Institut de Documentation et de Recherche sur la Paix

Les cahiers de l'IDRP

Janvier 2013

IDRP - -Siège de l'ARAC, 2 place du Méridien 94807 VILLEJUIF CEDEX - http://www.institutidrp.org

A propos de la cyberdéfense

Olivier, Kempf,
maître de conférences à Sciences Po, docteur en géopolitique ([1])

Cybersécurité, ou cyberdéfense ? Ces termes sont très proches, très souvent usités l'un pour l'autre, alors pourtant qu'ils ont, probablement, des significations différentes. Le débat fait rage parmi les stratégistes et spécialistes du sujet, mais c'est un débat confus, et la couche cyber ne fait que compliquer un flou préalable, entre défense et sécurité.

Distinguer défense et sécurité

Le flou, en France, vient du Livre Blanc sur la « défense et la sécurité nationale », publié en juin 2008. L'inclusion de la sécurité dans le spectre de la défense était sensée rendre compte d'un monde plus compliqué. Un retour aux textes s'impose.

Dans le Livre blanc (LB), la finalité de l'exercice est donnée en fin d'introduction (p. 16) : Le LB « *expose une stratégie non seulement de défense, mais aussi de sécurité nationale. Son objet est de parer aux risques et aux menaces susceptibles de porter atteinte à la vie de la nation. Les menaces peuvent provenir d'États et de groupes non étatiques transnationaux. Les risques peuvent résulter de catastrophes naturelles ou sanitaires qui appellent des réponses à l'échelle mondiale. Les atteintes possibles à la vie du pays peuvent être la conséquence soit d'intentions hostiles, soit de ruptures accidentelles. Dans tous les cas, la possibilité d'une atteinte à la sécurité nationale appelle un effort d'anticipation, de prévention et de réponse rapide, mobilisant l'ensemble des moyens des pouvoirs publics et la mise en œuvre de coopérations européennes et internationales. Cette stratégie inclut donc aussi bien la sécurité extérieure que la sécurité intérieure, les moyens militaires comme les moyens civils, la politique de défense proprement dite et la politique de sécurité intérieure et de sécurité civile, la politique étrangère et la politique économique. La définition d'une stratégie d'ensemble en matière de sécurité correspond à une nécessité nouvelle, qui s'impose à la France comme à l'ensemble de ses alliés et partenaires : s'adapter aux bouleversements engendrés par la mondialisation* ».

Constatons au passage qu'il n'y a pas de distinction claire entre défense et sécurité.

C'est pourquoi il est utile de revenir à la Loi de programmation (LPM) de juillet 2009 qui donne des précisions, d'autant qu'elle modifie l'article 1 de l'ordonnance de 1959[2]. Le nouvel article 1111-1 affirme : « *La stratégie de sécurité nationale a pour objet d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République et de déterminer les réponses que les pouvoirs publics doivent y apporter ». « L'ensemble des politiques publiques concourt à la sécurité nationale ». « La politique de défense a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées. Elle contribue à la lutte contre les autres menaces susceptibles de mettre en cause la sécurité nationale* ».

On le voit, il y a beaucoup de renvois à l'introduction du LB. Si on creuse attentivement, on

1 vient de publier « *Introduction à la cyberstratégie* » (Économica) et « *Géopolitique de la France* » (Technip).

2 Le texte originel énonçait : « La défense a pour objet d'assurer en tout temps, en toutes circonstances et contre toutes les formes d'agression, la sécurité et l'intégrité du territoire, ainsi que la vie de la population. Elle pourvoit de même au respect des alliances, traités et accords internationaux. (…) ». La LPM a malheureusement supprimé cette ancienne formulation qui était plus concise et plus claire que le texte qui l'a remplacé.

