Networks and Communication Studies
NETCOM, vol. 27 (2013), n° 3-4
pp. 293-308

Publié et imprimé en octobre 2014

FRAGILITE DU GEOCYBERESPACE A L'HEURE DES CONFLITS CYBERNETIQUES

Digital Conflicts and the Fragility of Geocyberspace

BAKIS HENRY

Résumé *- Alors que les actes d'hostilité cybernétique se multiplient à travers le monde et que la course aux armements cybernétiques s'accélère. Cela met en lumière la vulnérabilité des TIC à toutes les échelles. Malgré l'importance du problème posé, le contrôle efficace de la sécurité de l'Internet soulève de grandes difficultés (politiques, législatives et techniques). Cette note est une introduction à l'article suivant dû à E. M. Roche & M. J. Blaine, article qui se conclut sur un appel à la signature d'une Convention internationale de désarmement cybernétique.*

Mots clés *– Armes ; Convention Internationale ; Cyberespace ; Electronique ; Etats ; Géopolitique ; Information ; Internet ; Réseaux ; Vulnérabilité.*

Abstract *- While acts of cyber hostility are increasing around the world, the cyber armaments race continues. This highlights the vulnerability of ICT in every dimension. Despite the urgency of the problem, effective control of Internet security poses real challenges (political, legal and technical). This note is an introduction to the following paper (Roche & Blaine) which calls for the signing of an international convention on cyber disarmament.*

Key words *– Cyberspace ; Electronics ; Geopolitics ; Information ; International Convention ; Internet ; Networks ; States ; Weapons ; Vulnerability.*

Dans les années 70, l'approche géopolitique a été réhabilitée après le travail préparatoire de Jean Gottmann (1952)[1] et suite au travail pionnier d'Yves Lacoste (1976)[2] et de Paul Claval (1978)[3] en France. Avec l'affirmation du rôle des TIC dans le monde contemporain, l'étude géographique[4] et géopolitique des armements, des conflits et des politiques de défense, un nouveau chapitre s'ouvre à côté de ceux relatifs à l'étude des complexes militaro-industriels, du rôle nouveau des armes conventionnelles et des guérillas dans les confits récents, de la géostratégie nucléaire… Mais la géopolitique de l'information[5], de la communication et des médias[6] n'a pas connu l'essor qu'on aurait pu attendre. Si plusieurs géographes se sont intéressés à ce thème depuis vingt-cinq ans, c'est Frédérick Douzet[7] qui a principalement exploré la thématique de la fragilité de l'espace cybernétique dans plusieurs articles significatifs. Sur le plan académique, l'irruption des TIC dans l'espace géographique conduit à renouveler plusieurs concepts de la géographie ou des sciences politiques[8] : dont ceux de frontière, et de souveraineté.

La souveraineté dans l'espace cybernétique est l'objet de rivalités puissantes entre de nombreux acteurs, notamment privés (les grandes transnationales en

Cet article a été publié et imprimé en octobre 2014

[1] Voir son ouvrage : *La politique des Etats et leur géographie* (1952).

[2] Voir son ouvrage : *La géographie ça sert d'abord à faire la guerre* (1976) et surtout par la création de la revue *Hérodote* (1976).

[3] Voir ses ouvrages : *Espace et pouvoir* (1978); *Géopolitique et géostratégie : la pensée politique, l'espace et le territoire au XX^e siècle* (1994).

[4] Jacques Soppelsa (1980). *Géographie des armements.*

[5] Voir : nos publications

- (1979), *Réseaux d'entreprises et effets induits par l'utilisation des télécommunications dans les organisations. Une étude de cas: les communications internes d'IBM,* septembre, 138 p., voir la conclusion, Rapport CNET-MRC, Issy les Moulineaux ;
- (1983), *Télécommunications et organisation de l'espace*, Thèse d'Etat, vol. 2 (Partie IV, section II, 3 « Considérations sur la vulnérabilité nouvelle qu'introduisent les systèmes de télécommunications sophistiqués », pp. 1127-1147, Atelier National de Reproduction des Thèses, Université de Lille III;
- (1987), *Géopolitique de l'information,* PUF ;
- (1991), « La télégraphie sémaphorique sur le littoral français », in *L'Information historique*, rubrique « recherche historique », vol. 53, n° 1, pp. 27-39.

