncée et anticipée. La cible prend alors pleinement conscience du danger que représente cette arme et de sa capacité de destruction ou de nuisance.

Evaluer l'impact des cyberarmes

En 2013, lors de son audition par la Commission de la Défense nationale et des forces armées, le préfet Ange Mancini, coordonnateur national du renseignement, interrogé sur le domaine cyber déclare que « les cyberattaques doivent […] être considérées comme des actes de guerre »[25]. En suivant cette logique, en cas d'acte de guerre, il peut y avoir une riposte militaire proportionnée, contre un ennemi identifié, pour faire cesser l'agression. Toutefois, une riposte armée serait dans certains cas difficilement justifiable tant il est, à l'heure actuelle, difficile de mesurer précisément la gravité des cyberattaques et donc la proportionnalité de la réponse à adopter. En tout cas, aucune base officielle et internationale ne permet de les différencier. Il semble donc nécessaire de poser les bases d'une échelle mesurant la gravité des attaques informatiques, un peu à l'image de l'échelle internationale des événements nucléaires (*International Nuclear Event Scale,* INES) qui permet de mesurer la gravité des incidents ou accidents nucléaires. Cette échelle des événements cyber ne va pas catégoriser l'attaquant comme pour le classement du CSS de Zurich[26], elle ne va pas non plus s'attacher à différencier exclusivement les cyberattaques en fonction du mode d'action retenu mais elle va plutôt se focaliser sur les conséquences de l'attaque. Elle pourrait ainsi servir de base à une stratégie de riposte graduée.

Cette échelle doit tenir compte de la nature de la cible attaquée ; une attaque visant un OIV n'aura pas la même importance qu'une autre, identique, ciblant une petite entreprise. Le niveau de gravité retenu est donc lié au type de cible visée. La criticité de l'attaque sur les réseaux doit aussi être évaluée, en particulier concernant leur résilience et le temps nécessaire à l'organisme attaqué pour revenir à une situation de fonctionnement normale. Enfin, cette échelle doit prendre en compte la nature de la cyberattaque : de l'intrusion dans un réseau informatique, du vol de données, de la prise de contrôle d'un réseau, de la destruction dans le 1er ou le 3ème niveau…

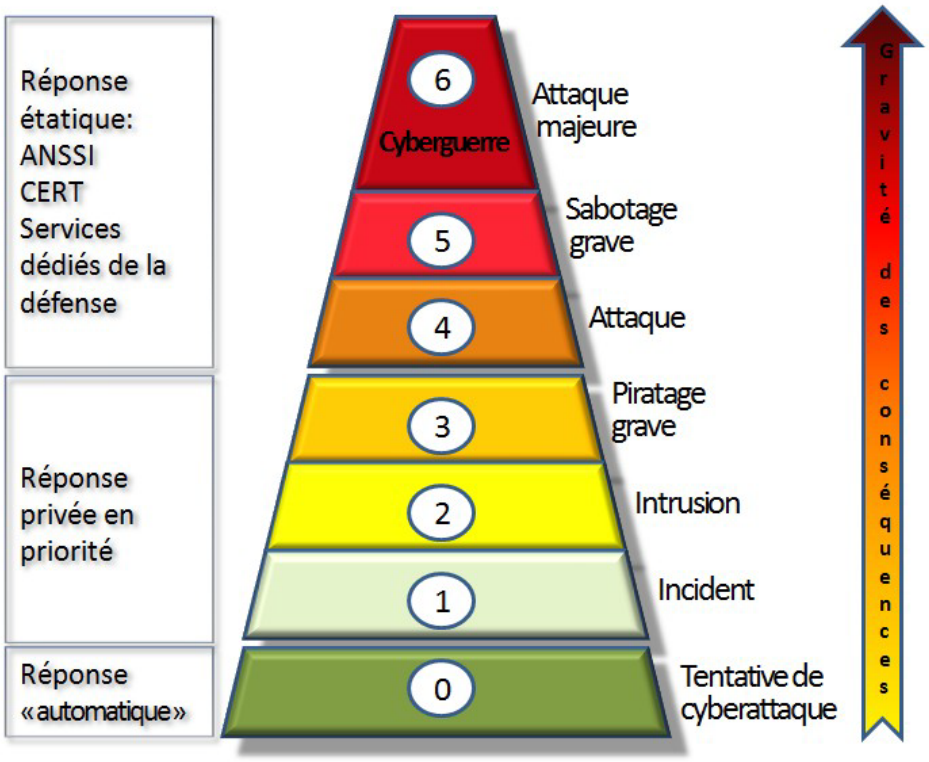
---

[24] Thomas Rid et Peter McBurney, *op. cit.*, p. 7.

[25] Commission de la défense nationale et des forces armées, *Audition de M. le préfet Ange Mancini, Coordonnateur national du renseignement*, 5 février 2013, p. 7, accessible à l'adresse : http://www.assemblee-nationale.fr/14/pdf/cr-cdef/12-13/c1213047.pdf.

[26] Le *Center for Security Studies* de Zurich a classé les cyberattaques par ordre croissant de gravité entre cybervandalisme, cybercrime, cyberespionnage, cyberterrorisme et cyberguerre. Cf. Myriam Dunn Cavelty, « Cyberwar: Concept, status quo, and limitations », *CSS Analysis in Security Policy*, n° 71, avril 2010, accessible à l'adresse : http://www.academia.edu/1058235/Cyberwar_Concept_Status_Quo_and_Limitations.

Figure 1 : Echelle des événements cyber[27]



Les événements cyber sont analysés en fonction de leurs conséquences sur le fonctionnement du cyberespace. Les niveaux sont classés en trois catégories : le niveau 0 ou la réponse face à une cyberattaque est « automatique », c'est-à-dire que les anti-virus et « firewall » installés sur la cible sont suffisants pour déjouer l'attaque. Aux niveaux 1, 2 et 3, la réponse doit être en priorité celle des administrateurs du réseau attaqué, ou éventuellement celui d'une société privée spécialisée en sécurité informatique. Enfin les niveaux 4, 5 et 6 justifient une réponse étatique au travers de l'action de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), des centres d'alerte et de réaction aux attaques informatiques (CERT : *Computer Emergency Response Teams*) ou des services dédiés du ministère de la Défense.

- Le niveau 0 est celui d'une tentative de cyberattaque qui a été repoussée par des moyens nominaux, elle est sans conséquence pour la cible. Ce peut être par exemple l'envoi du courriel avec une pièce jointe infectée qui est détectée et stoppée par l'antivirus installé sur l'ordinateur de la « cible ».

- Le niveau 1 est celui de l'incident informatique de nature mineure mais qui nécessite quand même une réponse appropriée pour revenir à une situation normale. Il peut s'agir d'un virus qui s'installe sur un ordinateur, et qui réclame l'intervention d'un spécialiste pour être supprimé du système.

[27] Ce schéma n'est qu'une proposition et ne représente que les vues de l'auteur.

- Le niveau 2 est celui de **l'intrusion** sur un réseau informatique, sur un serveur. L'objectif peut être de voler des données ou d'analyser le système et ses failles. Cette action permet éventuellement d'en connaître les défaillances pour une attaque future.

- Le niveau 3 est celui du **piratage grave**, il s'agit d'actions de corruption d'un système informatique ou d'un serveur, pour le reprogrammer et en modifier le fonctionnement normal. Il concerne aussi la falsification des données contenues dans les serveurs.

Si, dans les quatre premiers niveaux, la nature des cibles est de peu d'importance, pour les trois derniers, en revanche, l'Etat ou les OIV sont les cibles prioritaires, avec là aussi gradation des modes d'action cyber et de leurs conséquences.

- Le niveau 4 est celui de **l'attaque**. Ce peut être une attaque indirecte cherchant à pénétrer un réseau étatique, mais ce peut être aussi une attaque perturbant le fonctionnement d'un OIV. Cette attaque peut s'accompagner de la destruction de données contenues dans le système informatique.

- Le niveau 5 est celui du **sabotage grave**. Cette action paralyse un OIV, ou perturbe le fonctionnement des systèmes étatiques. Le virus Shamoon est un bon exemple, il a paralysé pendant plusieurs jours les entreprises RasGas et Saudi Aramco, entreprises de production énergétique dont le fonctionnement est vital pour n'importe quel Etat.

- Enfin, le niveau 6 est le niveau de gravité le plus élevé. L'**attaque majeure** a pour but de paralyser un système relevant de la souveraineté de l'Etat, voire l'ensemble du système étatique, en particulier dans le domaine de la défense ou de la sécurité. L'attaque, qui a duré trois semaines, dont a été victime l'Estonie en 2007 préfigure ce que pourrait être une attaque majeure : le gouvernement et la société de ce pays ont été totalement paralysés pendant plusieurs jours[28].

En somme, toute cyberattaque ne doit pas forcément être considérée comme un acte de guerre, et dans ce cadre « l'échelle des événements cyber » permet d'apporter une distinction claire en discriminant les attaques en fonction de la gravité de leur résultat. La diversité des modes d'actions envisageables dans le cyberespace permet d'entrevoir comment mettre en œuvre ces opérations. Pour être pleinement efficaces, elles doivent cependant s'inscrire dans le cadre d'une stratégie plus générale.

[28] Aaron Mannes et James Hendler, « The first modern cyberwarfare? », *The Guardian,* 22 août 2008, accessible à l'adresse : http://www.guardian.co.uk/commentisfree/2008/aug/22/russia.georgia1.

En quête d'une cyberstratégie

Lors des prémices de l'aviation militaire au début de la Première Guerre mondiale, l'idée est très vite apparue que l'Air allait devenir un nouveau domaine de conflictualité dans lequel il serait possible d'agir, d'effectuer des observations, de combattre ou de bombarder l'ennemi. En septembre 1914, les avions de reconnaissance français jouent déjà un rôle clé dans la bataille de la Marne, en détectant le mouvement tournant de l'armée allemande au nord-est de Paris, autorisant de la sorte la contre attaque franco-britannique de flanc[29]. Par la suite, l'Air est aussi devenu un domaine permettant d'atteindre d'autres espaces dans la profondeur stratégique, par le bombardement. Prenant en compte cette nouvelle dimension, une stratégie spécifiquement aérienne a progressivement émergé sous la plume d'officiers comme Douhet, Castex ou Gallois.

Près d'un siècle plus tard, une situation comparable propulse le cyber au rang de nouveau domaine de conflictualité qui offre l'opportunité d'agir sur d'autres milieux. C'est un champ original de réflexion pour les stratèges, qui a besoin de nouvelles règles et d'une nouvelle stratégie. Si la stratégie est l'art de combiner l'action de forces militaires en vue d'atteindre un but de guerre déterminé par le pouvoir politique, la « cyberstratégie » n'est alors rien d'autre que l'art de combiner les moyens cybernétiques afin de concourir à ce même but.