s'aperçoit que la sécurité « *relève de l'ensemble des politiques publiques pour répondre aux risques et menaces* » ; et que la défense « *a pour objet d'assurer l'intégrité du territoire et la protection de la population contre les agressions armées* ».
Ainsi, selon le nouveau corpus stratégique, la sécurité remplace l'ancienne défense nationale (interministérielle) quand la défense relève simplement de la chose militaire, autrement dit du ministère de la défense.
Pour autant, ce critère organique (pour une même politique, on utilise un mot différent selon l'organe qui va la mettre en œuvre) paraît peu suffisant. En effet, la distinction entre sécurité et défense a pu recouvrir d'autres articulations :
L'une est issue de la prise en compte de la menace terroriste après le 11 septembre 2001. La sécurité lutte contre le terrorisme, la défense contre des menaces plus traditionnelles.
L'autre est également organique, mais va en dessous de l'échelon ministériel, pour s'intéresser aux agents du monopole de la violence légitime : alors, la sécurité serait chose de la police, et la défense serait le fait des armées
La distinction géographique serait similaire : la défense serait « à l'extérieur » (aux frontières ou en expéditionnaire) quand la sécurité serait « à l'intérieur », où les armées seraient presque intruses. D'ailleurs, de façon opératoire, chacun le comprend ainsi, en distinguant la « sécurité intérieure » (sans trop se poser la question de savoir qui l'opère) et la « sécurité extérieure » (où l'on a tendance à considérer naturellement que c'est plutôt l'armée qui s'en occupe.
Une dernière distinction serait causale, la sécurité étant un état (l'objectif à atteindre) quand la défense serait le moyen d'y parvenir : l'une serait statique et l'autre dynamique, la seconde serait préalable à la première. On peut même raffiner en précisant que la sécurité est un état plus particulièrement psychologique qui définit le sentiment d'un état de sûreté (au sens physique). À cette aune, la cybersécurité serait un état (souhaité, réalisé,...) et la cyberdéfense serait la mise en œuvre par une entité politique de la protection de ses intérêts
On pourra se reporter à l'excellent article du Capitaine de corvette Porcher [2008] qui s'interrogeait déjà sur les deux notions en 2008 (voir aussi l'excellent Thiéblemont, 2008). Il y montrait que l'élargissement de la défense, proposé par l'ordonnance de 1959, n'avait pas donné satisfaction. Toutefois, on peut ajouter que son remplacement par « sécurité » ne devrait pas donner plus satisfaction, surtout en l'absence de définition. D'ailleurs, l'auteur poursuivait en évoquant « *deux conceptions de la sécurité nationale* ». La première est *intravertie* (sic), « *il s'agit de la sécurité intérieure* »; « *la seconde dimension est plus globale* » et « *s'apparente à ce que les Anglo-Saxons nomment "grande stratégie" et que les Français nomment "stratégie intégrale" »*. L'auteur s'efforce alors d'expliquer que la défense est plus passive et la sécurité plus active : je dois dire qu'il ne convainc pas. Force est de constater qu'une certaine confusion demeure.
S'étonnera-t-on alors que la même confusion existe également entre les termes de « cyberdéfense » et de « cybersécurité » ?

De la cybersécurité

Constatons tout d'abord que la confusion n'est pas propre à la France. En effet, un vigoureux débat a lieu aux États-Unis sur la place respective (voire la préséance) du « *Department of Homeland Security* » (DHS : en bon français, le ministère de la sécurité intérieure) et le cybercommand : l'un défendant les organismes en .gov, l'autre les organismes en .mil, pour donner l'idée d'une limite de responsabilité. Ces noms de domaine (TLD, voir chapitre 2) dessinent des territoires, publics ou privés…, selon l'extension dans le cyberespace de l'aire de responsabilité d'un organisme. Autrement dit, la « colonisation » du cyberespace peut être le fait d'organismes publics, mais aussi privés…

Toutefois, en matière cyber, la question de la « sécurité » est compliquée par trois facteurs qui accentuent les confusions.

Ordre public

Le premier tient à l'origine « civile » du trafic sur le cyberespace même si les premiers réseaux furent créés pour des besoins militaires : ARPANET fut lancé en 1969 par la DARPA, et il se dit que l'objectif consistait à assurer la permanence des réseaux après une frappe nucléaire. Très rapidement cependant, les réseaux informatiques ont été utilisés par le grand public, et ont manié énormément de données privées. La première exigence fut alors de garantir les libertés individuelles, et d'assurer la « sécurité » des données privées qui circulaient. Cette protection fut d'abord pensée contre l'État, perçu initialement comme omnipotent et pouvant utiliser ces moyens nouveaux comme l'outil d'un contrôle totalitaire. Cela explique par exemple la création de la Commission Nationale Informatique et Liberté (CNIL) en 1978 qui doit garantir qu'il n'y a pas interconnexion des fichiers de données sur la population. Rapidement, les craintes évoluèrent, et il fallut protéger non plus seulement les citoyens, mais aussi les consommateurs contre les escroqueries rendues possibles par les réseaux (phishing, spaming, vol de numéros de carte bancaire, usurpation d'identité, …). Le public exigea une sécurité individuelle.

L'ordre public devait être assuré, et l'État qui était une sorte de menace devint simultanément une garantie. Cette double perception de l'État (ou de toute instance publique de régulation) continue de polariser les réactions des internautes. Il reste que cette préoccupation sollicita d'abord les spécialistes de cet ordre public, chargé de le mettre en œuvre : au fond, il s'agit de « policer » le cyberespace, d'où l'intérêt des services de souveraineté « intérieure » que sont la police (et la gendarmerie) et la justice (avec une dimension pénale). La cybersécurité se comprend alors comme la lutte contre la cybercriminalité. Elle suit un mouvement ascendant, venant du bas (les individus) vers le haut (la puissance publique).

