Menaces, conflits dans le cyberespace et cyberpouvoir

Solange Ghernaouti

Dans Sécurité et stratégie **2011/3 7** , pages 61 à 67
Éditions Cercle des Directions de la Sécurité des Entreprises

ISSN 2101-4736
DOI 10.3917/sestr.007.0061
Date de mise en ligne : 11/06/2015

Menaces, conflits dans le cyberespace et cyberpouvoir

La récente révélation de postes de commande de drônes américains infectés par un virus constitue une énième alerte. Si ce genre d'intrusion ne s'est, à ce jour, pas soldé par une atteinte majeure à la sûreté d'un Etat, la plus grande vigilance est requise. Solange Ghernaouti-Hélie, professeur à l'université de Lausanne, présente dans cet article les diverses formes d'expression de conflits qui peuvent se manifester dans le cyberespace et met en exergue le rôle que peuvent jouer les civils, y compris les *hacktivistes*, dans la force de frappe informatique d'un pays. L'article donne un éclairage sur les notions de cyberguerre et de cyberdéfense, sur les moyens de prévention comme de réaction et soulève le problème de l'identification de l'origine des cyberattaques. Une réflexion sur les aspects légaux relatifs à la cyberguerre et à la cybercriminalité conclut cet article en identifiant le besoin d'une approche holistique de la cybersécurité, basée sur une coopération de tous les acteurs et une collaboration internationale efficace.

L'information, une arme de guerre

La première guerre du Golfe en 1990 a été révélatrice de nouvelles manières d'utiliser l'information et l'opinion publique mondiale lors d'un conflit armé, en s'appuyant notamment sur la télévision et la chaine d'information CNN. Cela a été un tournant, précurseur de l'appropriation d'Internet et des nouveaux médias de communication, des millions de téléspectateurs ayant pu suivre la guerre en direct. Ce conflit armé s'est doublé d'une guerre médiatique où l'information devenait un instrument d'influence auprès de l'opinion publique. De même, en révélant certains épisodes de la guerre en Irak en 2010, l'affaire wikileaks (dont les effets sont toujours d'actualité) relève du même ordre, bien que les motivations soient différentes. Leurs finalités sont identiques, à savoir interpeller et influencer l'opinion publique. L'information n'a même pas besoin de code malveillant pour être utilisée dans des campagnes de manipulation et d'influence idéologique, et ainsi être considérée comme une arme de soutien à tous types de conflits (*Information as a weapon*). Des pressions médiatiques ou psychologiques peuvent être infligées aux adversaires et peuvent toucher une population et ses dirigeants. Depuis toujours, la capacité à vaincre dépend en partie de la maîtrise de l'information et de son environnement humain et technologique.

Pour gagner une guerre, il a toujours fallu maîtriser l'information tant sur le plan stratégique qu'opérationnel. Avec Internet et le cyberespace, cette guerre de l'information a pris une toute autre dimension. C'est également sur le plan médiatique que l'information relative à la guerre doit être maitrisée, afin de contrôler l'image des parties impliquées, d'influencer l'opinion publique, de la mobiliser, voire de recruter des cyberpatriotes et/ou cyberdissidents. Les forums de discussion et autres plateformes de socialisation sont autant de moyens de communication utiles aux campagnes d'information et de propagande utilisés pour interpeller les individus et éventuellement les inciter, directement ou non, à réaliser des cyberactes de représailles ou de soutien à des conflits réels.

Pour gagner une guerre, il a toujours fallu maîtriser l'information tant sur le plan stratégique qu'opérationnel.

La désobéissance civique et l'atteinte à la démocratie peuvent trouver leur expression dans le cyberespace, mais les dénonciations de celles-ci peuvent tout aussi être facilitées par le Net. La définition du terme de cyberdissidence et de ce qu'il recouvre dépend du contexte dans lequel il est employé. Ainsi que le cas de Wikileaks en témoigne, la cyberdissidence relèvera pour certains d'un acte de guerre, de terrorisme ou de désobéissance civique, pour d'autres de la liberté d'expression et de la lutte contre le totalitarisme. La puissance d'Internet comme outil de communication n'est plus à démontrer. Par sa nature, à l'occasion d'un conflit, il peut être convoité par des internautes transformés en cyberpatriotes animés par l'intention de nuire à une communauté particulière, en saturant des sites hostiles à leur cause et en orchestrant des campagnes de désinformation. Des attaques en déni de service, issues de points divers de la planète, souvent téléguidées et instrumentalisées, sont difficiles à contrer pour les diasporas concernées.