[6] Philippe Boulanger (2014), *Géopolitique des médias, Acteurs, rivalités et conflits*, Paris, A. Colin, collection U, 2014, 310 p.

[7] Frédérick Douzet est Professeur à l'Institut français de géopolitique. Voir notamment : F. Douzet (1997 ; 2009 ; 2013 ; 2014).

[8] Les sciences politiques s'intéressent de plus en plus à cette thématique, et notamment l'une de ses branches, l'étude des relations internationales.

particulier). On le comprend lorsqu'on en cerne les enjeux : « Contrôler le cyberespace, c'est avoir l'œil sur les milliards de messages qui circulent entre les utilisateurs du monde entier, c'est l'accès à des bases de données en tout genre sans cesse actualisées, c'est la surveillance des transactions commerciales et financières, c'est la possibilité d'une politique agressive de diffusion massive d'information ou de désinformation, c'est aussi l'accès à tous les réseaux qui y sont reliés, aux satellites de communications, aux ordinateurs personnels connectés, et tout ce qui peut sortir de l'imagination de programmeurs particulièrement inventifs, c'est enfin l'assurance de gagner énormément d'argent en gérant son développement »[9]. On le comprend lorsque l'on sait que la Maison Blanche a reçu un rapport estimant qu'il y a une certitude : au cours des deux prochaines années, une cyberattaque majeure contre les infrastructures critiques américaines « pourrait avoir des répercussions sur le long terme »[10]. Dans le même ordre d'idées, le secrétaire général de l'OTAN a déclaré que la protection des réseaux informatiques de l'Alliance atlantique en cas de cyber-attaques constituait un problème sérieux car qui pouvait avoir « des conséquences dévastatrices »[11].

Aujourd'hui, le développement de la course aux armements cybernétiques risque d'empêcher le fonctionnement des réseaux et services de TIC, ce qui met en lumière la vulnérabilité des TIC en général et de l'espace cybernétique à toutes les échelles. Cela risque d'empêcher plus ou moins fortement la circulation de l'information et, en conséquence, de perturber la gouvernance des Etats et leur souveraineté, de gravement obérer le rôle de ces réseaux sur l'économie, la société ou la culture au point de contrarier les avancées en matière de développement et les multiples applications inséparables de l'usage des TIC.

[9] F. Douzet (1997), « Les enjeux géopolitiques du cyberespace », *Netcom*, vol. 11, n° 1, pages 206-207.

[10] USA. Departement of Defense (2013). Et : « Barack Obama : certaines cyberattaques chinoises sont soutenues par l'Etat », *01net.com*, 2013.

[11] *01net.com* (2014), 4 sept..

LA VULNERABILITE CYBERNETIQUE

L'article de Roche et Blaine a été publié en langue anglaise il y a quelques mois dans la revue *Orbis,* Revue du *Foreign Policy International Institue*[12]. La rédaction de *Netcom* a obtenu l'exclusivité d'une traduction en langue française car le thème traité concerne au plus haut point non seulement les réseaux de communications en général, mais aussi les infrastructures informationnelles localisées.

Le projet des auteurs est de convaincre les décideurs et sensibiliser l'opinion sur le point suivant. Aussi simple que fondamental : le développement rapide d'armes cybernétiques potentiellement dévastatrices fait que les armes cybernétiques peuvent avoir des effets si dévastateurs que certains les considèrent comme des armes de destruction massive[13].

Ces mots peuvent sembler excessifs, pourtant, le monde est devenu tellement dépendant des réseaux de la communication électronique que l'on n'ose plus penser le fonctionnement économique, social, culturel sans eux : centralité de l'Internet et de ses multiples applications; rôle incontournable des systèmes de localisation par GPS pour le transport ; pilotage des grands réseaux techniques d'infrastructures urbaines par les télécommunications (sondes, télécommandes); etc. Sans aller jusqu'à de telles extrémités, la délinquance cybernétique parvient déjà à troubler ou partiellement compromettre le fonctionnement continu d'entreprises ou d'administrations d'Etats. Il a été remarqué que l'espace cybernétique est « le lieu d'expression des passions humaines où le pire côtoie le meilleur. Pilier du développement économique, argument de puissance, le cyberespace s'affirme comme un milieu d'importance vitale pour les États et devient progressivement un nouveau champ d'affrontements»[14].