Sécurité économique

Le second facteur de confusion tient aux usages économiques du cyberespace : les grandes sociétés (et les petites) voulurent également bénéficier des avantages des réseaux, qui rendaient leur activité plus aisée : que ce soit pour l'organisation de la vie interne de la société ou pour les relations avec les tiers (partenaires ou clients). Ce faisant, elles rencontrèrent rapidement le besoin de se protéger.

Pour ce cas, les menaces diffèrent légèrement. Les intrus ne cherchent pas à voler directement de l'argent, mais plutôt à espionner et à connaître à l'avance tous les prototypes et axes de recherche et de développement de la société cible. Ces pratiques touchent directement à l'intelligence économique, dans sa partie grise, voire noire. Chacun prit peu à peu conscience que l'information interne de l'entreprise (ou de l'organisation, puisque les organismes publics firent face aux mêmes difficultés) a de la valeur, et qu'elle constitue un actif qui doit être protégé comme tel.

Sécurité des systèmes d'information (SSI)

Le troisième facteur est technologique. En effet, les directeurs informatiques des entreprises et des administrations virent émerger une tâche supplémentaire. Ils devaient non seulement gérer le parc informatique de leur société (machines, réseaux, infrastructures logicielles, logiciels propriétaires, suivi des évolutions techniques, …) mais aussi assurer une fonction supplémentaire, celle de la sécurité des systèmes informatiques. Cela favorisa le

développement de la sécurité des systèmes d'information (SSI). Le mot sécurité est ici approprié, nul n'en doute. Toutefois, si la SSI appartient incontestablement à la cybersécurité, on ne peut réduire la cybersécurité à la SSI, ni même à une SSI de niveau étatique.

Ainsi, la cybersécurité reprend ces trois significations : sécurité publique (au sens d'ordre public[3]), sécurité économique (au sens de protection économique) et sécurité technologique (au sens de la SSI). La cybersécurité serait alors, au minimum, la somme de ces trois dimensions.

De la cybersécurité à la cyberdéfense et la cyber-guerre.

Dès lors, on peut préciser l'approche cyberstratégique en distinguant les champs qu'elle recouvre.

Cybersécurité

Une partie traite de la sécurité intérieure, et ressort d'une police générale (même si des moyens militaires peuvent être utilisés) : au sens propre, c'est le champ de la cybersécurité. L'État en est responsable et utilise pour cela des organismes interministériels ou dépendant d'un ministère particulier (ministère de l'intérieur ou ministère de l'économie). Cette cybersécurité comprend notamment les trois aspects de police, de protection économique et de sécurité technologique, mais peut se préoccuper de politique industrielle ou de la protection des grands réseaux de service public. Elle ambitionne de protéger les individus, les entreprises mais aussi toutes les organisations publiques et collectivités territoriales.

Cyberdéfense

L'autre partie traite de la sécurité extérieure, la cyberdéfense proprement dite. Elle met en œuvre une politique de cyberdéfense qui a une dimension interministérielle, même si elle est logiquement concentrée au sein du ministère de la défense et de plusieurs de ses services. Elle organise la lutte informatique défensive et offensive, la protection des troupes et des services essentiels à la souveraineté de l'État, et touche à l'espionnage et au contre-espionnage. Elle prépare une éventuelle cyber-guerre.

Cyberguerre

Le mot de cyber-guerre. est régulièrement utilisé par les journalistes, d'autant plus fréquemment qu'ils n'y connaissent rien, ni à la guerre ni au cyberespace. Les spécialistes des deux domaines sont beaucoup plus réticents envers ce mot ou, pour être plus précis, envers ses abus.

La perception traditionnelle de la guerre suggère l'existence de morts. Certains experts estiment que le seuil de 1000 morts permet de caractériser un événement du nom de « guerre ». Or, jusqu'à présent, aucun acte hostile dans le cyberespace n'a jamais provoqué 1000 morts ! Toutefois, la possibilité reste ouverte : la dérégulation d'un système de contrôle d'une centrale nucléaire pourrait provoquer son emballement et son explosion ; la mise hors service d'un réseau de distribution d'eau pourrait lever tous les contrôles sanitaires et envoyer de l'eau contaminée. Beaucoup d'exemples viennent à l'esprit. Mais ils n'ont pas eu lieu. Cela conduit à relativiser cette notion de cyber-guerre.

3 Notons que la cryptologie était l'apanage de l'État régalien. Elle est devenue aussi privée, puisqu'elle est nécessaire à la sécurité de nombreuses transactions. Il y a ainsi une sorte de concurrence (de course technologique) entre la cryptologie publique (souveraineté) et la cryptologie privée.

Elle est pourtant valide, de deux façons.

La première tient à la dimension cybernétique que comprendra désormais toute guerre, qu'elle soit conventionnelle ou nucléaire. À partir d'aujourd'hui, une guerre sera forcément une cyber-guerre.