Des cyberactions visant à nuire à l'Etat

L'espionnage des communications, la domination de certains acteurs du Net ou encore des actions de surinformation ou de désinformation portant atteinte au moral des citoyens d'un pays, peuvent alimenter des actions visant à lui nuire. Internet peut en effet servir des stratégies indirectes qui, même en temps de paix, visent à affaiblir un secteur d'activité, une entreprise, un pays et fournir ainsi des avantages concurrentiels à certains acteurs socio-politico-économiques. Tous les conflits peuvent être transposés dans le cyberespace au moyen de cyberattaques et de manipulations de l'information. Si toutes les cyberattaques ne relèvent pas du terrorisme ou de la guerre entre Etats, Internet introduit de nouveaux risques en devenant parfois un outil de destruction comme cela a été le cas avec le vers informatique Stuxnet découvert en 2010[1]. Internet peut soutenir un projet politique et être utilisé dans un but conflictuel, voire éventuellement infliger des dégâts à l'ennemi sans combattre, en réduisant son pouvoir dans les domaines économique, scientifique et culturel. Aucun Etat n'est à l'abri de cyberactions malveillantes.

Désormais, il faut considérer les technologies de l'information et de la communication comme des éléments d'innovation dans l'art de faire la guerre. Internet, les ordinateurs, le code informatique ainsi que les données, sont de nouvelles armes de guerre dans un nouveau champ de bataille qu'est

[1] *Vers informatique ciblant les systèmes de contrôle industriel SCADA (Supervisory Control and Data Acquisition) existant notamment dans les installations nucléaires et ayant porté particulièrement préjudice aux installations iraniennes.*

le cyberespace. Le Net induit un nouveau paradigme : le cyberpouvoir dont la conquête ou la défense justifie le recours à des dispositifs de cyberdéfense passive et active. Ils sont à intégrer aux stratégies nationales de cybersécurité.

Le cyberespace, facteur d'innovation dans l'art de faire la guerre

Le cyberespace, tout comme l'air, la mer, la terre peut s'avérer être un théâtre d'opérations militaires auquel l'ennemi n'est pas familier et qui le place donc en situation d'infériorité. Comme la criminalité en col blanc, la guerre en col blanc existe aussi. Une guerre dans le cyberespace peut sembler de prime abord, et *a priori*, moins sale qu'une guerre réelle. Dissociée d'actes militaires dits classiques, elle est néanmoins hypocrite et indirecte. En effet, faire la guerre dans le cyberespace, via des systèmes informatiques, des logiciels et des données, ne nécessite plus d'affrontement direct entre des forces armées, ni de franchissement de frontières géographiques pour envahir un pays. De même, l'identité du cyberguerrier est dissimulée par divers intermédiaires techniques, humains et géographiques. La responsabilité de la cyberattaque est donc difficile à établir et ses auteurs difficilement identifiables.

De la cyberguerre

Les conséquences d'un acte de guerre s'évaluent habituellement en termes de combattants tués ou blessés et de destructions infligées à l'ennemi. Le brouillage des communications, les attaques informatiques sur les systèmes de contrôle aérien ou de contrôle des pipelines et les réseaux de distribution du gaz, ou encore sur des usines de fabrication de produits indispensables à la vie économique tels que ceux de la chimie industrielle, pourraient être considérés comme étant des actes de guerre. Par de telles attaques, la population civile ne serait pas plus épargnée qu'elle ne l'a été dans le cas d'Hiroshima ou qu'elle ne l'est presque toujours dans les conflits actuels.