D'autres acteurs peuvent trouver avantage à la fragilité de l'espace cybernétique, lorsqu'ils entendent réagir à l'encontre d'Etats ou d'institutions dont ils contestent les politiques d'opacité informationnelle. Depuis 2006, le site WikiLeaks, très controversé, s'est fait connaître pour porter à la connaissance du public des documents confidentiels d'Etats. Il a publié aussi des informations sur la dangerosité

[12] Institut fondé en 1955 par le Pr. Robert Strausz-Hupé qui a dit un jour les mots suivants « une nation doit penser avant d'agir » (*A nation must think before it acts*) qui inspirent toujours cet institut et sa revue.

[13] Les auteurs citent : James P. Farwell, Rafal Rohozinski (2009), pp. 31-36 ; Richard Brust (2012), p. 40 ; Samuel Greengard, (2010), pp. 20-22 ; Thomas Zeitzoff (2011), p. 938 (voir les références complètes à la fin de l'article de Roche & Blaine).

[14] Bertrand Boyer (2012).

connue de centrales nucléaires japonaises, bien avant la catastrophe de Fukushima (2011)[15].

Alors que les actes d'hostilité cybernétique se multiplient à travers le monde, divers grands Etats ont mis sur pied des unités spécialisées opérationnelles et des structures de commandement, équipées d'outils de défense et d'attaques cybernétiques. La course aux armements cybernétiques s'accélère. Le Royaume-Uni a investi 580 millions d'euros pour sa défense cybernétique sur 4 ans alors qu'en Allemagne ce sont 500 personnes dont les activités sont directement dédiées à la défense cybernétique [16]. L'Alliance Atlantique qui subit environ 100 attaques cybernétiques par jour[17] en a tiré les conséquences. En 2008, elle a officiellement souligné lors de son sommet de Bucarest « la nécessité pour l'Otan et pour les pays de protéger les systèmes d'information clés… et de mettre en place une capacité visant à aider, sur demande, les pays de l'Alliance à contrer les cyberattaques ». En 2010, elle a été plus loin, intégrant la notion de guerre cybernétique dans son nouveau concept stratégique[18].

[15] Un « câblogramme diplomatique américain » dont a eu connaissance le réseau Wikileaks a révélé « qu'un expert de l'Agence internationale de l'énergie atomique (AIEA) s'était inquiété de ce que les réacteurs japonais n'étaient conçus que pour résister à des séismes d'une magnitude de degré 7. Selon ce même document, le responsable de l'AIEA avait indiqué lors d'une réunion du « Groupe sur la sûreté et la sécurité nucléaires » du G8 à Tokyo en 2008, que les critères de sécurité du Japon étaient obsolètes. Un autre câble de 2006 indique que le gouvernement japonais s'est opposé à l'ordre d'un tribunal de fermer une centrale dans l'ouest en raison de doutes sur sa résistance à un séisme. L'Agence de sécurité nucléaire et industrielle du Japon avait estimé que le réacteur était « sûr » et que « toutes les analyses sur sa sécurité avaient été effectuées de façon appropriée » (Wikileaks, cité par « Les centrales japonaises, 'un problème sérieux' pour l'AEIA, révèle Wikileaks », *Liberation.fr*, 17 mars 2011 (*https://fr.wikipedia.org/wiki/WikiLeaks#cite_note-lib.C3.A9-japon2011-95,* consulté le 7 sept. 2014).

[16] Nelly Moussu (2011), « Un effort financier notable en Allemagne et au Royaume-Uni » (23 août).

[17] Nelly Moussu (2011), « Cyberdéfense : un enjeu du nouveau concept stratégique de l'OTAN » (10 août).