La deuxième tient à la relativisation de la létalité. Il y a aujourd'hui plus de mille morts par an pour cause d'homicide par arme à feu aux États-Unis. De même, aux frontières de l'Europe, il y a plus de 1000 immigrants clandestins qui meurent chaque année dans leur tentative de rejoindre leur destination. Pourtant, la plupart des Américains et des Européens n'a pas le sentiment d'être « en guerre ». Pour beaucoup d'entre eux, à tort ou à raison, il ne s'agit là que des conséquences d'un ordre public nécessaire à la bonne vie en société.

Simultanément, le cyberespace présente l'opportunité de mener facilement des actions offensives. De ce point de vue, un cyberconflit (le mot est peut-être plus adéquat) se déroule déjà dans le cyberespace. Il n'occasionne pas (encore) de morts, mais il est de plus en plus virulent, notamment au Proche- et au Moyen-Orient où il s'articule à une conflictualité préexistante, et fort vive. De plus, on ne peut exclure le phénomène d'escalade de la violence (et il faut bien constater une augmentation des incidents à résonance politique). Dès lors, il est possible de parler de cyberconflit, voire de « cyber-guerre. » pour désigner des actions hostiles menées dans le cyberespace par des États pour résoudre par la violence (maîtrisée) leurs conflits.

Notons en incise que l'État est ici le critère de la « guerre » : la notion de « guerre privée » renvoie à des conflits de possession de territoire non soumis à des souverainetés étatiques. Les autres conflits dans le cyberespace relèvent plus de la cybersécurité que de la cyberdéfense.

La cyberpaix : un thème stratégique marginal

Daniel Ventre,
Ingénieur au Centre national de la recherche scientifique (CNRS),
chercheur au Centre de recherche sociologique
sur le droit et les institutions pénales (CESDIP) [4]

En conclusion d'un article publié récemment dans la revue *Foreign Policy*, John Arquilla[5] évoquait la nécessité de rechercher les moyens d'une cyberpaix, sans toutefois la définir. Un premier constat s'impose : les recherches sur la paix font peu de cas du concept ; et les rares occurrences du sujet se trouvent plus généralement dans la presse Internet[6]. La cyberpaix est néanmoins l'objectif de quelques initiatives internationales œuvrant dans le champ de l'action humanitaire ; on parle alors plus volontiers de l'utilisation des nouvelles technologies de l'information et de la communication (TIC) dans la construction de la paix. Mais globalement, la cyberpaix suscite un bien moindre intérêt que la cyberguerre, le cyberconflit ou la cyberdéfense[7]. Si le traitement de la guerre appelle le plus souvent des réflexions sur la paix – ou inversement – en associant les deux concepts en un couple indéfectible, l'un étant considéré comme le contraire ou le complément de l'autre, l'un succédant à l'autre, les réflexions sur le cyberconflit n'appellent pas de manière aussi systématique de considérations sur la cyberpaix.
Nous proposons dans cet article une synthèse des quelques considérations émises sur la cyberpaix et verrons si les définitions et théories afférentes recoupent celles portant sur la paix.

Définir la cyberpaix

Nous avons ainsi identifié trois acceptions principales du concept de cyberpaix.

Tout d'abord, la cyberpaix est l'état de paix (absence de cyberguerre) qui doit être préservé, en raison des menaces de destruction et de perturbation que fait peser la cyberguerre sur la société. La cyberpaix doit être donc l'empêchement de la cyberguerre.
Le concept de « cyberpaix » fut utilisé lors du Forum sur la gouvernance de l'Internet en 2009, et plus récemment par Hamadoun I. Touré, Secrétaire général de l'Union internationale des télécommunications (UIT), dans un rapport publié en janvier 2011[8], où l'introduction du concept est motivée par la crainte des perspectives de destructions et de souffrances d'une éventuelle cyberguerre. La démarche de l'UIT vise à établir un « ordre

4 cet article est paru dans le numéro d'automne de la Revue Internationale et Stratégique, nous remercions l'auteur et l'IRIS d'avoir permis sa reproduction..
5 John Arquilla, " Cyberwar is already upon us ", *Foreign Policy*, mars-avril 2012, p. 84-85.
6 Lucy Sherriff, " Pentagon pleas for cyber peace fall on deaf ears ", The Register, 9 août2000, http://www.theregister.co.uk/2000/08/09/pentagon_pleas_for_cyber_peace/
Bruce Sterling, " Cyberwar and Cyberpeace Treaties ", Wired Magazine, 2 février 2010, http://www.wired.com/beyond_the_beyond/2010/02/cyberwar-and-cyberpeace-treaties/
7 Thomas Rid, " Think Again: Cyberwar ", *Foreign Policy*, mars-avril 2012, http://www.kcl.ac.uk/sspp/departments/warstudies/people/readers/rid.aspx
8 Dr. Hamadoun I. Touré, *En quête de cyberpaix*, UIT, janvier 2011, 152 p.
http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-F.pdf

universel du cyberespace [9]» fondé sur le principe selon lequel « la cyberpaix doit être l'objectif auquel s'efforcent de parvenir toutes les nations [10]». Dans ce même rapport, Henning Wegener (diplomate allemand) définit la cyberpaix par opposition aux notions qu'il qualifie de « négatives » (cyberguerre, cyberterrorisme, cybercriminalité)[11].
Les responsables du projet Impact (International Multilateral Partnership Against Cyberthreats) travaillent eux aussi à la promotion de la cyberpaix dans le cyberespace.