En s'intéressant au bouleversement provoqué par l'émergence des cyberarmes, on peut essayer d'analyser les rapports de force, le spectre des menaces et l'échelle d'intensité au sein du cyberespace, en distinguant en particulier ce qui relève de la sécurité nationale et de moyens étatiques et même militaires, et ce qui n'en relève pas. Pour autant, la « cyberguerre » demeure une notion hautement problématique, très éloignée de l'idée classique de guerre, et dépourvue de réelle autonomie ; à un niveau strictement militaire, il s'agit surtout d'adjoindre une dimension cyber à des opérations planifiées dans d'autres domaines. Le conflit dans le cyberespace est ainsi faussement banalisé par le terme de « cyberguerre », et il semble donc préférable de parler de cyberopérations. De même la comparaison avec la stratégie nucléaire fait-elle apparaître toute la difficulté d'une « cyberdissuasion » éventuelle. Parce qu'elle constitue un domaine original, par rapport auquel analogies et précédents sont nécessairement partiels et imparfaits, la cyberstratégie doit être pensée selon ses propres termes. Apparaissent alors quelques spécificités de ce domaine stratégique et en particulier le fait que les dimensions défensive et offensive ne peuvent y être qu'artificiellement séparées ; en

[29] John Andreas Olsen, *A History of Air Warfare*, Dulles, Potomac Books, 2010, p. 6.

cyberstratégie plus qu'ailleurs, l'attaque et la défense forment en effet deux aspects complémentaires et indissociables de l'action.

Qu'est ce que la cyberguerre ?

Les risques dans le cyberespace ne sont pas tous du même niveau et peuvent avoir des répercussions de nature totalement différente. Il peut s'agir par exemple du « défacement » d'un site web, action qui vise à modifier la page d'accueil d'un site Internet en modifiant son contenu – une action relevant davantage de la propagande et de la guerre de l'information. La Géorgie en est victime en 2008 lors de la guerre contre la Russie à propos de l'Ossétie du Sud. Le site du parlement est « défacé » et la page d'accueil est remplacée par un montage photo où le président géorgien, Mikheil Saakachvili, est comparé à Hitler. Pourtant, les conséquences d'attaques informatiques peuvent être beaucoup plus graves et avoir des répercussions sur l'utilisation de matériels militaires. Début 2009, le vers *Win 32 Conficker* infecte certains réseaux dont ceux des ministères de la défense américain, britannique et français. Il se propage sur certains ordinateurs ayant pour tâche de préparer les plans de vol des Rafales de la Force d'Action Navale. Même si le vers ne cible pas spécifiquement ces avions, ceux-ci restent cloués au sol deux jours durant, par mesure de sécurité[30].

Les attaques informatiques sont donc d'une extrême variété et toutes ne justifient pas une réponse militaire. Dans cette logique, la cyberguerre est, clairement, le type d'attaque le plus grave qui mette en jeu la sécurité d'un Etat ou ses intérêts fondamentaux. Ce type de menace justifie une réponse étatique adaptée. Le domaine de la cyberguerre est donc un domaine régalien, où s'affrontent les volontés de domination entre Etats, où chacun a sa propre conception du cyberespace et des intérêts qu'il entend protéger.

En octobre 2011, Thomas Rid publiait « *Cyber war will not take place* »[31], un article qui a eu un certain écho dans les milieux du cyber, et qui démontre que jusqu'à présent aucune cyberguerre ne s'est produite, et qu'il est fort peu probable que cela arrive dans le futur. Sa thèse s'inspire de l'idée développée par Clausewitz selon laquelle chaque partie « utilise la force physique pour obliger l'autre à se soumettre à sa volonté […] La guerre est donc un acte de violence dont l'objet est de contraindre l'adversaire à se plier à notre volonté »[32]. Or, actuellement, les cyberopérations ne se caractérisent pas par un usage de la force, déterminé et politique. Cependant, cette thèse ne peut remettre en cause la réalité des affrontements dans le cyber, ni la possibilité, à terme, de les voir déboucher sur des conséquences physiques pour les individus.

---

[30] « Les armées attaquées par un virus informatique », blog Secret Défense, 5 février 2009, accessible à l'adresse : http://secretdefense.blogs.liberation.fr/defense/2009/02/les-armes-attaq.html.

[31] Thomas Rid, « Cyber war will not take place », *Journal of Strategic Studies,* vol. 35, n° 1, février 2011, pp. 5-32.

[32] Carl Von Clausewitz, *De la guerre*, Paris, Perrin, 2006, p. 37.

Pour le Département de la Défense américain, la cyberguerre est définie comme « un conflit armé conduit totalement ou partiellement par des moyens cyber, [c'est à dire] des opérations militaires menées pour interdire à l'ennemi l'utilisation efficace des systèmes du cyberespace et des armes au cours d'un conflit. Cela inclut les cyberattaques, la cyberdéfense et les actions cyber »[33]. En 2010, un rapport définit la cyberguerre comme « un conflit entre Etats, mais qui peut aussi engager des acteurs non étatiques de plusieurs manières. Dans la cyberguerre, il est extrêmement difficile d'avoir une force ciblée et proportionnée ; la cible peut être militaire, industrielle ou civile, mais elle peut aussi être le local d'un serveur qui héberge de nombreux clients, dont un seul est la cible visée »[34]. La « cyberguerre » est donc un ensemble d'opérations coordonnées menées dans le cyberespace, avec des objectifs définis, au moyen de systèmes d'information et de communication. La « cyberguerre » stratégiquement autonome n'a donc pas de réalité, cette notion traduit un ensemble d'opérations menées dans le cyberespace. Ces opérations ont vocation à s'intégrer dans un plan d'action plus large qui peut s'inscrire dans la conduite d'un conflit, où le cyber n'est que l'une des composantes. En tant qu'opération spécifique, la « cyberguerre » n'intègre donc pas directement des notions de violence, de destructions physiques ou de morts, mais peut y participer.

Pourquoi il ne peut y avoir de cyberdissuasion

Aux Etats-Unis, le *Defense Science Board*, un organisme indépendant, a recommandé la création d'une unité militaire capable de contrer une attaque majeure dans le cyberespace. Au côté des outils traditionnels (forces nucléaires, forces armées conventionnelles, etc…), cette nouvelle unité offrirait au pouvoir politique un nouvel instrument dans sa stratégie de dissuasion globale[35]. En fonction des cyberopérations envisagées, on peut imaginer le développement d'une stratégie dissuasive, dont l'objectif serait d'intimider tout Etat cherchant à s'en prendre aux intérêts numériques de la France. Un peu à l'image de la dissuasion nucléaire, un discours des autorités publiques pourrait, au-delà des capacités défensives déjà connues, révéler l'existence de capacités offensives opérationnelles, et assumer leur emploi éventuel. En cas d'attaque de nos intérêts stratégiques (sabotage grave ou attaque majeure dans l'échelle des événements cyber), il y aurait automaticité d'une réponse cyber qui s'attaquerait à l'une des trois couches du système informatique ennemi pour le neutraliser durablement. Dans de telles opérations de représailles, la partie offensive devrait nécessairement comprendre un volet défensif afin que le niveau technique et l'investissement financier requis soient disproportionnés par rapport au bénéfice envisageable et dissuadent ainsi l'ennemi de toute escalade.

---

[33] Department of Defense, *Joint terminology for cyberspace operations,* accessible à l'adresse : http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

[34] Paul Cornish, David Livingstone, Dave Clemente et Claire Yorke, « On Cyber Warfare », *A Chatham House Report*, novembre 2010, p. 37, accessible à l'adresse : http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf.

[35] Yousaf Butt, « Rabid Response », *Foreign Policy*, 22 mars 2013, accessible à l'adresse : http://www.foreignpolicy.com/articles/2013/03/22/rabid_response?wp_login_redirect=0.

Il importe que ces représailles soient symétriques et proportionnelles. Les caractéristiques de cette réponse n'empêchent pas l'éventuelle utilisation de moyens non cybernétiques, à condition que l'ennemi soit connu. L'identification de l'attaquant revêt donc une importance toute particulière, une riposte ne pouvant pas être de même nature s'il s'agit d'un Etat, d'un groupe ou d'un individu.

Cette stratégie de dissuasion, dans un cadre symétrique, pourrait s'appuyer sur le concept stratégique de l'OTAN, le MC 14/3 de 1968. Ce document présente trois niveaux de riposte : la défense directe au niveau choisi par l'adversaire, l'escalade délibérée et la riposte massive. « En d'autres termes, il s'agirait pour un Etat 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 le droit, 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 (*sic*) d'emblée des dommages majeurs à l'adversaire » [36].

Dans les faits, cependant, et comme le rappelle Martin C. Libicki, « les ambiguïtés de la cyberdissuasion contrastent durement avec la clarté de la dissuasion nucléaire »[37]. Tout d'abord, en termes de fréquence d'utilisation, si l'arme nucléaire n'a pas été utilisée dans le cadre d'un conflit au cours de ces 60 dernières années, les cyberattaques sont, quant à elles, quotidiennes. Au Royaume-Uni par exemple, il y aurait plus de 120 000 attaques par jour[38]. Le « tabou » nucléaire consubstantiel à la dissuasion ne s'applique donc absolument pas dans le cadre des cyberattaques.

D'autre part, les dommages physiques et matériels provoqués par une explosion nucléaire sont largement prévisibles. La puissance de l'arme atomique permet de connaître assez précisément l'ampleur des destructions. De ces informations, on peut par exemple déduire la zone immédiatement contaminée par les retombées nucléaires. Dans le cadre d'une cyberattaque, ces dégâts sont beaucoup plus difficilement prévisibles. Les risques de dommages collatéraux ne peuvent pas être exclus, le mode de transmission d'une cyberarme s'apparentant davantage à la guerre biologique qu'au nucléaire. De plus, lors d'une cyberattaque, après une phase initiale qui paralyse l'attaqué, il est difficile de connaître ses capacités de résilience, et donc au final les dommages durables réellement causés. Enfin, et si dans le domaine nucléaire les « essais » ont valeur de démonstration, dans le cyber, ils sont synonymes de révélation et rendent improbable toute utilisation ultérieure de la cyberarme.

---

[36] Bruno Gruselle, Bruno Tertrais, et Alain Esterle, « Cyberdissuasion », *Recherches & documents*, Fondation pour la Recherche Stratégique, n° 3, 2012, p. 53.