Parmi les attaques informatiques majeures sont classées celles qui visent les systèmes contrôlant les infrastructures critiques et dont les conséquences sont dommageables pour la société et la sécurité nationale d'un pays. Si les commanditaires de telles attaques sont eux-mêmes des Etats, elles peuvent s'inscrire dans une stratégie de guerre informatique à but offensif, d'intimidation ou de rétorsion. La Russie contre l'Estonie ou Israël à l'égard de certains de ses voisins en fournissent des exemples.

Par ailleurs, les attaques informatiques offensives peuvent se coupler avec des stratégies militaires classiques, afin de fragiliser les défenses de l'adversaire, le leurrer, déstabiliser son renseignement, contribuer à altérer son processus de décision, neutraliser voire paralyser des centres stratégiques ou encore bloquer les moyens de communication. Force est de constater que plus les Etats sont développés, plus leur capacité militaire et leur pouvoir économique sont dépendants des technologies de l'information. Ils sont alors davantage vulnérables aux attaques informatiques et donc d'autant plus fragilisés.

Les ordinateurs télécommandés après leur prise de contrôle par des programmes informatiques lancés ou commandités par des militaires (notion de *Botnets* militaires), seraient similaires à des combattants infiltrés et commandés à distance. Dès lors, le piratage informatique pourrait être considéré comme une arme de guerre et la distinction de ce qui relève du domaine civil ou militaire devient encore plus floue.

Il est difficile de pouvoir attribuer des actes de guerre informatique à un Etat ou d'en prouver la responsabilité directe ou indirecte en raison des nombreux intermédiaires techniques, du recours éventuel à des mercenaires ou à l'usage de *botnets*.

Par ailleurs, il est difficile d'attaquer sur Internet sans passer par des infrastructures traversant des pays neutres ou alliés. Les acteurs potentiels d'une cyberguerre à l'échelle mondiale ne sont pas isolés car toutes les infrastructures sont interconnectées et interdépendantes.

Si des scénarios d'attaques majeures et massives sont possibles, ils ne se sont pas encore manifestés dans leur intégralité et ne sont pas forcément d'actualité en raison de la cyberdissuasion. En effet, la capacité des Etats à répondre à la cyberguerre par la cyberguerre neutralise les acteurs internationaux, à l'instar de la dissuasion nucléaire. L'analogie est certes exagérée, mais à ce jour, ce qui change, c'est le nombre potentiel d'Etats capables de lancer une attaque ou une contre-attaque informatique massive. Ce serait une erreur de sous-estimer ce potentiel de cybermenaces dans les rapports de force entre gouvernements, dans le jeu de leurs alliances et dans les équilibres géostratégiques. Pour autant, la destruction totale d'Internet (par des attaques sur les serveurs DNS – *Domain Names Servers* – racines par exemple) est peu envisageable car celle-ci ne profiterait à personne. En conséquence, il existe une certaine volonté internationale pour prévenir une cyberguerre massive et respecter le seuil de survie d'Internet.

La cybersécurité fait beaucoup parler d'elle et les cyberrisques font peur. Encore faut-il ne pas omettre non plus le cyberrisque lié à l'usage d'armes à impulsions électromagnétiques[2] capables d'anéantir tout traitement informatique et de télécommunication de manière rapide et définitive (notion de guerre d'anéantissement technologique). L'impact qu'un tel scénario aurait sur les activités humaines, qui dépendent de plus en plus des technologies de l'information, serait considérable.