[18] *Sommet de l'OTAN*, Lisbonne, 19 et 20 novembre 2010. Voir : Général Stephane Abrial, (2011).

UNE MENACE SYSTEMIQUE

Le développement du réseau internet mondial a pu faire espérer le dégagement de nouveaux espaces de liberté pour les individus, minorités et sociétés face aux Etats. Ce développement a pu sembler inéluctable au point qu'une *Déclaration d'Indépendance du Cyberespace* a pu être proclamée[19]. Ces espoirs, comme le rôle des médias ou des réseaux sociaux dans les soulèvements populaires de pays non démocratiques, ou l'apparition de « contre-flux » informationnels pour contrebalancer la puissance des grandes agences de presse[20], seraient évidemment compromis si le développement du cyber-armement et l'utilisation de ce dernier devait se banaliser ôtant toute fiabilité aux infrastructures et services de TIC. Cela serait également vrai pour nombre d'autres effets attendus comme devant découler d'une libre circulation des informations à travers le monde, véritablement indépendante des puissances économiques ou politiques.

Les exemples d'attaques ou d'actions d'espionnage cybernétiques dans le monde ne manquent pas[21]. Plusieurs cas ont été signalés récemment en France[22], aux Etats-Unis[23] et dans de nombreux pays[24]. Les cibles potentielles sont nombreuses,

[19] John Perry Barlow (1996). L'auteur, un poète libertaire américain y écrivait à l'adresse des Etats : « Vous n'avez pas de souveraineté où nous nous rassemblons… Je déclare l'espace social global que nous construisons naturellement indépendant des tyrannies que vous cherchez à nous imposer. Vous n'avez aucun droit moral de dicter chez nous votre loi et vous ne possédez aucun moyen de nous contraindre que nous ayons à redouter. Le Cyberespace est fait de transactions, de relations, et de la pensée elle-même, formant comme une onde stationnaire dans la toile de nos communications. Notre monde est à la fois partout et nulle part, mais il n'est pas où vivent les corps…. Nous sommes en train de créer un monde où tous peuvent entrer sans privilège et sans être victimes de préjugés découlant de la race, du pouvoir économique, de la force militaire ou de la naissance. Nous sommes en train de créer un monde où n'importe qui, n'importe où, peut exprimer ses croyances, aussi singulières qu'elles soient, sans peur d'être réduit au silence ou à la conformité ».

[20] Tristan Mattelart (2014).

[21] La propagation du virus informatique STUXNET a endommagé des centrifugeuses d'enrichissement de l'uranium et contrarié le programme nucléaire militaire de l'Iran.

[22] Les cibles ont été de grandes entreprises (telle AREVA), le Ministère de l'Economie à la veille de la présidence française du G8/G20, des sites Internet institutionnels tel celui du Sénat. Voir : J.-M. Bockel (2012), *« La cyberdéfense : un enjeu mondial, une priorité nationale »,* Sénat, Paris.

[23] Un rapport officiel du Pentagone met en cause la Chine : *«* Les pirates informatiques chinois ont tenté en 2012 d'atteindre les ordinateurs du réseau gouvernemental, qui auraient pu offrir à Pékin un meilleur aperçu des capacités militaires et des délibérations politiques aux Etats-Unis » (*01net.com*, 7 mai 2013).

dont les plus évidentes sont les centres de commutation électroniques des réseaux des opérateurs, les systèmes informatiques des Etats et grandes entreprises, les serveurs Internet et datacentres[25], etc.