[37] Martin C. Libicki, *Cyberdeterrence and cyberwar*, Pittsburgh, RAND Corporation, 2009, p. 16.

[38] Brian Fung, « How Many Cyberattacks Hit the United States Last Year? », *National Journal*, 8 mars 2013, accessible à l'adresse : http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/?oref=ng-dropdown.

Se pose également le problème de l'attribution : lors de la Guerre Froide, l'origine d'une attaque atomique ne faisait aucun doute et le droit à la riposte ne pouvait donc être contesté. Dans le cadre du cyber, les difficultés rencontrées par les spécialistes pour identifier avec certitude l'auteur d'une attaque ne permettent pas, pour le moment, une riposte immédiate, ce qui décrédibilise une stratégie de cyberdissuasion. C'est le problème de l'attribution de l'attaque.

Au final, la dissuasion nucléaire est généralement pensée dans un cadre symétrique opposant deux Etats, étant donné que le coût de développement et de possession de telles armes les réserve à un nombre restreint d'Etats. Dans une « cyberguerre », ce cadre vole en éclats. L'Etat est confronté à un attaquant, mais aussi éventuellement à une troisième entité via des sociétés de cybersécurité qui peuvent jouer un rôle actif, un peu à l'image des sociétés militaires privées dont le rôle est de plus en plus significatif dans certains conflits modernes. L'ennemi n'est pas forcément étatique, il peut être irrégulier (groupe de hackers, mouvement terroriste…). Il ne respecte pas le droit de la guerre, il peut, par exemple, attaquer et paralyser les réseaux informatiques d'un hôpital. L'Etat concerné est déstabilisé par cette asymétrie, et de nouveau le concept de « cyberdissuasion » ne s'applique qu'imparfaitement.

La dissuasion n'est donc pas le modèle le plus approprié pour aborder la stratégie dans le cyberespace, ou du moins doit-il être appliqué de manière originale et distincte de ce qui se fait dans le nucléaire. Cette dissuasion doit s'appuyer sur des capacités de défense, d'attaque et d'attribution. Le défensif est largement développé en France, actuellement, par des agences spécialisées comme l'ANSSI ou par des structures militaires ou privées. L'offensif reste quant à lui plus confidentiel et pourrait voir son rôle évoluer à l'avenir. Enfin, l'attribution de l'attaque reste un véritable écueil, en raison à la fois de sa difficulté intrinsèque et de ses délais de réalisation.

De la continuité « défensif-offensif »

« Sera maître du monde, celui qui sera maître de l'Air » prédisait Clément Ader au tout début de l'aviation[39]. De fait, la puissance aérienne ou *Airpower* a joué un rôle souvent central dans des opérations des vingt dernières années, de la guerre du Golfe en 1991 jusqu'à l'Irak en 2003, l'Afghanistan ou encore la Libye[40]. Or, tous les spécialistes s'accordent à penser depuis Douhet que l'obtention de la supériorité aérienne constitue le premier principe de la stratégie dans la troisième dimension. Sans ce préalable décisif, en effet, l'aviation non seulement ne peut pas produire des effets stratégiques et tactiques à l'encontre des centres de commandement et des forces ennemies, mais encore est incapable de protéger de l'aviation adverse les forces terrestres amies ou même ses propres bases. Ainsi, dans les opérations aériennes, les aspects défensifs

[39] Etienne de Durand et Bastien Irondelle, « Stratégie aérienne comparée: France, États-Unis, Royaume-Uni », *Centre d'études en sciences sociales de la défense*, 2006, p. 10.
[40] Etienne de Durand, « Le renouveau de la puissance aérienne », *Hérodote*, n° 114, 2004, pp. 17-34.

et offensifs sont-ils intimement mêlés : se défendre efficacement suppose de conquérir et de maintenir la supériorité aérienne, donc d'initier d'emblée des actions offensives. Si le cyber prend aujourd'hui une place de plus en plus importante, il est légitime de se demander s'il n'est pas appelé, à son tour, à dominer les autres éléments, terrestre, maritime et aérien, et si la maîtrise du cyberespace ne va pas un jour représenter un préalable obligé.

Pour des raisons politiques évidentes, la tendance actuelle veut opposer le défensif à l'offensif, comme s'il y avait d'un côté une utilisation défensive et donc vertueuse du cyber, cherchant à préserver les réseaux des actes malveillants, et de l'autre la dimension offensive, nécessairement illégitime et fauteuse de guerre – pour mémoire, le ministère de la Défense français s'appelait autrefois le ministère de la Guerre. En extrapolant un peu, on peut donc envisager qu'à terme ceux qui sont chargés de cyberdéfense soient en réalité responsables à la fois des aspects défensifs et offensifs du cyber. Fonder la cyberstratégie uniquement sur une approche défensive est risqué, comme le rappelle Daniel Ventre : « penser la sécurité sur le thème de la forteresse, c'est retourner à des principes du Moyen Age, ou de l'époque de Vauban. Ce n'est peut-être pas le modèle le mieux adapté à la sécurité du XXI^{e} siècle »[41].

Longtemps, la dimension offensive a été officiellement rejetée par les pays occidentaux, et ce pour plusieurs raisons. Mener des cyberattaques révèle aux autres acteurs le niveau de technicité que l'on a soi-même atteint, ce que l'on ne souhaite pas divulguer. Ce type d'attaques peut être mal perçu par les opinions publiques, mais plus encore par les gouvernements tiers. Enfin, les risques de dommages collatéraux ne peuvent être écartés, et à partir d'une cible purement militaire à l'origine, les victimes peuvent par ricochet être civiles[42].

Dans son rapport d'information sur la cyberdéfense, le sénateur Bockel rappelle que la menace provenant des attaques informatiques n'est toujours pas suffisamment prise en compte[43]. Comme l'indique son titre, *Défense et sécurité des systèmes d'information,* la stratégie de la France ne se concentre officiellement que sur le volet défensif : « le gouvernement a décidé de renforcer significativement les capacités nationales en matière de cyberdéfense »[44]. On est là bien loin de la doctrine officielle américaine intitulée *Strategy for Operating in Cyberspace* de juillet 2011 dans laquelle on peut lire : « Le Département de la Défense doit s'assurer d'avoir les capacités nécessaires pour opérer efficacement dans tous les domaines – Air, Terre, Mer, Espace et cyberespace »[45]. Pour les Etats-Unis, la menace cyber est officiellement pensée dans son intégralité, tant sur le plan défensif que sur le plan offensif. La donne est ainsi en train de changer : le président Obama et la Maison blanche disposent désormais de larges pouvoirs pour mener non seulement des représailles, mais également des

[41] Daniel Ventre, *Cyberattaque et cyberdéfense*, Paris, Lavoisier, 2011, p. 294.
[42] Michel Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, 2:2012, p. 314.
[43] Jean-Marie Bockel, *op. cit.*, p. 80.
[44] Stratégie de la France, *op. cit.*, p. 7.
[45] Department of defense, *Strategy for operating in cyberspace*, p. 5, accessible à l'adresse : http://www.defense.gov/news/d20110714cyber.pdf.

frappes préemptives, par cyberattaques, sur des cibles étrangères. Cette riposte aura lieu si les Américains ont une preuve tangible de risque d'une cyberattaque d'envergure contre leurs intérêts stratégiques, cyberattaque menée par une puissance étrangère[46].

A l'image de la stratégie aujourd'hui adoptée par les Américains et les Israéliens, fondée à la fois sur de robustes capacités défensives et sur le développement de capacités offensives, il semble que la frontière entre le défensif et l'offensif devienne de plus en plus ténue. La principale raison est de nature technique : développer une cyberdéfense efficiente implique de s'intéresser aux techniques développées par les cyberattaquants et peut conduire à l'utilisation de capacités offensives, ne serait-ce que pour identifier l'attaquant qui se cache derrière un *botnet* (capacités offensives dont la France se prive aujourd'hui). Actuellement, il est en effet très difficile d'attribuer les attaques, les techniques qui le permettent faisant appel à des moyens d'investigation offensifs, apparentés à des cyberarmes, et considérés par nombre de pays, dont la France, comme illégaux. D'autre part, développer des cyberarmes nécessite d'analyser les failles potentielles de la cyberdéfense d'un réseau. Cette recherche mène naturellement à renforcer sa propre sécurité, c'est donc un bon moyen d'accroître la résilience de ses systèmes informatiques. En fait, « le point de vue offensif est le seul qui permette de voir la réalité en face et de produire une défense efficace »[47]. Un peu à l'image du matériel militaire qui équipe les armées, pour avoir des capacités défensives crédibles, il faut posséder des moyens offensifs qui le sont tout autant.

Ainsi l'aspect offensif du cyber est-il de moins en moins tabou. Au départ chasse gardée des services spéciaux ou de la nébuleuse des hackers, la recherche dans ce domaine est de plus en plus assurée par des acteurs privés à des fins lucratives. Aux Etats-Unis, l'industrie de défense exploite déjà le créneau. Les sociétés Raytheon et Northrop Group ont ouvert des départements de « sécurité informatique offensive »[48]. En Europe, des sociétés comme l'anglo-allemande Gamma Group développe le logiciel espion *Finisher*, tandis que la société italienne Hacking Team met au point un logiciel de hacking pour les interceptions gouvernementales. En France même, la société Vupen développe des outils de « sécurité offensive »[49]. Le développement de ces aspects offensifs pourrait déboucher sur une forme de course aux armements informatiques.

---

[46] David E. Sanger et Tom Shanker, « Broad powers seen for Obama in cyberstrikes », *The New York Times*, 3 février 2013, accessible à l'adresse : http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=1&.

[47] Éric Filiol, « L'«affaire» Vupen où quand la compétence française fait peur aux États Unis », *Les Echos.fr*, 6 février 2013, accessible à l'adresse : http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221164714/affaire-vupen-quand-competence-francaise-fai.

[48] Yves Eudes, « Hackers d'Etat », *Le Monde*, 19 février 2013, accessible à l'adresse : http://www.lemonde.fr/technologies/article/2013/02/19/hackers-d-etat_1834943_651865.html.

[49] Site Internet Vupen / accessible à l'adresse : http://www.vupen.com/english/services/lea-index.php.