La deuxième acception relève d'une pérennisation d'une cyberstabilité permettant le développement de l'économie et de la connaissance.
La World Federation of Scientists (WFS) publia en 2009 la « Déclaration d'Erice sur les principes régissant la cyberstabilité et la cyberpaix [12]». Le constat initial de cette déclaration expose le caractère paradoxal des TIC, qui, d'une part participent à la croissance économique et sont des vecteurs d'accès et de partage de la culture et de la connaissance, et d'autre part présentent des risques et des menaces potentielles pour les droits des utilisateurs (vie privée, liberté d'expression, de conscience, de religion, etc.). L'état de cyberpaix implique une utilisation avertie et précautionneuse des nouvelles technologies afin d'éviter conflits, actes de criminalité et violations des droits humains/fondamentaux en tout genre.

Enfin, le concept de cyberpaix prône l'utilisation des TIC dans les opérations de (re)construction de la paix[13]. Permettant le rapprochement des peuples, la compréhension des cultures, l'expression des identités, ces outils facilitent l'action humanitaire en favorisant la coordination, la communication et l'échange de données. À la fin des années 1990, le projet Tech4peace[14] – cofinancé notamment par les Nations unies et l'association Fulbright de l'United States Agency for International Development (USAID) – visait à rapprocher les communautés chypriotes. Puis en 2007, le ministère des Communications et des technologies de l'information égyptien initia le projet Cyber Peace Initiative[15] afin de renforcer les liens culturels et nationaux entre les jeunes générations. Ainsi, sites et réseaux sociaux s'avèrent être des instruments usuels et facilitant la mise en relation des individus, le partage d'informations, la promotion de la culture de la paix et la prévention des conflits.

De la définition de la cyberpaix à sa mise en pratique

Préserver l'absence de cyberguerre

Lassées par les atteintes incessantes dont elles sont victimes (les États-Unis ne cessent de dénoncer les intrusions russes et chinoises dans leurs entreprises et institutions depuis une vingtaine d'années) et par la menace de potentielles cyberattaques qui détruiraient ou paralyseraient leurs infrastructures vitales, certaines nations évoquent la possibilité de

9 *Ibid.*, p. 108.
10 *Ibid.*, p. 24.
11 *Ibid.*, p. 89-98.
12 World Federation of Scientists, *Déclaration d'Erice sur les principes régissant la cyberstabilité et la cyberpaix*, août 2009, www.ewi.info/system/files/Erice.pdf
13 Jonas Hartelius, *Making Peace after Cyber War*, 13 décembre 2011.
14 http://www.tech4peace.org/nqcontent.cfm?a_id=1
15 http://projects.tigweb.org/CYBERPEACE?langrand=1523037576 ; Arab Republic of Egypt, Ministry of Communications and Technology, *Cyber Peace Initiative*, mars 2008, 16 p.

répondre de manière conventionnelle (diplomatique, économique tout d'abord, militaire ensuite), ou non conventionnelle (c'est-à-dire répondre à des cyberattaques par des cyberattaques). Le cyberespace serait ainsi non plus seulement un outil, mais une cause de la guerre.

L'enjeu est donc d'éviter que le cyberespace ne devienne une zone de guerre, mais aussi qu'il ne devienne un casus belli. Comment y parvenir alors que les nations industrialisées majeures se sont engagées sur la voie de la militarisation du cyberespace élaborent politiques et stratégies de cyberdéfense (défensives et offensives), et ont déjà eu, pour certaines d'entre elles, l'occasion d'user de leurs capacités de cyberagression ?

Empêcher la cyberguerre passerait par des mesures juridiques (définir l'acte de guerre ; contrôler le développement et encadrer l'utilisation des cyberarmes), techniques (systèmes sûrs) et politiques (coopération internationale, traités, codes de bonne conduite, prise de conscience des risques majeurs d'une cyberguerre). Certains estiment ainsi nécessaire la limitation de la course au cyberarmement par l'élaboration d'un cadre juridique international pour le développement de ces armes, ou par l'augmentation de leur coût d'accès[16]. Mais contrairement aux armes conventionnelles, ni la première solution ni la seconde ne semblent aujourd'hui applicables[17].