La nature de l'espace géographique a été modifiée en profondeur depuis le développement de l'usage massif des TIC. On parle de cyberespace, de géocyberespace[26], d'exogéographie[27] ou d'espace cybernétique. En fait, derrière ces mots se dessine l'apparition d'une géographie nouvelle, car les activités économiques sont devenues intrinsèquement liées aux produits, réseaux et services des télécommunications et notamment à l'Internet. Cet espace n'est pas le résultat de représentations, il n'est pas « dans un nuage », mais il s'appuie bien sur l'espace réel : réseaux de communications, centres de traitement informatiques des Etats et entreprises, serveurs, datacentres. Le système-monde et sa mondialisation sont devenus, plus que jamais, structurés par les TIC. S'agissant des Etats-Unis, il a été souligné : « le cyberespace est une véritable vulnérabilité de l'économie et du

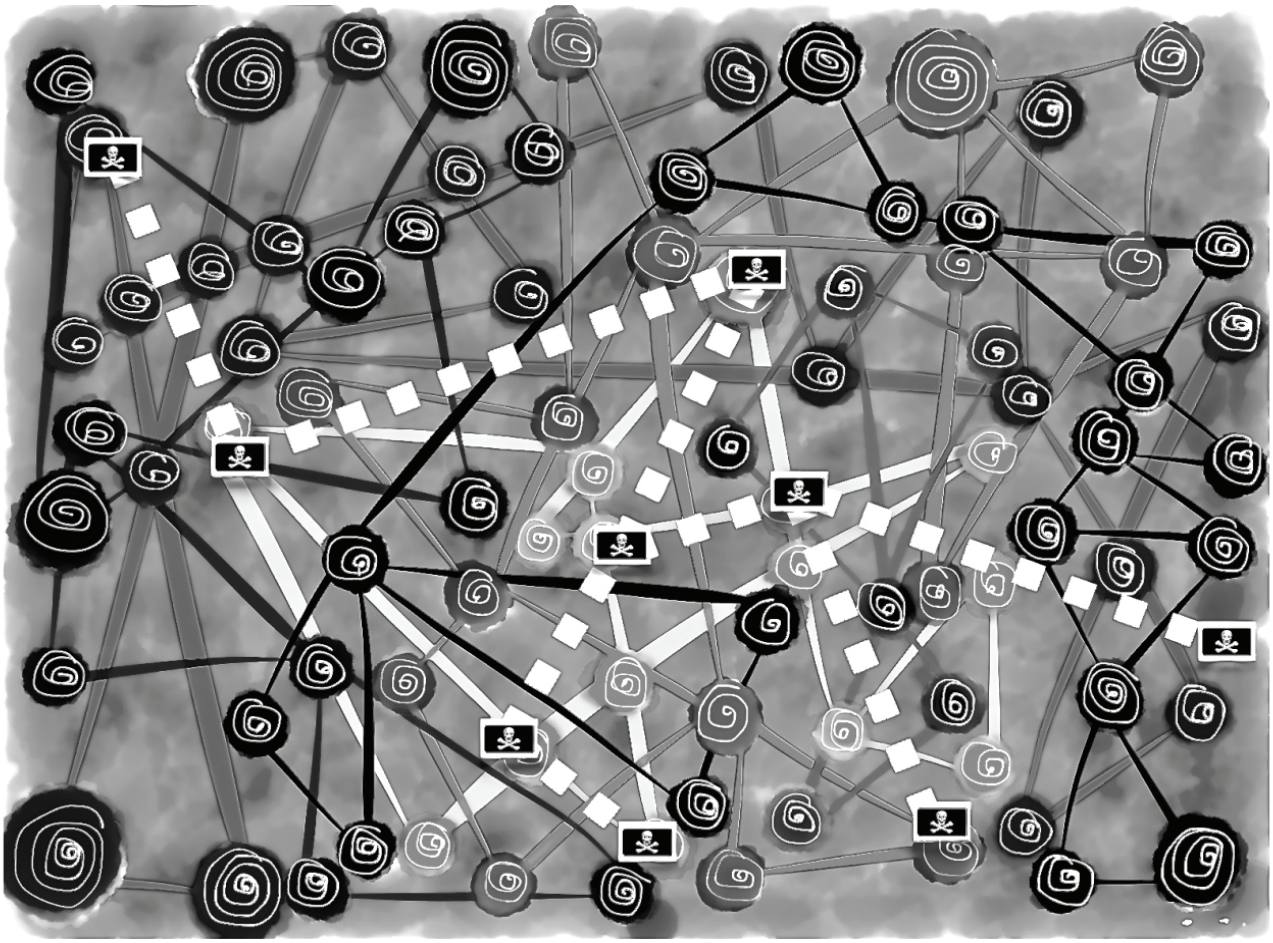
[24] « En 2007, à la suite d'une décision du gouvernement estonien de déplacer un mémorial de guerre datant de l'époque soviétique dans la ville de Tallinn, des hackers russes avaient semé la panique en attaquant simultanément les sites des ministères du pays ainsi que ceux de nombreuses entreprises privées, paralysant les principales institutions financières et les systèmes de télécommunication de l'état balte. Les mêmes techniques avaient vraisemblablement été employées lors de la crise géorgienne en 2008 et au début de la crise actuelle en Ukraine. Les autorités russes n'ont jamais reconnu être à l'origine de ces attaques, affirmant qu'il s'agissait du fait de hackers isolés. Et l'OTAN, prise au dépourvu, s'est rendue compte qu'elle n'avait pas de ligne politique claire ni de réponse à apporter à ce genre d'agression » peut-on lire dans *la Tribune* (Sauné 2014).