En définitive, le développement de la « cyberguerre » est né de la vulnérabilité nouvelle induite par la numérisation des Armées. Si, face à ces risques, deux approches sont à permière vue possibles, l'une défensive, l'autre offensive, l'avantage semble privilégier l'attaquant. Surtout, la nature des cyberopérations et la nécessité de l'identification à des fins de dissuasion interdisent de se limiter à la seule dimension défensive. En outre, et si le cyber fait partie du cœur de souveraineté de l'Etat, au même titre que le nucléaire[50], l'analogie entre les deux domaines ne doit pas être poussée trop loin. La gravité d'éventuelles frappes nucléaires comme l'identification incontestable de l'agresseur expliquent ainsi que le « jour d'après » n'ait pas été sérieusement envisagé, et que la peur de l'holocauste ait suscité entre grandes puissances une retenue certaine, confinant parfois à la paralysie. Le domaine cyber introduit ainsi une véritable révolution à un autre niveau : un Etat peut de nouveau mener des opérations clandestines d'envergure, dans le cyberespace, sans crainte de les revendiquer. La cyberstratégie apparaît ainsi très clairement comme une stratégie d'emploi, et il est donc indispensable d'analyser la manière dont elle peut être mise en œuvre.

[50] Entretien avec le Lieutenant-colonel Patrice Tromparent, Délégation aux Affaires Stratégiques, lundi 15 avril 2013.

Les armées face au défi cybernétique

Définir une stratégie cyber est essentiel pour coordonner l'action des forces en vue de la défense de nos intérêts dans ce domaine. Si l'élaboration de cette stratégie prend progressivement forme grâce à la multiplication de travaux de recherche, son application est confrontée à de nombreuses difficultés[51]. Différentes initiatives mondiales ou régionales n'apportent pas une réponse totalement satisfaisante, et il semble que la seule approche valable reste avant tout nationale. On peut ainsi étudier l'exemple américain du Cyber Command pour comprendre comment les Etats-Unis ont élaboré une doctrine pour la conduite des cyberopérations. En France aussi, une filière cyber est actuellement en plein développement dans les armées, cependant cette évolution ne peut se faire sans certaines remises en question.

A quel niveau la cyberdéfense doit-elle être organisée ?

Pour contrer la prolifération des menaces, le champ du cyber devrait logiquement faire l'objet d'une coopération internationale. Cependant, on constate une divergence fondamentale d'appréciation de ce domaine en fonction des différents Etats. En matière de sécurité dans le cyberespace, les visions s'affrontent. D'un côté les pays du nord de l'Europe, Suède et Pays-Bas, sont opposés à toute règlementation de ce milieu qu'ils considèrent avant tout comme un espace de liberté. D'un autre, les Etats-Unis et certains Européens dont la France considèrent cet espace comme un lieu de liberté, où le droit international s'applique, et où l'adoption de principes de comportements vertueux permet d'établir la confiance entre Etats. Enfin, un dernier groupe, composé par la Russie et la Chine, veut élaborer un instrument juridique international contraignant pour encadrer l'action des Etats et éviter une escalade des réactions ou une montée des tensions[52]. C'est ainsi qu'ils ont proposé en 2009 un code de conduite à l'assemblée générale des Nations Unies et que la Russie a présenté une résolution sur la sécurité de l'information à cette même instance. Pourtant, derrière ces arguments louables se cache aussi la volonté de contrôler les citoyens, comme en Chine, où les autorités pratiquent un filtrage très sophistiqué des moteurs de recherche et des réseaux sociaux

[51] Olivier Kempf, *Introduction à la cyberstratégie, op. cit.* ; Bertrand Boyer, *Cyberstratégie l'art de la guerre numérique*, *op. cit.*.

[52] Jean-François Blarel, « La France dans le débat international sur la cybersécurité », *Cybercercle défense & stratégie*, 5 décembre 2012.

occidentaux[53]. En réalité, ces pays veulent surtout que leur conception de la souveraineté nationale puisse s'appliquer dans le cyberespace.

A l'heure actuelle, la seule initiative internationale juridiquement contraignante dans le domaine de la cyberdéfense est un échec. Le Conseil de l'Europe a souhaité apporter une réponse appropriée au problème connexe de la cybercriminalité. Son principal objectif est de poursuivre « une politique pénale commune destinée à protéger la société contre la cybercriminalité, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale »[54]. En novembre 2001, la convention de Budapest est signée par une quarantaine de pays dont les Etats-Unis, l'Australie, le Canada et le Japon. Mais cette convention n'est signée ni par la Russie, pourtant membre du Conseil de l'Europe, ni par la Chine, ni par l'Inde. L'approche internationale dans le cadre du cyber n'a donc pas de réalité, elle ne fait que mettre en exergue les différences d'analyses qui existent entre les Etats.

Une prise en compte régionale, en particulier au sein d'organisations chargées de la sécurité, peut apparaître comme une meilleure solution. Pour les pays occidentaux, cette approche peut se faire au sein de l'OTAN. Dans le nouveau concept stratégique de l'Alliance, adopté le le 19 novembre 2010 à Lisbonne, les cyberattaques sont décrites comme participant des grandes évolutions de l'environnement stratégique auxquelles l'Alliance doit faire face : « nous continuerons de développer notre capacité à prévenir et à détecter les cyberattaques, à nous en défendre et à nous en relever, y compris en recourant à la planification OTAN pour renforcer et coordonner les capacités nationales de cyberdéfense, en plaçant tous les organismes de l'OTAN sous une protection centralisée et en intégrant mieux les fonctions de veille, d'alerte et de réponse de l'OTAN avec celles des pays membres »[55]. Le concept de « cyberdéfense dans la profondeur » se traduit de manière concrète par la création de deux centres. D'une part, le centre de recherche sur la cyberdéfense de l'OTAN installé à Tallinn en Estonie, créé en 2008, et que la France devrait rejoindre en 2013[56] ; d'autre part, le centre technique de la capacité OTAN de réaction aux attaques informatiques (NCIRC), qui est doté depuis fin 2012 d'une équipe de réaction rapide (RRT). « L'Alliance veut pouvoir répondre de manière appropriée à toute attaque significative, en adaptant sa réaction à l'étendue des dommages, au degré d'incertitude dans l'attribution (de l'attaque), à l'identité des agresseurs et de leurs

[53] Julien Nocetti, « Russie : le Web réinvente-t-il la politique ? », *Politique étrangère*, 2:2012, p. 286.
[54] Conseil de l'Europe, *Convention sur la cybercriminalité*, 23 novembre 2001, préambule, accessible à l'adresse : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm.
[55] Concept stratégique pour la défense et la sécurité des membres de l'Organisation du Traité de l'Atlantique Nord adopté par les chefs d'État et de gouvernement à Lisbonne, alinéa 19.8, accessible à l'adresse : http://www.nato.int/cps/fr/natolive/official_texts_68580.htm.
[56] Damien Kerlouet, « La France va participer au Centre de recherche de Cyberdéfense de l'OTAN », *Blog B2*, 3 décembre 2012, accessible à l'adresse : http://www.bruxelles2.eu/marches-de-defense/cyber/la-france-va-participer-au-centre-de-recherche-de-cyberdefense-de-lotan.html.

intentions »[57]. Pour le sénateur Jean-Marie Bockel, en dépit de ses efforts, l'OTAN n'est pourtant pas complètement armée face à cette menace[58] ; rappelons que les capacités de l'Alliance ne sont que le reflet de celles de chacun de ses pays membres : elle ne possède rien en propre et pour chaque engagement elle demande la mise à disposition de moyens spécifiques.

La réponse semble donc se situer au niveau national, seul échelon, où le pouvoir politique est capable, au-delà de la capacité d'analyse de la menace, d'orienter la stratégie en matière de cyber et de définir les différents moyens à y consacrer. Le *Livre Blanc* de 2008 sur la défense et la sécurité nationale a permis une réelle prise en compte des faiblesses de la France dans ce domaine - faiblesses qui ont été mises en exergue dans le rapport Romani de 2008 qui estime que « la France n'est ni bien préparée, ni bien organisée » pour faire face aux cybermenaces. L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) est créée en 2009. Elle présente l'avantage d'être une agence interministérielle dépendant directement du Premier ministre, d'être l'interlocuteur français unique en matière de cyberdéfense et de garantir un certain continuum sécurité-défense. L'ANSSI a publié en février 2011 la *Stratégie sur la défense et la sécurité des systèmes d'information*[59]. Celle-ci repose sur quatre objectifs : faire de la France une puissance mondiale de cyberdéfense tout en conservant son autonomie ; garantir sa liberté de décision par la protection de l'information de souveraineté ; renforcer la cybersécurité des infrastructures vitales nationales ; enfin assurer la sécurité dans le cyberespace.

Encore actuellement, dans les faits, les cyberopérations offensives sont clandestines, ce qui renforce la nécessité d'une approche exclusivement nationale. Les Etats ne les revendiquent pas. Dans le cadre de l'affaire *Stuxnet*, Américains et Israéliens, supposément à l'origine du programme, n'ont toujours pas assumé officiellement l'utilisation de cyberarmes. Des investigations de journalistes tendent à démontrer que ces différentes attaques informatiques ont été développés dans le cadre d'un programme appelé *Olympic Games*, non reconnu officiellement par les autorités américaines[60]. Avec le cyber, les Etats semblent avoir retrouvé une capacité d'action, une marge de manœuvre. On est là dans le domaine des actions secrètes de services spécialisés, ce qui peut expliquer l'absence de coopération internationale, et la difficulté à établir des relations de confiance pour encadrer ces différents rapports.

---

[57] Stéphane Abrial, « NATO builds its cyberdefenses », *The New York Times*, 27 février 2011, accessible à l'adresse : http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html?_r=0.

[58] Jean-Marie Bockel, *La cyberdéfense : un enjeu mondial, une priorité nationale*, Rapport d'information du Sénat, Commission des affaires étrangères de la défense et des forces armées du Sénat, Paris, juillet 2012, p. 57.

[59] Stratégie de la France, accessible à l'adresse : http://www.ssi.gouv.fr/IMG/pdf/2011-02 15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

[60] David E. Sanger, *Confront and Conceal*, New York, Crown publishers, 2012, p. 110.

Les Américains sur le front

Le *Livre Blanc* de 2013 apporte une évolution sur le périmètre des actions cyber qui peuvent être conduites par les forces armées, en ne les limitant plus au strict défensif : « La France développera sa posture sur la base d'une organisation de cyberdéfense étroitement intégrée aux forces, disposant de capacités défensives et offensives pour préparer ou accompagner les opérations militaires »[61]. Cela semble être, avec quelques années de retard, le même scénario que celui auquel a été confrontée l'armée américaine. Créé en 2010, le Cyber Command américain « planifie, coordonne, intègre, synchronise et conduit des actions pour commander les opérations et la défense de certains réseaux d'information du Département de la Défense ; prépare et, au besoin, conduit, tout le spectre d'opérations militaires du cyberespace dans le but de permettre des actions dans tous les domaines, assurer la liberté d'action des Etats-Unis et de leurs alliés dans le cyberespace, et l'interdire à nos adversaires »[62]. Initialement, à la date de création du Cyber Command, les militaires américains peuvent mener des actions défensives ou bloquer des attaques uniquement sur leurs propres réseaux[63].