Dans le chapitre « Cyber Peace [18]» de son ouvrage « Cyber War: the Next Threat to National Security and What to Do About It », Richard Clarke soulève la question du contrôle du développement et de la prolifération à l'échelle internationale des cyberarmes. L'idée de leur contrôle fut initialement proposée par la Russie qui s'est faite, à l'échelle internationale, la porte-parole d'un projet de convention internationale. Ce dernier, perçu comme un outil de propagande[19] a été rejeté par les États-Unis, sous l'Administration Clinton puis aujourd'hui celle de Barack Obama. Les Américains estiment que la vérification de la mise en œuvre d'un tel contrôle, la validation de l'efficacité et de la réalité de la mise en application d'une telle régulation, s'avèrent impossibles. En 2010, R. Clarke estime toutefois que la situation n'est plus la même, et qu'il est temps de réfléchir au contrôle des cyberarmes. Une vingtaine de pays (non cités dans l'ouvrage) se sont selon lui dotés d'unités de cyberguerre offensive, ce qui n'était pas encore le cas dix ans plus tôt. Mais cela nécessiterait tout d'abord de s'interroger sur l'efficacité attendue d'un accord international sur le sujet.

Très vulnérables face aux cyberattaques, les États-Unis ont grand intérêt dans l'instauration de contrôle et de limitation des cyberarmes : aucune autre nation au monde, affirme toujours R. Clarke, n'est aussi dépendante du cyberespace que les États-Unis (tous les secteurs d'activité sont informatisés/connectés : distribution d'énergie, transports, système financier, gouvernement, éducation, armées) ; les systèmes essentiels vitaux pour le pays sont la propriété du secteur privé ; nulle part ailleurs dans le monde ces opérateurs privés ne sont aussi puissants d'un point de vue politique (lobbying, contributions aux financements des campagnes politiques par exemple) ; l'armée américaine est très vulnérable aux cyberattaques (l'asymétrie est flagrante : en 2009 les insurgés irakiens ont utilisé un logiciel coûtant 26 dollars pour intercepter les vidéos transmises par un drone Predator coûtant des millions de dollars)[20]. R. Clarke examine la question de l'intérêt d'une politique internationale de contrôle

16 Craig Eisele, *Striking a Balance between Cyber War and Cyber Peace*, 21 avril 2012, http://craigeisele.wordpress.com/2012/04/21/striking-a-balance-between-cyber-war-and-cyber-peace/

17 Dorothy Denning, *Obstacles and Options for Cyber Arms Control*, 22 juin 2001, 13 p., http://faculty.nps.edu/dedennin/publications/berlin.pdf

18 Richard A. Clarke, Robert K. Knake, *Cyber War, The next threat to national security and what to do about it*, New York, Harper Collins Publisher, 2010, 290 p.

19 *Ibid.*, p. 220.

20 Siobhan Gorman, Yochi J. Dreazen, August Cole, " Insurgents Hack U.S. Drones ", *The Wall Street Journal*,

des cyberarmes en ne considérant que le seul point de vue étatsunien et conclut que le traité ne serait utile que s'il permettait aux États-Unis de conserver un avantage sur les autres nations.

Au-delà des interrogations portant sur le contrôle des armes elles-mêmes et l'efficacité des traités internationaux, c'est la question de l'interdiction des opérations de cyberespionnage[21] qui est soulevée, et plus largement celle de l'interdiction de la cyberguerre, des attaques contre les civils ou les infrastructures critiques (à commencer par le secteur bancaire[22]). Cela implique aussi une réflexion nécessaire sur l'utilité, l'efficacité et la faisabilité des mesures visant à réguler, interdire ou contrôler le développement et l'utilisation des cyberarmes (doit-on imaginer des inspecteurs dans le cyberespace ?[23]). Aux États-Unis, le principe d'un contrôle ou d'une limitation des cyberarmes ne semble plus être envisagé en 2012. Au regard des investissements ouvertement consacrés à leur production, le département de la Défense américain a attribué en 2012, 500 millions de dollars à l'Agence pour les projets de recherche avancée de défense (DARPA). D'autres nations se sont également officiellement lancées dans des programmes de développement des cyberarmes. Par exemple le Japon, distinguant cyberarmes défensives et offensives (en raison notamment de contraintes juridiques) a initié un projet créant une solution technologique (autrement dit une arme) capable de neutraliser les cyberattaques, de tracer leur chemin et d'identifier les sources[24].