[25] Sur les datacentres, voir H. Bakis (2014), « Les facteurs de localisation d'un nouveau type d'établissements tertiaires : les datacentres ». Communication préparée pour la Conférence régionale de l'UGI à Cracovie, 20 août 2014. Dans ce numéro : pp. 351-384.

[26] Voir Henry Bakis (1997), "Approche spatiale des technologies de l'information", *Revue Géographique de l'Est*, n°4, pp. 255-262 ; Henry Bakis (1997), "From Geospace to Geocyberspace; Territories and Teleinteraction" pp. 15-49, in Roche E. M. & Bakis H. (eds., 1997), *Developments in telecommunications. Between global and local*, Avebury ; Henry Bakis (2007), « Le 'géocyberespace' revisité : usages et perspectives », *NETCOM*, Vol. 21, No 3-4, pp. 285-296 *http://www.netcom-journal.com/volumes/articlesV213/285_296bakisgeocyberspace.pdf*.

[27] Alexis Bautzmann (2001) oppose au terme d'« espace endogéographique », l'« espace exogéographique » où il range aussi bien le cyberespace que l'espace extra-atmosphérique. Voir : Bautzmann Alexis (2001), *Exogéographie politique des autoroutes de l'information : globalisation de la communication et mutation du système-monde,* Thèse de IIIe cycle, Paris.

gouvernement américains, dans la mesure où tous deux dépendent fortement de l'utilisation des ordinateurs et de leur connexion à l'Internet »[28].



L'espace cybernétique vu par le Pr. Edward M. Roche

Composition E. M. Roche.
Utilisation de : "Pirate flag 'WarX' edited by Manuel Strehl, Creative Commons Attribution/Share-Alike License". 5 sept. 2014.

[28] Rapport au Congrès de la Commission Sur l'Economie et la Sécurité US-Chine [USCC 2008, p. 9]. Cit F. Douzet (2009).

Dans ce contexte, la sécurité du bon fonctionnement du hardware et du software de la société de l'information est devenue vitale.

Les avis et appréciations sur la réalité des menaces sont certes partagés et le *blitzkrieg* numérique peut sembler un « mythe »[29]. Mais si une menace réelle devait s'abattre sur les réseaux mondiaux, cela pourrait dégrader voire empêcher partiellement ou totalement - et ce pour un temps plus ou moins long - le fonctionnement économique et social dans les territoires. Les conséquences qui en découleraient seraient considérables sur l'organisation de l'espace à toutes les échelles.

Le titre d'un article écrit en 1998[30] avec l'un des auteurs de l'article qui suit, soulignait combien le développement des réseaux de télécommunications était d'un intérêt central pour la société et l'économie de la planète. Ce titre notait que le développement des réseaux de la communication électronique débouchait sur le « système nerveux émergent de la société globale » qui avait notamment des fonctions spatiales. En 2011, un rapport du Sénat allait dans le même sens : « Avec le développement de l'Internet, les systèmes d'information constituent aujourd'hui de véritables 'centres nerveux' de nos sociétés, sans lesquels elles ne pourraient plus fonctionner » [31]. On qualifie parfois l'Internet de « réseau des réseaux ». Cela ne manque pas de pertinence car nombre de réseaux fonctionnent notamment à partir d'informations (capteurs par exemple[32]) ou de commandes qui leur proviennent en empruntant l'Internet.