L'état-major du Cyber Command dispose d'un effectif de 917 personnes qui devrait être porté à 4 900 personnes à terme. On estime qu'il existe au sein de l'armée américaine entre 53 000 et 58 000 « cybersoldats »[64], en excluant les contractants civils et les services de renseignement[65]. A terme, trois types de forces seront sous l'autorité du Cyber Command : « les forces de combat » qui auront pour mission d'aider les états-majors en opération à planifier et exécuter des cyberattaques à l'étranger, « les forces nationales » qui devront veiller sur les systèmes informatiques des infrastructures critiques, enfin « les forces de cyber protection », chargées des réseaux du Département de la Défense.[66].Ce commandement interarmées a autorité sur la *24ème Air Force*, la *Navy Fleet Cyber Command/10ème flotte*, le *Marine Cyberspace Command* et l'*Army Cyber Command*. Cet effectif conséquent doit cependant être relativisé, certaines unités comme la 10ème Flotte ont des missions qui ne sont pas considérées comme purement cyber en France : guerre électronique, opérations

[61] Direction de l'information légale et administrative *Livre blanc Défense et sécurité nationale*, Paris, 2013, p. 94.
[62] US Department of Defense*, U.S. Cyber Command fact sheet*, 25 mai 2010.
[63] Ellen Nakashima, « Pentagon proposes more robust role for its cyber-specialists », *The Washington Post*, 10 août 2012, accessible à l'adresse : http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story.html.
[64] Militaires dont le cœur de mission est en lien avec le cyber.
[65] John Reed, « How many cyber troops does the U.S. have? », *Foreign Policy*, 7 mars 2013, accessible à l'adresse : http://killerapps.foreignpolicy.com/posts/2013/03/07/how_many_cyber_troops_does_the_military_have.
[66] Ellen Nakashima, « Pentagon to boost cybersecurity force. », *The Washington Post*, 27 janvier 2013, accessible à l'adresse : http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

d'information, renseignement d'origine électromagnétique[67]. Le budget du Cyber Command est estimé à 191 millions de dollars pour 2013.

En 2012, le Pentagone a proposé que les cyberspécialistes militaires puissent agir hors de leurs réseaux dédiés pour pouvoir défendre les réseaux informatiques critiques américains, à condition que ces opérations répondent à des critères très restrictifs, critères qui selon certains analystes paralyseraient toute capacité d'action[68]. C'est une première étape qui élargit le domaine d'action de cette grande unité militaire. C'est aussi le constat d'une vulnérabilité face au cyber, vulnérabilité qui ne peut se résoudre par une cyberdéfense exclusive, et qui nécessite le développement d'un discours fondé sur la cyber-dissuasion[69]. La situation évolue encore en 2013, avec une appropriation très claire des missions offensives, non seulement sur le territoire américain mais aussi sur le reste du globe. Auditionné par le Sénat américain, le général Keith B. Alexander, commandant du Cyber Command, décrit la mission des 13 unités cyber offensives chargées de la dissuasion face aux cyberattaques destructrices dont peuvent être victimes les Etats-Unis : « Laissez-moi être clair, ces *Unités de défense nationale* ne sont pas des unités défensive, ce sont des unités offensives que le Département de la Défense peut utiliser pour défendre le pays si nous sommes attaqués dans le cyberespace ». En complément de cette première force, le Cyber Command met sur pied 27 unités qui vont fournir une assistance pour la planification de cyberopérations au profit des états-majors déployés sur l'ensemble du globe[70]. D'après le Vice-amiral Michael Rogers, chef des forces cyber de la Marine américaine, les commandants de théâtre ont maintenant le choix dans leurs modes d'action entre la guerre électronique, le cyber ou les actions cinétiques ; les cyberarmes doivent être intégrées avec les autres outils dont ils disposent comme un moyen pour remplir leurs missions[71].

Le développement de capacités militaires duales, tant défensives qu'offensives, est donc pleinement assumé par l'armée américaine. Cette approche pragmatique lui permet d'occuper militairement toute la largeur

---

[67] United States Naval Academy, *IDC Overview*, avril 2013, pp. 2-3, accessible à l'adresse : http://www.usna.edu/Cyber/documents/IDC/IDC_Overview.pdf.

[68] Ellen Nakashima, « Pentagon proposes more robust role for its cyber-specialists », *The Washington Post*, 10 août 2012, accessible à l'adresse : http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story.html.

[69] Entretien avec le Lieutenant-colonel Patrice Tromparent, Délégation aux Affaires Stratégiques, lundi 15 avril 2013.

[70] U.S. Senate, Committee on Armed Services, *Hearing to receive testimony on U.S. strategic command and U.S. cyber command in review of the defense authorization request for fiscal year 2014 and the future years defense program*, *Additional statements for the record full transcript*, 12 mars 2013, p. 8, accessible à l'adresse : http://www.armed-services.senate.gov/hearings/event.cfm?eventid=0daf354e2970a9db3a6d0023abe58a27.

[71] John Reed, « U.S. military working to integrate cyber weapons into commanders' arsenals, *Foreign Policy,* 9 avril 2013 : http://killerapps.foreignpolicy.com/posts/2013/04/09/us_military_starting_to_integrate_cyber_weapons_into_commanders_arsenals#.UWUwgOWglhw.twitter.

du spectre cyber, avec des moyens pour protéger ses réseaux, mais aussi des forces pour agir dans le cyberespace et apporter un appui significatif aux forces déployées dans des opérations militaires. Cette approche n'est pas encore celle de la France.

Une filière cyber française en devenir

La réponse officielle des armées françaises face au défi cyber est actuellement centrée sur la défensive. Cette mission est confiée d'une part au Haut fonctionnaire correspondant de défense et de sécurité du ministère, dont dépend la chaîne fonctionnelle SSI (Sécurité des Systèmes d'Information), qui agit au travers de cinq autorités qualifiées (CEMA, DGA, SGA, DGSE et DPSD), d'autre part, à une chaîne de cyberdéfense opérationnelle qui s'intègre aux structures de commandement[72].

A la tête de cette chaîne se trouve l'officier général en charge de la cyberdéfense (OG CYBER). Il est rattaché au sous-chef opérations avec un mandat transverse de l'Etat-major des Armées (EMA) sur l'ensemble des armées pour la partie transformation et développement des capacités. Concernant la partie planification et conduite des opérations, il est intégré au CPCO[73] et a autorité sur différentes cellules, dont celle des systèmes d'information et de communication[74]. Le positionnement à ce niveau décisionnel permet une analyse globale des menaces et donne des possibilités d'action concrètes pour la protection des forces face aux menaces cyber. L'officier général en charge de la cyberdéfense est secondé par un Officier en lutte informatique défensive central (OLID) qui pilote la montée en puissance du domaine cyber dans les armées et l'action des entités cyber interarmées (CALID[75])[76]. Une équipe de direction de cyberdéfense (CYBERDIR) met en œuvre les décisions prises par l'OG Cyber. Pour relayer les directives de la chaîne cyber, on retrouve au sein des états-majors des officiers LID (Lutte Informatique Défensive) puis des ALID (adjoints LID) dans les unités.

Dans sa mission, l'OG Cyber peut s'appuyer sur le CALID qui est le centre d'expertise du ministère de la Défense. Cet organisme est le centre d'alerte et de réaction aux attaques informatiques (CERT[77]) des armées. Cette structure assure un travail de veille et d'alerte sur les réseaux militaires déployés sur le territoire français et en opération. Il analyse les vulnérabilités et propose des solutions techniques pour renforcer la protection des réseaux. Il assure une mission de surveillance et de détection permanente des cyberattaques qui visent les forces armées. Actuellement armé par une trentaine de spécialistes, son effectif devrait être plus que doublé, pour atteindre 80 militaires. Ce centre devrait être regroupé dans le même bâtiment que le COSSI (Cellule Opérationnelle de

[72] Entretien avec le Capitaine de vaisseau Gourtay, Centre interarmées de concepts de doctrines et d'expérimentations, 2 avril 2013.
[73] Centre de Planification et de Conduite des Opérations.
[74] Contre-Amiral Arnaud Coustillière, « Ministère de la défense : Opérer en sécurité dans le cyberespace », *Cybercercle défense & stratégie*, 24 octobre 2012.
[75] Centre d'Analyse en Lutte Informatique Défensive.
[76] Entretien avec l'officier X, 4 septembre 2012.
[77] Computer Emergency Response Team.

la SSI de l'ANSSI[78]) pour permettre une meilleure synergie entre les deux organismes.

Au niveau tactique, la conduite des opérations de cyberdéfense relève du COMSIC (commandant des systèmes d'information et de communication) dont la mission est de conseiller le commandant de la force terrestre ou aérienne. Il dispose d'équipes de techniciens spécialisés en SSI aux ordres d'un Officier chargé de la sécurité des systèmes d'information (OSSI).

L'effectif de la chaîne centrale de cyberdéfense française est à peu près d'une centaine de personnes, ce qui reste relativement modeste en comparaison avec son homologue américain qui a pour objectif d'atteindre 4 900 personnes[79]. Pour Jean-Claude Mallet, « le développement des capacités de cyberdéfense comme de capacités offensives est une ambition qui ouvre un champ formidable pour nos jeunes ingénieurs et nos militaires : c'est le meilleur des technologies et des intelligences […] qu'il faudra mobiliser »[80]. Cette ambition se heurte pourtant à certains obstacles. Ainsi, l'armée américaine doit relever un véritable défi pour recruter, former et conserver dans ses rangs un si grand nombre de spécialistes. Les armées françaises sont confrontées au même problème et souffrent d'un manque d'experts LID et SSI[81]. Le déficit de spécialistes de haut niveau dans le domaine cyber est aujourd'hui une réalité en France et en Europe. L'Agence européenne ENISA (European network and information security agency) a par ailleurs souligné les difficultés comparables auxquelles sont confrontées les CERT européens pour le recrutement de certains spécialistes cyber[82]. De plus, reste à savoir quel statut, militaire ou civil, donner. Il n'est pas sûr que le cadre de leur engagement, dans un contexte uniquement technique avec des actions par « écran interposé », justifie d'en exiger les mêmes compétences que celles de soldats engagés dans des conditions opérationnelles rustiques et éprouvantes. Au-delà du recrutement, la fidélisation de la ressource pose également problème. Le système d'une prime spécifique de qualification qui avait été mis en place, il y a plusieurs années, pour éviter l'hémorragie de techniciens informatiques dans les forces a été étendu aux spécialistes du domaine cyber ; mais ce niveau de rémunération reste insuffisant pour rivaliser avec ce même secteur d'activité dans le civil, alors même que le marché de l'emploi connaît une offre importante dans cette filière. Une estimation

[78] Agence Nationale de Sécurité des Systèmes d'Information.
[79] Elisabeth Bumiller, « Pentagon expanding cybersecurity force to protect network s against attacks », *The New York Times*, 27 janvier 2013, accessible à l'adresse : http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html?_r=1&.
[80] Michel Cabirol, « Cyberdéfense: les espions vont disposer de capacités informati ques offensives », *La Tribune*, 13 mars 2013, accessible à l'adresse : http://www.la tribune.fr/entreprises-finance/industrie/aeronautique-defense/20130313trib000753767/cyberdefense-les-espions-vont-disposer-de-capacites-informatiques-offensives-24.html.
[81] Entretien avec l'officier X, 4 septembre 2012.
[82] ENISA, « Deployment of baseline capabilities of national / governmental CERTs », p. 59, accessible à l'adresse : https://www.enisa.europa.eu/activities/cert/support/files/status-report-2012.

haute donne le chiffre de 38 000 postes à pourvoir dans l'ensemble du secteur informatique en France en 2013[83].