L'hacktivisme au service d'un conflit

Le potentiel d'Internet permet d'attiser des conflits et peut inciter spontanément des civils à réaliser des cyberattaques contre des sites y compris gouvernementaux.
Les actions de propagande peuvent être soutenues par la diffusion d'adresses de sites web mettant à disposition des modes d'emploi et des outils de cyberattaques. L'hacktivisme (contraction de *hacker* et d'activisme) est une forme de protestation basée sur l'usage de cyberattaques pour défendre des idéologies ou des objectifs politiques. *Hackers* patriotiques ou cyberdissidents concentreront leurs attaques contre des cibles considérées comme hostiles, se traduisant entre autres par des dénis de service ou des défigurations de sites web. L'hacktiviste peut également utiliser toute la panoplie des outils de communication d'Internet (blogs, réseaux sociaux, YouTube...) pour informer, dénoncer ou tenter de convaincre et rassembler des personnes à sa cause.
Le hacker-activiste peut penser que son activité de *hacking* (pénétration non autorisée dans des systèmes informatiques) est légitimée par l'existence même d'Internet et par la passion qu'il nourrit à son égard. Possédant généralement une haute opinion de lui-même associée à un profond sentiment de supériorité et se sentant investi d'une mission, son activité s'imposera à lui comme étant naturelle. Il est parfois complexe de comprendre les motivations qui animent les hacktivistes qui agissent cachés derrière un écran et à distance, via de multiples intermédiaires techniques et des identités généralement fausses, anonymisées ou usurpées. Leurs actes relèvent-ils d'une action citoyenne, d'une recherche de reconnaissance, du fanatisme, du mysticisme, de la criminalité ou du terrorisme ?

[2] *Les armes à impulsions électromagnétiques (electromagnetic impulse weapons) communément dénommées E-bomb (Electromagnetic bombs) produisent des radiations électromagnétiques telles que les systèmes électroniques et informatiques ne sont plus en mesure de fonctionner.*

L'internaute, le cybermilicien et le cybermercenaire

La charge malveillante de certains programmes informatiques (virus, bombe logique,...) peut être lancée par n'importe qui possédant une connexion Internet. Par ailleurs, des ordinateurs « zombies » faisant partie de réseaux de *botnets* et contrôlés à distance peuvent être activés à tout moment[3]. Ainsi, tout individu peut éventuellement devenir acteur à part entière dans les conflits du cyberespace pour servir une cause idéologique ou nationale. Dans la lutte engagée contre Anonymous, les individus interpellés sont bien souvent jeunes et parfois titulaires d'un simple diplôme d'ingénieur. La guerre de l'information sur Internet n'est pas le pré carré d'une élite ou réservée aux seuls militaires, elle est ouverte à tous les internautes. Par exemple, le site *www.le-post.fr* permet ainsi aux internautes de s'improviser journalistes pour disséminer toutes sortes d'informations : tribunes politiques, lobbying contre la guerre en Libye ou en Côte d'Ivoire...

Par Internet, la mobilisation des civils peut être extrêmement rapide et efficace leur permettant de devenir des cyberagents au service de causes particulières. Des attaques informatiques transfrontalières sur les infrastructures d'un autre Etat sont possibles. En temps de « guerre », Internet, comme tout type de réseaux, peut se transformer en unité de guerre offensive. Jean Bodin[4] disait qu'il n'y avait « de richesse que d'hommes ». Dans ce contexte, en supposant que le nombre de cyberagents reflète d'une certaine manière la puissance d'une cyberforce, seule la Chine peut alors se prévaloir de disposer d'un nombre potentiel de cyberguerriers important[5], en supposant toutefois que ses internautes soient tous animés du même sentiment patriotique. Il est alors possible d'avancer que la Chine se place au premier rang des puissances mondiales de cyberforce, disposant d'une force de frappe informatique offensive ou défensive potentielle conséquente.

> **Le Pentagone a récemment révélé le vol en mars 2011 de 240 000 fichiers « de données sensibles ».**

Dès lors, quels pays peuvent affirmer être prêts à faire face à des cyberattaques massives ? Réponse : ceux capables de démontrer qu'ils possèdent une force de frappe offensive puissante en la matière et à cette fin, de s'appuyer sur des alliances stratégiques entre Etats. Une manière éprouvée de défense est de dissuader par la menace de cyberattaques puissamment destructrices. La cybersécurité passe également par la diplomatie et la coopération internationale.

Par analogie, la *Code war* succède à la *Cold war*. Nous l'avons dit, dans le cyberespace, l'ennemi peut être difficilement identifiable et la responsabilité d'une cyberattaque masquée ou anonymisée via un acteur tiers. Par conséquent, comment distinguer l'implication de terroristes, de personnes isolées, du crime organisé, de mercenaires à la solde d'un Etat, de forces armées ou encore d'une combinaison de ces types de commanditaires ?