L'existence de l'espace cybernétique tient à celle d'infrastructures localisées dans l'espace physique (donc susceptible de devenir la cible d'attaques par des armes mécaniques, chimiques ou nucléaires). La fragilité de cet espace tient aussi à sa nature propre qui le rend vulnérable aux armes cybernétiques. Dans un cas comme dans l'autre, l'origine de ces attaques peut provenir d'Etats ou d'autres agresseurs, terroristes par exemple.

---

[29] Boyer 2011. Le même auteur reconnaît cependant : « la cyberguerre n'aura peut-être pas lieu, mais il n'y aura plus de guerre sans 'cyber' », B. Boyer (2012).

[30] Henry Bakis & Edward M. Roche (1998), « Cyberspace - The Emerging Nervous System of Global Society and its Spatial Functions », *http://cybergeo.revues.org/5342*.

[31] J.-M. Bockel (2012).

[32] Pour optimiser la surveillance des réseaux d'eau potable, des solutions de surveillance des réseaux d'eau potable sont munis de capteurs pour éviter tout risque de fuite, de dégradation ou contamination de l'eau acheminée vers les clients. Voir : Florence Roussel (2007), « La technologie au service de la surveillance des réseaux d'eau potable », Actu-environnement, 4 mai, *http://www.actu-environnement.com/ae/news/surveillance_reseaux_eau_potable_2624.php4*.

Or, toute atteinte au système nerveux du système-monde serait préjudiciable au bon fonctionnement de nos sociétés. L'ampleur des dommages varie selon la nature de la « frappe ». Car toutes les atteintes ne visent pas les mêmes effets : *spams, scams, phishing* relèvent de la *«* cyberpiraterie frauduleuse »[33] ; l'intrusion dans les systèmes d'information et de communication adverses relève de la « cyberpiraterie de renseignement»[34] ; l'altération ou la destruction des réseaux de l'ennemi relève de la « cyberpiraterie stratégique »[35] ou selon le terme généralement utilisé, de la cyberguerre. La dimension géopolitique et géostratégique est évidente dans les deux derniers types. Les Etats tentent de faire prévaloir une souveraineté numérique que d'autres acteurs (dont ceux du secteur privé, d'autres Etats, d'opposants de toute nature) grignotent avec une certaine efficacité.

OBSTACLES A LA MISE EN ŒUVRE D'UNE CONVENTION

Malgré l'importance du problème posé, et les grandes qualités de la proposition de Roche & Blaine, les difficultés politiques, législatives et techniques à un contrôle efficace en vue de la sécurité de l'Internet sont bien réelles.

Les difficultés politiques

Les Etats, notamment les plus puissants, peuvent avoir quelque réticence à signer une telle convention. Pourquoi coopérer en matière cybernétique alors que ce sont les rapports de force qui prévalent en matière de relations internationales. Alors que leur souveraineté est de fait contestée et contrariée n'est-il pas plus pertinent, peuvent-ils estimer, de charger une structure propre d'affronter ces problèmes nouveaux ? Quelle confiance accorder aux supposés effets positifs d'une Convention internationale en la matière ? Ne serait-il pas préférable de rendre effective, en interne, une réelle supériorité cybernétique stratégique ?

[33] Selon la typologie de F. Douzet (2009).
[34] Selon la typologie de F. Douzet (2009).
[35] Selon la typologie de F. Douzet (2009).

Autre difficulté, ce phénomène ignore les frontières géographiques classiques (terrestres, aériennes, maritimes). Comment dans ces conditions organiser une coopération internationale entre gouvernements alors qu'il s'agit de « lutter contre un phénomène qui bâtit sa puissance et se propage hors de toute conception géographique classique de temps et d'espace »[36]. Comment aussi organiser une meilleure gouvernance mondiale et la sécurisation de l'Internet alors que « la majorité des pays utilisateurs ne sont pas des démocraties et qu'il est dès lors difficile d'envisager de leur donner un pouvoir sur l'architecture et la régulation du Net »[37].