Pour élargir son vivier d'experts, la France pourrait suivre l'exemple de certains pays étrangers. En Allemagne, il existe une communauté reconnue d'experts informatiques non conventionnels (hackers), représentée par l'association du *Chaos Computer Club*. En France, un projet similaire aurait été conduit il y a une dizaine d'année pour regrouper des hackers au sein d'une structure. Mais derrière cette initiative se cachaient en réalité les services de renseignement français dont l'action, une fois révélée, a eu pour conséquence d'installer une défiance durable entre hackers et services de l'Etat[84]. Malgré ce précédent regrettable, Il faut développer, en France, des liens plus étroits entre les spécialistes en charge de la cyberdéfense et les hackers, une sorte de « libre communauté cyber ». La compétence technique de ceux-ci pourrait être mise au profit de la défense des intérêts cyber de la nation comme le rappelle Eric Filiol : « nous souffrons d'un manque de recherches ouvertes, alors qu'il y a un excellent potentiel en France. Il faut laisser ce potentiel s'exprimer. L'Etat ne peut plus payer de recherches parce que les budgets sont restreints. Il doit donc s'appuyer sur une communauté de hackers vivante et qui assez souvent est là pour aider. L'Etat doit comprendre que cette ressource existe et l'utiliser »[85]. Ces experts pourraient devenir des corsaires des temps modernes ; travaillant au profit de l'Etat mais de manière indépendante et ponctuelle, et en retirant de leur activité un bénéfice en termes de réputation.

D'autres approches intéressantes peuvent être étudiées pour le recrutement des cyberspécialistes. L'une de ces techniques est décrite par Jacob Appelbaum dans *Menace sur nos libertés*[86]. Aux Etats-Unis, de grandes compétitions sont organisées entre plusieurs universités sur le thème de la cyberguerre, avec de véritables mises en situation sur des réseaux informatiques. Lors de ces wargames, les missions sont à la fois défensives et offensives. L'un des organisateurs de cet événement n'est autre que le SPAWAR[87], une composante civile de l'US Navy. Au cours de ce championnat, le SPAWAR mais aussi la CIA proposent de recruter les étudiants les plus talentueux en leur offrant des perspectives de carrière intéressantes dans le domaine du cyber. En Grande-Bretagne, un programme de recrutement de jeunes de la « X-Box génération » a été lancé. Ce sont des jeunes sans formation universitaire, mais passionnés

[83] Ingrid Lemelle, « Un recrutement sur quatre dans l'informatique », *La Dépêche.fr*, 18 mars 2013, accessible à l'adresse : http://www.ladepeche-emploi.fr/edito/actualite-ladepeche/article/un-recrutement-sur-quatre-dans-linformatique.html.
[84] Entretien avec un cyber hacktiviste, 19 avril 2013.
[85] Jean-Marc Manach, « Eric Filliol : « L'Etat doit s'appuyer sur les hackers », *Le Monde Blog*, 24 mai 2010, accessible à l'adresse : http://bugbrother.blog.lemonde.fr/2010/05/24/eric-filliol-letat-doit-sappuyer-sur-les-hackers/.
[86] Julian Assange avec Jacob Appelbaum, Andy Müller-Maguhn et Jérémie Zimmermann, *Menace sur nos libertés,* Paris, Robert Laffont, 2013, pp. 48-49.
[87] Space and Naval Warfare Systems Command.

par les jeux et les réseaux sociaux, qui après deux années de formation mettent leurs compétences au profit du gouvernement britannique[88].

Une approche qui doit encore évoluer

Si pour le recrutement de cyberspécialistes, il n'y a pas de différence fondamentale entre un technicien civil et son homologue militaire, c'est qu'il existe une certaine porosité dans le monde du cyber. Ce principe de porosité, c'est-à-dire d'une difficulté à compartimenter deux espaces, se retrouve également dans le champ d'application du cyber. Le cyberespace se caractérise en effet par des frontières mal définies, voire une absence de frontières[89]. L'Internet se voulait à ses débuts un espace de liberté avec une sécurité minimale. Dans les faits, on constate la difficulté des Etats à imposer leur souveraineté sur un espace mal limité. Lors du « Printemps Erable », mouvement de contestation étudiant qui a eu lieu au Canada début 2012, nombre d'attaques menées par le mouvement cyber-anarchiste *Anonymous* contre les sites canadiens officiels étaient originaires de France[90]. L'une des difficultés de la réponse apportée par les autorités québécoises est justement venue du fait que ces attaques étaient menées à partir d'un pays étranger, non soumis à la juridiction canadienne. Dans ce cas, la bonne coopération avec les autorités françaises a permis l'arrestation et la poursuite en justice de trois cyberattaquants. Toutefois, en l'absence de collaboration, on peut aisément imaginer les difficultés auxquelles auraient été confrontées les autorités canadiennes face à des attaques provenant, par exemple, de Chine.

Pour adapter cette réponse aux problèmes posés par le cyberespace, une approche globale à la fois civile mais aussi militaire doit être privilégiée. Cette réponse doit être graduée et, en fonction de la gravité de l'attaque (cf. échelle des événements cyber), de multiples acteurs peuvent intervenir. En 2009, lors de l'attaque par le ver *WIN 32 Conficker* qui a touché plusieurs millions d'ordinateurs dans le monde, la réponse fut duale, menée à la fois par la direction centrale de la sécurité des systèmes d'information – remplacée par l'ANSSI au cours de l'année 2009 – mais aussi par les services de la Défense en charge de la sécurité informatique. Dans la réponse à une attaque majeure ou grave, les moyens employés ne peuvent être uniquement militaires. Il y a une nécessaire collaboration entre instances civiles et militaires. Dans ce cadre, un renforcement des structures de cyberdéfense s'avère nécessaire. En effet, comme le rappelle le sénateur Jean-Marie Bockel dans son rapport, « notre pays accuse encore un important retard concernant les moyens et les effectifs de l'agence chargée de la sécurité des systèmes d'information, par rapport à ceux dont disposent leurs homologues en Allemagne ou au Royaume Uni »[91]. Dans ces deux pays, les effectifs sont le double de ceux de l'ANSSI, et le budget de l'agence britannique est de plus de 780 millions

[88] Pierluigi Paganini, « UK recruits "Xbox generation" youngsters for cyber war games », *Security Affairs*, 23 octobre 2012, accessible à l'adresse : http://securityaffairs.co/wordpress/9650/security/uk-recruits-xbox-generation-youngsters-for-cyber-war-games.html.

[89] Olivier Kempf, « Le cyberespace, nouveau milieu stratégique ? », *Cybercercle défense & stratégie*, 10 avril 2013, parle ainsi de « frontières poreuses ».

[90] Entretien avec le Lieutenant Jacques Oeullet, Sûreté du Québec, 22 mars 2013.

[91] Jean-Marie Bockel, *op. cit.*, p. 80.

d'euros sur 4 ans, contre 75 millions d'Euros en 2012 pour son homologue française.

Au-delà de cette réponse défensive, il faut aussi adapter le discours aux exigences d'une approche offensive. Mener des cyberopérations dans un cadre militaire ne peut être envisageable qu'après une décision d'engagement validée par l'autorité politique. Or, même si une utilisation de capacités offensives est envisagée dans le Livre Blanc sur la sécurité et la défense nationale de 2013, le plus grand secret entoure encore ce sujet. Néanmoins, le 19 juillet 2012, le sénateur Jean-Marie Bockel a quand même révélé, à propos de ces capacités offensives, que « dans ce domaine, on n'est pas manchots ». Une affirmation qui permet d'envisager une appropriation et une utilisation de telles capacités par les forces armées tout en les confrontant à certains dilemmes.

Les affrontements cyber peuvent être assimilés à des conflits asymétriques (du moins lorsque des acteurs non étatiques comme les *Anonymous* attaquent les Etats), affrontements dans lesquels l'usage de la force militaire n'est pas aisé, en particulier au niveau légal.

Dans l'hypothèse d'une riposte dans le domaine du cyberespace, il peut être nécessaire d'agir dans un temps très court, or la décision politique d'un engagement pour une opération militaire nécessite des délais conséquents. Cela est encore plus vrai si cet engagement se fait dans un contexte multinational, ce qui représente la majorité des dernières opérations dans lesquelles la France s'est engagée.

Le Droit des Conflits Armés impose en outre un principe de proportionnalité entre l'attaque et la riposte. Les parties en conflit doivent éviter les dommages collatéraux, même si ceux-ci ne sont pas strictement interdits, ils ne doivent pas être excessifs par rapport à l'avantage militaire concret et direct attendu[92]. Dans le cadre d'une « cyberguerre », ces règles sont particulièrement difficiles à respecter. Un important travail d'adaptation du *jus ad bellum* et du *jus in bello* pour interpréter les normes de droit international aux conflits cyber a été mené dans le *Manuel de Tallinn*[93], rédigé par des experts indépendants en dehors de tout cadre institutionnel. Cependant, cette étude ne traduit ni la position de l'OTAN sur ce sujet, ni la position française, nos experts n'ayant pas participé à ce travail.

A l'inverse, serait-il possible de mener une cyberattaque sans décision d'engagement militaire, sans « déclaration de guerre » ? Lors d'une cyberattaque, le problème de l'attribution de celle-ci rend incertaine la légalité de la riposte…

[92] Ministère de la défense, Secrétariat général pour l'administration, *Manuel de droit des conflits armés*, ,9 avril 2013, p. 4, accessible à l'adresse : http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/droit-des-conflits-armes/droit-des-conflits-armes.