Dans cette *Code war* en devenir, impossible de répondre à la question de savoir quel pays est mieux préparé que les autres. Remarquons seulement que les Etats-Unis d'Amérique (dont les militaires ont été à l'origine d'Internet dans les années 1960) possèdent une maîtrise certaine des technologies de l'information ainsi que des

[3] *Sur Internet, il est possible de recruter les compétences et de se procurer des outils pour réaliser des cyberattaques (programmes malveillants, ordinateurs infectés faisant partie de réseaux de botnets, ...).*
[4] *Jean Bodin (1529/30–1596) juriste, économiste, philosophe, historien et politologue français influent du XVIème siècle.*
[5] *Le nombre d'internautes chinois a atteint 477 millions à la fin du mois de mars 2011 (et est appelé à croitre) http://french.peopledaily.com.cn/Sci-Edu/7381640.html*

politiques de cybersécurité, mais ne sont pas pour autant épargnés par des actes informatiques hostiles. Pour ne citer qu'un exemple, le Pentagone a récemment révélé le vol en mars 2011 de 240 000 fichiers « de données sensibles » lui appartenant, consécutif à des intrusions dans les systèmes informatiques d'un industriel de la défense, provenant d'un gouvernement étranger (Source : *Associated Press*).

Vers une perméabilité des frontières entre les mondes civil et militaire

Certains Etats ont bien compris le risque qu'ils encouraient autant que l'intérêt qu'ils pouvaient tirer d'une population de personnes spécialement formées aux TIC et de recourir à leurs compétences d'experts dans les domaines militaire, diplomatique ou politique, y compris parmi la communauté des cybermercenaires. Ces derniers utilisent les mêmes armes (savoir-faire et boîte à outils) que les cybercriminels. D'ailleurs, ces cybermercenaires acquièrent et testent généralement leurs compétences via des activités cybercriminelles (cyberattaques sur des cibles civiles) qui les enrichissent et augmentent leur expérience en la matière et leurs tarifs. C'est une des raisons pour lesquelles les militaires trouveront un bénéfice à collaborer avec des experts issus du monde civil (instances de justice et de police) qui possèdent une certaine expérience en matière de lutte contre la cybercriminalité et des spécialistes en informatique, télécommunication et sécurité qui maîtrisent les environnements et technologies liés à la cybersécurité.

En revanche, toujours de manière générale, le monde militaire possède une bien meilleure maitrise des techniques de renseignement et a naturellement investi le cyberespace pour pratiquer la surveillance ou l'espionnage. Le cyberespace, encore récemment essentiellement cantonné à la société civile, est dorénavant exploité par le monde militaire qui met à profit des moyens civils pour être opérationnel. Des termes tels que cyberattaques, cyberforces, cyberarmées, appartiennent à un vocabulaire qui ne cesse de se développer et de s'enrichir de toute la nomenclature militaire existante. Ce n'est pas l'évolution de la terminologie qui pose problème, c'est ce qu'elle reflète : une réappropriation d'Internet par les militaires et l'omniprésence des germes de la guerre économique qui se sont déplacés sur le terrain informationnel et dans le cyberespace. La maîtrise d'Internet devient de ce fait un enjeu stratégique communautaire alors que l'on constate une perméabilité des frontières entre les domaines ludique et professionnel, privé et public, civil et militaire.

De la doctrine militaire à une approche globale de cybersécurité

Contrairement aux autres espaces naturels et biens communs, aucun traité international ne régit le cyberespace. L'ensemble des Conventions, Traités et Protocoles internationaux relatifs à la guerre ne sont pas adaptés aux caractéristiques des cyberconflits et de la cyberguerre. Inversement, le corpus légal existant en matière de cybercriminalité n'est pas suffisant. En effet, il va notamment à l'encontre des notions de défense active et de représailles, notions présentes dans toute doctrine militaire. De surcroît, la notion de dissuasion, prise au sens militaire, ne peut pas être efficace si elle respecte scrupuleusement les lois qui répriment la criminalité (la cybercriminalité). Cela est également exacerbé en raison de l'existence de paradis digitaux[6] et du fait que la

[6] *Par analogie au paradis fiscal, un paradis digital est un pays ou la criminalité informatique et la cybercriminalité ne sont pas considérées comme étant illégales.*

collaboration internationale en matière de lutte contre la criminalité informatique transnationale n'est pas toujours suffisamment efficace.