Dans le cyberespace, d'autres facteurs contribuent cependant à limiter les capacités d'attaques stratégiques et retiennent le bras armé des agresseurs potentiels : les risques d'effets non recherchés, l'absence de maîtrise des impacts des attaques, la complexité même des systèmes. Se référant à l'accident du 17 août 2009 survenu dans la centrale hydroélectrique de Sayano-Shushenskaya (Russie), Thomas Rid[25] nous rappelle que cette catastrophe industrielle est le résultat d'une succession complexe et unique d'événements (il n'y a d'ailleurs aucune cause « cyber » dans cet accident). Il estime que produire un effet similaire à l'aide d'une cyberattaque supposerait d'anticiper toutes les vulnérabilités qui pourraient être déclenchées en cascade, rendant l'exercice d'une complexité extraordinaire pour des acteurs internes, à plus forte raison pour des agresseurs externes. Un « cyber Pearl Harbor » ne serait donc sans doute pas si imminent que le discours veut bien le laisser penser. La cyberpaix, que viendrait rompre un acte de cyberguerre, pourrait donc être maintenue tant que la complexité ne sera pas maîtrisée. Stuxnet, présenté comme une attaque étatique américaine contre le programme nucléaire iranien, n'est-il pas cet acte qui vient rompre la cyberpaix jusqu'alors maintenue ?

Pour Les Bloom et John E. Savage[26] assurer la cyberpaix c'est éviter les attaques. La paix ne signifie pas ici une absence de guerre, mais surtout une préservation contre les attaques, et leurs effets, une prévention des coups pouvant être portés contre des cibles et/ou contre la société via le cyberespace. Les auteurs proposent quelques solutions pour parvenir à cette paix-sécurité : la dissuasion tout d'abord, reposant sur une attitude ferme dans la lutte contre les risques nationaux et internationaux ; le développement d'un arsenal significatif (technique et juridique) ensuite ; la coopération internationale enfin. Cette posture appelle donc à la cyberpaix par la cyberforce[27].

17 décembre 2009, http://online.wsj.com/article/SB126102247889095011.html#printMode

21 *Ibid.* p. 228.

22 *Ibid.* p. 238-245.

23 *Ibid.* p. 247-255.

24 Yomiuri Shimbun, *Government working on defensive cyberweapon. Virus can trace, disable sources of cyberattacks*, 3 janvier 2012. http://www.yomiuri.co.jp/dy/national/T120102002799.htm

25 Thomas Rid, Marc Hecker, *War 2.0: Irregular Warfare in the Information Age*, Praeger Security International, 2009.

26 Les Bloom, John E. Savage, *On Cyber Peace*, Atlantic Council, août 2011, 8 p. http://www.acus.org/files/publication_pdfs/403/080811_ACUS_OnCyberPeace.PDF

27 Alan W. Dowd, *Cyber-P*eace through Cyber-Strength, 16 mars 2011, http://frontpagemag.com/2011/03/16/cyber-peace-through-cyber-strength/

L'approche juridique du maintien de la cyberpaix, c'est-à-dire l'interdiction d'utiliser le cyberespace à des fins guerrières inscrite dans des traités ou codes de bonne conduite, se confronte quant à elle à au moins deux obstacles. Premièrement, les États ne sont pas les seuls à utiliser la dimension cybernétique pour se battre (pluralité d'acteurs, parmi lesquels certains ignorent le droit international), et deuxièmement l'interdiction n'aurait de force que si les garants de la paix avaient les moyens de sanctionner les contrevenants (et pour cela les moyens de les identifier).

Permettre l'utilisation paisible du cyberespace

L'objectif de cyberpaix défini par la WFS – assurer aux sociétés l'usage paisible et bénéfique du cyberespace en empêchant ou limitant les effets du cyberconflit, de la cybercriminalité et des actes portant préjudice aux droits fondamentaux des individus – ne peut prendre assise que dans les sociétés démocratiques : les États doivent s'assurer que la loi garantit la libre circulation des informations et des idées dans le cyberespace ; tous les États devraient travailler à l'élaboration d'un code de bonne conduite ; utilisateurs, fournisseurs de services, gouvernements doivent veiller à protéger les utilisateurs les plus vulnérables (les jeunes par exemple) ; il leur faut également renforcer la protection de la vie privée par le déploiement de solutions technologiques sûres (empêchant l'interception des données personnelles par exemple) respectant des standards internationaux ; les gouvernements doivent participer aux efforts des Nations unies afin d'éviter l'utilisation du cyberespace pour le conflit. La cyberpaix est donc entre les mains de tous les acteurs : entreprises, citoyens, institutions, initiatives publiques/privées, mais principalement des gouvernements (dans un cadre de coopération internationale). Les principaux outils sont juridiques[28], techniques (applications sécurisées) et politiques (convaincre ou contraindre les États à garantir la libre circulation des informations).