[93] *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, accessible à l'adresse : http://www.ccdcoe.org/249.html.

Mener des cyberopérations militaires amène ainsi à se poser la question du positionnement de ces actions sur la base de la distinction entre stratégique, opératif et tactique. Si les orientations dans le domaine cyber sont prises au niveau stratégique, le niveau de la réponse doit se situer sur le plan opératif. En effet, le niveau stratégique est plus centré sur l'état final recherché, et la définition des orientations politiques de l'opération. Le niveau tactique est chargé de l'application des décisions prises par le niveau opératif pour remplir les missions correspondantes aux objectifs définis par le niveau stratégique ; la vision de l'opération s'avère alors trop compartimentée. La réponse cyber développée par les armées, au-delà de son aspect purement défensif, doit donc se faire au niveau opératif grâce à des unités interarmées. C'est en effet le denier niveau où le chef militaire possède une vue de l'ensemble des opérations menées sur un théâtre, or le champ d'action du cyber est transverse, il irrigue l'ensemble des autres domaines (terre, air, mer et espace).

S'il ne faut pas tomber dans la dérive d'une militarisation excessive du cyberespace, la réponse doit s'intégrer dans une approche globale en synergie avec les organismes civils en charge de ce domaine. Les Américains suivent d'ailleurs cette logique de collaboration entre militaires et civils : le Général Keith Alexander commandant le Cyber Command est aussi le chef de la NSA, l'une des agences civiles de cyberdéfense, comparable, pour certaines de ses missions, à l'ANSSI française. Toujours est-il qu'aux Etats-Unis mais plus encore en France, cette approche ne pourra se concrétiser sans une politique volontariste pour développer la filière technique cyber et acquérir une ressource humaine qualifiée suffisante. Pour pérenniser cette filière, il reste indispensable de mettre en place des perspectives de carrière et de rémunération qui permettent de conserver cette expertise au sein des armées.

Conclusion

Malgré toutes les tentatives pour appréhender et analyser le cyber, ce champ d'action reste complexe. Les Etats eux-mêmes se trouvent déstabilisés dans leurs modes de fonctionnement comme dans leur stratégie et sont obligés de s'adapter à ces nouveaux enjeux. Avec le cyber, ils ont progressivement perdu le monopole de l'action clandestine, confrontés à des acteurs difficilement identifiables, mais ils ont aussi retrouvé une marge d'action pour mener des opérations dans ce même cyberespace. Comme le souligne Jean-Marie Bockel, « le cyberespace paraît inévitablement voué à devenir un domaine de lutte, au même titre que les autres milieux dans lesquels interviennent nos forces armées ; il est légitime d'en tirer les conséquences, une telle capacité pouvant avoir des effets, tant aux niveaux tactique, opérationnel que stratégique »[94]. La réponse face à la menace cyber s'élabore avant tout dans une stratégie nationale, mais cette réponse demeure particulièrement difficile à mettre en œuvre, en raison de la variété des acteurs qui interviennent dans le cyberespace, de la défiance relative qui existe entre eux et de l'absence de frontières physiques qui caractérise le cyberespace.

L'approche ici retenue s'inscrit dans le continuum sécurité-défense et est nécessairement globale, en ce sens qu'elle doit concerner l'ensemble des acteurs, de la petite société jusqu'à l'Organisme d'Intérêt Vital, des agences étatiques civiles chargées de la sécurité informatique jusqu'aux acteurs militaires. Cette approche globale concerne aussi l'ensemble des actions qui peuvent être menées dans le spectre cybernétique, depuis la cyberdéfense, garante indispensable de la résilience de notre société, de notre Etat et de nos armées, jusqu'au champ d'action cyberoffensif où, à l'image des Américains, il convient maintenant d'assumer pleinement le développement de telles capacités. Cette stratégie renforcerait notre crédibilité sur la scène internationale dans le domaine cyber, et permettrait techniquement aux experts de maîtriser l'ensemble du spectre en améliorant le contrôle de nos capacités défensives par une connaissance approfondie des modes d'attaque.

Militairement, la mise en application d'une telle stratégie pourrait avoir pour conséquence la création d'unités interarmées spécialisées du domaine cyber, capables d'actions défensives comme offensives. Ces unités seraient systématiquement déployées avec les grands états-majors pour les appuyer dans leurs missions, et offrir des capacités d'action complètes dans le domaine cyber. Une telle ambition demande un

[94] Jean Guisnel, « En route vers la cyberdissuasion ! », *Le Point.fr*, 19 juillet 2012, accessible à l'adresse : http://www.lepoint.fr/editos-du-point/jean-guisnel/en-route-vers-la-cyberdissuasion-19-07-2012-1487243_53.php.

renforcement de cette filière par une augmentation de ses effectifs et de ses capacités de formation. Dans cette montée en puissance, la question du recrutement et de fidélisation de la ressource apparaissent cruciales.

A l'image de la domination des airs, devenue progressivement indispensable à la victoire au cours des soixante dernières années, la maîtrise du cyberespace semble être l'un des enjeux stratégiques du XXI^{ème} siècle. Ce domaine n'a pas pour autant gagné une véritable autonomie stratégique ; les affrontements qui s'y déroulent ne font que refléter la réalité des tensions qui existent par ailleurs. Comme pour le nucléaire il y a plus d'un demi-siècle, les Etats sont aujourd'hui engagés dans une compétition qui leur permettra de prendre un avantage stratégique indéniable, pour peu que soient consentis, dans la durée, les investissements humains et matériels.

Références

Documents officiels

ASSEMBLEE PARLEMENTAIRE DE L'ORGANISATION DU TRAITE DE L'ATLANTIQUE NORD, *Concept stratégique pour la défense et la sécuri té* alinéa 19.8, accessible à l'adresse : http://www.nato.int/cps/fr/natolive/official_texts_68580.htm.

BOCKEL Jean-Marie, *La cyberdéfense : un enjeu mondial, une priorité nationale*, Commission des affaires étrangères de la défense et des forces armées du Sénat, Paris, juillet 2012.

COMMISSION DE LA DEFENSE NATIONALE ET DES FORCES ARMEES, *Audition de M. le préfet Ange Mancini, Coordonnateur national du renseignement*, 5 février 2013, accessible à l'adresse : http://www.assemblee-nationale.fr/14/pdf/cr-cdef/12-13/c1213047.pdf.

CONSEIL DE L'EUROPE, *Convention sur la cybercriminalité*, 23 novembre 2001, accessible à l'adresse : http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm.

DEPARTMENT OF DEFENSE, *Joint terminology for cyberspace operation,* accessible à l'adresse*:* http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

DEPARTMENT OF DEFENSE, *Strategy for operating in cyberspace*, p. 5, accessible à l'adresse : http://www.defense.gov/news/d20110714cyber.pdf.

DEPARTMENT OF DEFENSE*, U.S. Cyber Command fact sheet*, 25 mai 2010.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, « Deployment of baseline capabilities of national / governmental CERT», p. 59, accessible à l'adresse : https://www.enisa.europa.eu/activities/cert/support/files/status-report-2012.

MINISTERE DE LA DEFENSE, SECRETARIAT GENERAL POUR L'ADMINISTRATION, Manuel de droit des conflits armés, 9 avril 2013, p. 4, accessible à l'adresse : http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/droit-des-conflits-armes/droit-des-conflits-armes.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, accessible à l'adresse : http://www.ccdcoe.org/249.html.

UNITED STATES NAVAL ACADEMY, *IDC Overview*, avril 2013, pp. 2-3, accessible à l'adresse : http://www.usna.edu/Cyber/documents/IDC/IDC_Overview.pdf.

US SENATE, Committee on Armed Services, *Hearing to receive testimony on U.S. strategic command and U.S. cyber command in review of the*

defense authorization request for fiscal year 2014 and the future years defense program, *Additional statements for the record full transcript*, 12 mars 2013, accessible à l'adresse : http://www.armed-services.senate.gov/hearings/event.cfm?eventid=0daf354e2970a9db3a6d0023abe58a27.

Ouvrages et monographies

ASSANGE Julien, avec APPELBAUM Jacob, MÜLLER-MAGUHN Andy et ZIMMERMANN Jérémie, *Menace sur nos libertés,* Paris, Robert Laffont, 2013.

BOYER Bertrand, *Cyberstratégie : l'art de la guerre numérique*, Paris, Nuvis, 2012.

CLAUSEWITZ Carl (Von)*, De la guerre*, Paris, éditions Perrin, avril 2006.

COLEMAN Kevin, « Cyber warfare doctrine », *The Technolytics Institute*, Analysis, 1er juin 2008.

CORNISH Paul, LIVINGSTONE David, CLEMENTE Dave et YORKE Claire, « On Cyber Warfare », A Chatham House Report, novembre 2010, accessible à l'adresse : http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf.

DURAND Etienne (de) et IRONDELLE Bastien, « Stratégie aérienne comparée: France, États-Unis, Royaume-Uni », *Centre d'études en sciences sociales de la défense*, 2006.

GRUSELLE Bruno, TERTRAIS Bruno, et ESTERLE Alain, « Cyberdissuasion », *Recherches & documents*, Fondation pour la Recherche Stratégique, n°3, 2012.

KEMPF Olivier, *Introduction à la cyberstratégie*, Lonrai, Economica, 2012.

LIBICKI Martin C., *Cyberdeterrence and Cyberwar*, Pittsburgh, RAND Corporation, 2009.

OLSEN John Andreas, *A History of Air Warfare*, Dulles, Potomac book, 2010.

SANGER David E., *Confront and Conceal*, New York, Crown publishers, 2012.

VENTRE Daniel, *Cyberattaque et cyberdéfense*, Paris, Lavoisier, septembre 2011.

Articles de revues

BAUD Michel, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique étrangère*, n° 2, 2012, pp. 305-316.

BERMAN Ilan, « The Iranian cyber threat to US homeland », *Pundicity Informed Opinion & Review*, 26 avril 2012, accessible à l'adresse: http://www.ilanberman.com/11611/the-iranian-cyber-threat-to-the-us-homeland.

BRONK Christopher et TIKK RINGAS, « The Cyber Attack on Saudi Aramco », *Survival: Global Politics and Strategy*, vol. 55, n°2, avril 2013, pp. 81-96.

BUTT Yousaf, « Rabid Response », *Foreign Policy*, 22 mars 2013, accessible à l'adresse : http://www.foreignpolicy.com/articles/2013/03/22/rabid_response?wp_login_redirect=0.