Le recours à un Traité de non-prolifération de cyberarmes est parfois évoqué par analogie au Traité de non-prolifération des armes nucléaires[7]. Bien que ce Traité soit essentiel, il n'était d'aucune utilité pour prévenir la catastrophe nucléaire de Fukushima de mars 2011 qui ne relevait pas d'un acte de guerre. En revanche une structure organisationnelle comme l'IAEA (*International Atomic Energy Agency*)[8] prend tout son sens dans la coordination du suivi de la catastrophe et dans l'élaboration de mesures préventives. Une structure équivalente devrait exister pour promouvoir la sécurité publique, l'innocuité de l'usage des technologies de l'information et des communications, un cyberespace sûr, de confiance, sécurisé et pacifique.

Cette analogie aux armes et centrales nucléaires ne doit pas nous faire oublier qu'il est nécessaire de disposer d'une démarche globale et holistique d'appréhension des menaces, des risques et de la sécurité liés au cyberespace. Elle pourrait s'appuyer sur un traité international du cyberespace (ou un ensemble de traités liés à la cybersécurité), des structures organisationnelles à l'échelon national et international adaptées. De plus, elle devrait tenir compte des perspectives militaire et civile liées à la cyberdéfense et à la cybersécurité.

Les cyberattaques ne sont souvent que la partie visible de l'usage d'Internet à des fins malveillantes. Impossible d'oublier qu'Internet est aussi au service de la performance de l'économie illicite, de la délinquance et de la criminalité organisée et qu'il contribue à tous les types de trafics (trafic de drogue, d'êtres humains, blanchiment d'argent, ...).

Lutter pour prévenir les cyberattaques relevant de cyberconflits ou de la cybercriminalité, passe par le renfort de la résilience des infrastructures, le développement des capacités humaines, organisationnelles, juridiques et technologiques adaptées et la mobilisation de tous les acteurs de la société. La cybersécurité n'est pas uniquement l'affaire de l'Etat ou d'une stratégie gouvernementale. Aucun livre blanc, aucune doctrine militaire ne peut pallier le manque de responsabilité individuelle et collective de la société civile, le manque de partenariats efficaces entre le secteur privé et le secteur public. ■

Solange Ghernaouti-Hélie,
Professeur à la faculté des HEC
de l'Université de Lausanne

Bibliographie

J. Carr « Inside Cyberwarfare » O'Reilly, 2009.

K. Geers « Strategic Cyber security ». NATO Cooperative Cyber Defence Centre of Exexellence , Estonie 2011.

S. Ghernaouti-Hélie « La cybercriminalité. Le visible et l'invisible ». Collection Le savoir suisse, Presses polytechniques et universitaires romandes, 2009.

International Telecommunication Union « Global Cybersecurity Agenda : strategic report » http://www.itu.int/osg/csd/cybersecurity/gca/

M. Quemener, Y. Charpenel, « Cybercriminalité : droit pénal appliqué », Economica, 2010.

Revue Défense nationale et sécurité collective, Cybersecurité & Cyberconflits, n° 08-09, 2009

S. Schjolberg & S. Ghernaouti-Hélie, « A global treaty on cybersecurity and cybercrime : a contribution for peace, justice and security in cyberspace », Second edition, Cybercrimedata, Oslo, 2011.

« The Russia- U.S. Bilateral on critical infrastructure protection. Working towards rules for governing cyber conflicts. Rendering the Geneva and Hague conventions in cyberspace » EastWest Institute, 2011.

[7] *Treaty on the Non-Prolifération of Nuclear Weapons. Opened for signature at London, Moscow and Washington on 1 July 1968 http://www.un.org/fr/disarmament/instruments/npt.shtml*

[8] *http://www.iaea.org/*