Cependant, la cyberpaix semble difficilement atteignable car au-delà des limites du droit et des moyens des acteurs sécuritaires, un consensus sur ce qui doit être protégé fait également défaut. La Déclaration de la WSF, tout comme le projet de Traité de cyberpaix ou tout autre projet de code de bonne conduite, repose sur un principe – la libre circulation des idées sans contrainte de frontières – qui n'est pas partagé par tous les acteurs de la scène internationale[29] . Pour les États-Unis et l'Occident, la menace est celle de cyberguerre ; pour la Russie et la Chine la menace est avant tout informationnelle (la menace relève de la guerre de l'information). Le terme « cyber » n'apparaît d'ailleurs pas dans les résolutions proposées par la Russie à l'Assemblée générale des Nations unies. L'approche russe ou chinoise justifie, de leur point de vue, censure et contrôle[30]. Les risques de déstabilisation pouvant venir des idées et de l'information, il n'est pas question d'adhérer au principe de libre circulation des idées sans contrainte de frontière. Le projet de cyberpaix de l'UIT impliquerait de concilier les visions opposées de l'Occident et de la Russie/Chine.

28 Scott Shackelford, *Cyber Peace: Managing Cyber Attacks in International Law, Business, and Relations*, Cambridge University Press, 2012.

29 Bruce Sterling, " Cyberwar and Cyberpeace Treaties ", *Wired Magazine*, 2 février 2010, http://www.wired.com/beyond_the_beyond/2010/02/cyberwar-and-cyberpeace-treaties/

30Tom Gjelten, " Shadow Wars: Debating Cyber Disarmament ", *World affairs*, décembre 2010, http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament

Conclusion

La cyberpaix actuelle est-elle une « cyberpaix armée », entendue comme période de paix pendant laquelle des États se livrent à la course aux armements (le cyberconflit n'est ni parfaitement défini ni certain, mais les principales nations industrialisées se sont engagées dans un processus de développement capacitaire cyberdéfensif et offensif) en prévision d'un conflit[31] ?

La définition de la cyberpaix, dépend étroitement de celle de la cyberguerre. Or nous le savons, il y a au moins deux acceptions du terme : la cyberguerre strictement limitée à la dimension cybernétique de la guerre, et la définition plus large qui considère les attaques menées contre les infrastructures critiques (systèmes de distribution d'énergie, transports, systèmes financiers), voire la seule menace de ces attaques potentielles, comme constitutives d'un état de cyberguerre.

- Si la cyberguerre est un conflit armé dans lequel au moins l'un des belligérants est un acteur étatique légitime, la cyberpaix peut être définie comme l'absence de cyberguerre : soit une guerre se déroulerait sans cette dimension cybernétique (la non sollicitation du cyberespace dans un conflit, maintiendrait celui-ci en état de paix) ; soit la cyberpaix est conditionnée à l'absence de guerre (toute guerre ayant une dimension cybernétique). La cyberguerre n'a pas nécessairement pour objectif la cyberpaix.
- Si la cyberguerre est définie par les menaces/attaques contre les infrastructures critiques, contre les intérêts étatiques, alors il faut définir un seuil d'acceptabilité qui marque la frontière entre paix et conflit.

Les récentes divulgations sur la paternité et l'objectif de Stuxnet, attribuant l'attaque aux États-Unis et à Israël dans une opération conjointe contre l'Iran, démontrent qu'un pas vient d'être franchi dans l'utilisation agressive du cyberespace par les États. Cette nouvelle lecture du problème souligne l'existence de relations entre l'État agresseur et les pays tiers, parfois alliés, victimes des effets collatéraux de l'opération (dans le cas de Stuxnet, la propagation du ver dans de nombreux pays peut être considérée comme un dommage collatéral). Ces derniers peuvent réagir, exiger réparations, explications, voire lancer des cyberattaques (s'estimer en droit de légitime défense) ; l'agresseur a une responsabilité vis-à-vis de ces États. C'est de cet enchaînement d'effets et de conséquences que peuvent naître de nouvelles situations conflictuelles. L'attaque n'a pas été menée dans un contexte de guerre, elle confirme les capacités existantes en matière d'attaques contre des infrastructures critiques, elle illustre la faisabilité de telles opérations. Elle ne peut que relancer les débats sur l'urgence qu'il y a à légiférer sur le contrôle de l'utilisation des cyberarmes et de leur développement.

Nous pourrions alors imaginer une cyberpaix fondée sur le principe de puissance, reprendre la typologie aronienne[32] qui distingue paix d'équilibre (forces en balance), d'hégémonie (forces dominées par l'une d'entre elles) et d'empire (forces surclassées par l'une d'entre elles, avec perte d'autonomie des unités élémentaires). La cyberpaix pourrait reposer sur le principe de la dissuasion : mais la cyberdissuasion est-elle seulement possible ?

31 Centre national de ressources textuelles et lexicales, http://www.cnrtl.fr/definition/paix

32 Raymond Aron, *Paix et guerre entre les nations*, Paris, Calmann-Lévy, janvier 2004, p. 158