DUNN CAVELTY Myriam, « Cyberwar: Concept, status quo, and limitations », *CSS Analysis in Security Policy*, n° 71, avril 2010, accessible à l'adresse : http://www.academia.edu/1058235/Cyberwar_Concept_Status_Quo_and_Limitations.

DURAND ETIENNE (de), « Le renouveau de la puissance aérienne », *Hérodote*, n° 114, 2004, pp. 17-34.

FARWELL James P. et ROHOZINSKI Rafal, « Stuxnet and the Future of Cyberwar », *Survival: Global Politics and Strategy*, vol. 53, n° 1, 2011, pp. 23-40.

HENNI Abdelghani, « Middle East Attacks Raise Cyber Security Questions », *Journal of petroleum technology*, octobre 2012, pp. 68-69.

NOCETTI Julien, « Russie : le Web réinvente-t-il la politique ? », *Politique étrangère*, n° 2, 2012, pp. 277-289.

REED John, « How many cyber troops does the U.S. have? », *Foreign Policy*, 7 mars 2013, accessible à l'adresse : http://killerapps.foreignpolicy.com/posts/2013/03/07/how_many_cyber_troops_does_the_military_have.

REED John, « U.S. military working to integrate cyber weapons into commanders' arsenals », *Foreign Policy,* 9 avril 2013, accessible à l'adresse : http://killerapps.foreignpolicy.com/posts/2013/04/09/us_military_starting_to_integrate_cyber_weapons_into_commanders_arsenals#.UWUwgOWglhw.twitter.

RID Thomas, « Cyber war will not take place », *Journal of Strategic Studies,* vol. 35, n°1, février 2011, pp. 5-32.

RID Thomas et McBURNEY Peter, « Cyber-Weapons », *The RUSI Journal*, vol. 157, n°1, p. 6-13, accessible à l'adresse : http://www.tandfonline.com/doi/full/10.1080/03071847.2012.664354#tabModule.

SIBONI Gabi et KRONENFELD Sami, « Iran and Cyber Warfare », *Military and Strategic Affairs*, vol. 4, n°3, décembre 2012, pp. 77-99.

Sites Internet

« Des milliers de clients d'EDF visés par une vague de faux emails », *Le Monde.fr*, 31 janvier 2013, accessible à l'adresse : http://www.lemonde.fr/technologies/article/2013/01/31/edf-cible-d-une-cyberattaque-d-ampleur_1825096_651865.html

« First-ever cyber drills planned », *Iran daily*, 25 octobre 2012, p. 3.

« Les armées attaquées par un virus informatique », blog *Secret Défense*, 5 février 2009, accessible à l'adresse : http://secretdefense.blogs.liberation.fr/defense/2009/02/les-armes-attaq.html

« Rapport Exclusif : le cyberespace se « militarise » de plus en plus », 01.net, 18 janvier 2013, accessible à l'adresse : http://www.01net.com/editorial/584645/rapport-clusif-le-cyberespace-se-militarise-de-plus-en-plus/.

ABRIAL Stéphane, «NATO builds its cyberdefenses», *The New York Times*, 27 février 2011, accessible à l'adresse : http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html?_r=0.

BUMILLER Elisabeth, « Pentagon expanding cybersecurity force to protect networks against attacks », *The New York Times*, 27 janvier 2013, accessible à l'adresse : http://www.nytimes.com/2013/01/28/us/pentagon-to-beef-up-cybersecurity-force-to-counter-attacks.html?_r=1&.

CABIROL Michel, « Cyberdéfense : les espions vont disposer de capacités informatiques offensives », *La Tribune*, 13 mars 2013, accessible à l'adresse : http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20130313trib000753767/cyberdefense-les-espions-vont-disposer-de-capacites-informatiques-offensives-24.html.

EUDES Yves, « Hackers d'Etat », *Le Monde*, le 19 février 2013, accessible à l'adresse : http://www.lemonde.fr/technologies/article/2013/02/19/hackers-d-etat_1834943_651865.html.

FILLIOL Eric, « L'«affaire» Vupen où quand la compétence française fait peur aux États Unis », *Les Echos.fr*, 6 février 2013, accessible à l'adresse : http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221164714/affaire-vupen-quand-competence-francaise-fai.

FRANCIS David, « Pentagon Readies a Cyber Arsenal to Fight Attackers », *The Fiscal Times*, 18 février 2013, accessible à l'adresse : http://www.thefiscaltimes.com/Articles/2013/02/18/Pentagon-Readies-a-Cyber-Arsenal-to-Fight-Attackers.aspx#page1.

FUNG Brian, « How Many Cyberattacks Hit the United States Last Year? », *National Journal*, 8 mars 2013, accessible à l'adresse: http://www.nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/?oref=ng-dropdown.

GUISNEL Jean, « En route vers la cyberdissuasion ! », *Le Point.fr*, 19 juillet 2012, accessible à l'adresse : http://www.lepoint.fr/editos-du-point/jean-guisnel/en-route-vers-la-cyberdissuasion-19-07-2012-1487243_53.php.

KERLOUET Damien, « La France va participer au Centre de recherche de Cyberdéfense de l'OTAN », *Blog B2*, 3 décembre 2012, accessible à l'adresse : http://www.bruxelles2.eu/marches-de-defense/cyber/la-france-va-participer-au-centre-de-recherche-de-cyberdefense-de-lotan.html.

LE BLOHEC Emmanuel, « Internet, champ de bataille des temps modernes ? », *Les Echos.fr*, 16 février 2012, accessible à l'adresse : http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221143516/internet-champ-bataille-temps-modernes.

LEMELLE Ingrid, « Un recrutement sur quatre dans l'informatique », *La Dépêche.fr*, 18 mars 2013, accessible à l'adresse : http://www.ladepeche-emploi.fr/edito/actualite-ladepeche/article/un-recrutement-sur-quatre-dans-linformatique.html.

MANACH Jean-Marc, « Eric Filliol : « L'Etat doit s'appuyer sur les hackers », *Le Monde Blog*, 24 mai 2010, accessible à l'adresse :

http://bugbrother.blog.lemonde.fr/2010/05/24/eric-filliol-letat-doit-sappuyer-sur-les-hackers/

MANNES Aaron et HENDLER James, « The first modern cyberwarfare ? », *The Guardian*, 22 août 2008, accessible à l'adresse : http://www.guardian.co.uk/commentisfree/2008/aug/22/russia.georgia1.

NAKASHIMA Ellen, « Pentagon proposes more robust role for its cyber-specialists », *The Washington Post*, 10 août 2012, accessible à l'adresse : http://www.washingtonpost.com/world/national-security/pentagon-proposes-more-robust-role-for-its-cyber-specialists/2012/08/09/1e3478ca-db15-11e1-9745-d9ae6098d493_story.html.

PAGANINI Pierluigi, « New weapons for cyber warfare. The CHAMP project », *blog Security Affairs*, 4 décembre 2012, accessible à l'adresse : http://securityaffairs.co/wordpress/10783/cyber-warfare-2/new-weapons-for-cyber-warfare-the-champ-project.html.

PAGANINI Pierluigi, « UK recruits "Xbox generation" youngsters for cyber war games », *Security Affairs*, 23 octobre 2012, accessible à l'adresse : http://securityaffairs.co/wordpress/9650/security/uk-recruits-xbox-generation-youngsters-for-cyber-war-games.html.

SANGER David E. et SHANKER Tom, « Broad powers seen for Obama in cyberstrikes », *The New York Times*, 3 février 2013, accessible à l'adresse : http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=1&.

Site Internet Vupen/ accessible à l'adresse : http://www.vupen.com/english/services/lea-index.php.

Communications

BLAREL Jean-François, « La France dans le débat international sur la cybersécurité », *Cybercercle défense & stratégie*, 5 décembre 2012.

Contre-Amiral COUSTILLIERE Arnaud, « Opérer en sécurité dans le cyberespace », *Cybercercle défense & stratégie*, 24 octobre 2012.

KEMPF Olivier, « Le cyberespace, nouveau milieu stratégique ? », *Cybercercle défense & stratégie*, 10 avril 2013.

Entretiens

Entretien avec l'officier X, 4 septembre 2012.

Entretien avec le Lieutenant Jacques Oeullet, Sûreté du Québec, 22 mars 2013.

Entretien avec le Capitaine de vaisseau Gourtay, Centre interarmées de concepts de doctrines et d'expérimentations, 2 avril 2013.

Entretien avec le Lieutenant-colonel Patrice Tromparent, Délégation aux Affaires Stratégiques, 15 avril 2013.

Entretien avec le Colonel Jérome Pellistrandi, officier chargé de domaine, Centre interarmées de concepts, de doctrines et d'expérimentation, 16 avril 2013.

Entretien avec une cyber hacktiviste, 19 avril 2013.

Informations aux lecteurs

Si vous êtes intéressé (e) par d'autres publications de la collection, veuillez consulter la section « Focus Stratégique » sur le site Internet de l'Ifri :

www.ifri.org/

Les derniers numéros publiés de la collection « Focus stratégique » sont :

- John Louth, « Defence Reform in the United Kingdom: A Twenty-First Century Paradox », *Focus stratégique*, n° 43, mars 2013. http://www.ifri.org/downloads/fs43louth.pdf

- Sophie Lefeez, « Toujours plus chers ? Complexité des armements et inflation des coûts militaires », *Focus stratégique*, n° 42, février 2013. http://www.ifri.org/downloads/fs42lefeez.pdf

- Michael W. Kometer, Stephen E. Wright, « Winning in Libya: By Design or Default? », *Focus stratégique*, n° 41, janvier 2013. http://www.ifri.org/downloads/fs41kometerwright.pdf

- Martial Foucault, « The Defense Budget in France: between Denial and Decline », *Focus stratégique*, n° 36 *bis*, décembre 2012. http://www.ifri.org/downloads/fs36bisfoucault.pdf

- Hugues Eudeline, « Contenir la piraterie: des réponses complexes face à une menace persistante », *Focus stratégique*, n° 40, novembre 2012. http://www.ifri.org/downloads/fs40eudeline.pdf

- Elie Tenenbaum, « The Battle over Fire Support: The CAS Challenge and the Future of Artillery », *Focus stratégique*, n° 35 *bis*, octobre 2012. http://www.ifri.org/downloads/fs35bistenenbaum.pdf

- Michel Baud, « Les réserves en première ligne ? Du citoyen-soldat à l'intérim », *Focus stratégique*, n° 39, septembre 2012. http://www.ifri.org/downloads/fs39baud.pdf

- Olivier Neola, « Building Security Institutions: Lessons Learned in Afghanistan », *Focus stratégique*, n° 38, juillet/août 2012. http://www.ifri.org/downloads/fs38neola.pdf