Les difficultés juridiques

Elles tiennent aux restrictions de la liberté des échanges et à la plus grande capacité d'intrusion ou surveillance des régulateurs : « il n'existe pas de socle juridique commun entre les États sur lequel pourrait s'appuyer une harmonisation des pratiques »[38].

Les difficultés techniques

Par ailleurs, il ne faut pas ignorer les difficultés techniques que pose toute réponse adéquate de la part de l'Etat victime d'une cyber-agression. Quand bien même une cyber-attaque à l'encontre des réseaux, serveurs ou logiciels d'un Etat serait avérée, comment l'interpréter comme résultant effectivement d'une agression causée par un autre Etat[39] ? La grande facilité d'accès aux technologies numériques mises en œuvre par les hackers non étatiques (mafias, organisations terroristes, simples individus)[40] rend l'interprétation non évidente et l'éventuelle réplique cybernétique

[36] F. Douzet (2009).

[37] F. Douzet (2009).

[38] F. Douzet (2009).

[39] C'est ainsi que l'agression cybernétique subie par l'Estonie en avril 2007 a été diversement interprétée : attaque de hackers aux motivations prorusses ou intimidation directe de l'Etat russe. Deux ans plus tard, le ministre estonien de la Défense du pays a choisi de réduire cette agression à un acte de cyberpiraterie (cité par de F. Douzet, 2009).

[40] F. Douzet (2009) remarque qu'« un avion de combat coûte aujourd'hui au moins 100 millions de dollars, un système satellitaire plus d'un milliard de dollars et un navire de guerre plus de trois milliards. À l'inverse, une connexion Internet coûte moins de quarante dollars, un ordinateur performant revient à 600 dollars et n'importe quel individu avec quelques compétences en informatique peut créer un logiciel pouvant être transformé en *malware*. On peut facilement trouver sur des forums Internet des kits de cybercriminalité dont il ne reste qu'à régler quelques variables avant de le lancer. La lutte contre la prolifération informatique est tout bonnement impossible et on ne peut donc que mieux comprendre le phénomène

peut-être non pertinente. Comme le remarque F. Douzet, « toute cartographie des agissements dans le cyberespace se trouve vite soumise à des limites méthodologiques. L'implication au cours d'une attaque d'une machine ou d'un réseau de machines localisés dans un pays ne signifie pas nécessairement l'implication des propriétaires de machines ou de réseaux. La mobilisation de leurs machines a pu se faire à leur insu ou bien par usurpation de l'identité de leurs machines. Il est extrêmement difficile de géolocaliser avec certitude la provenance des attaques »[41].

CONCLUSION

Netcom a décidé d'éditer et traduire l'article d'*Orbis*, car les implications géopolitiques et géostratégiques de l'information et de la communication présentées dans ma *Géopolitique de l'information* (PUF, 1987) sont restées importantes dans les vingt-cinq dernières années. Bien plus, ces implications déjà caractérisées par les qualificatifs « fortes » ou « importantes » sont aujourd'hui plutôt caractérisées par les qualificatifs « essentielles » ou « vitales » tant elles sont inséparables du fonctionnement du système monde du début du 21ème siècle.

Roche & Blaine sont justement préoccupés par les dégâts potentiellement grands d'une guerre cybernétique. Si leurs craintes devaient s'avérer, la géographie des TIC et la géopolitique de l'information n'auraient plus de pertinence pour une durée plus ou moins longue. Leur appel à la signature, sous l'étude des Nations unies, d'une *Convention Internationale sur l'Utilisation Pacifique du Cyberespace* par les Etats vise à éviter ce futur que l'on ne peut plus exclure, hélas !

L'humanité a su, jusqu'à ce jour, éviter une apocalypse nucléaire même si la Guerre froide a pu connaître des moments d'extrême tension. On sait aujourd'hui « vivre avec » le nucléaire, et, dans une moindre mesure avec les armes chimiques et biologiques. Saura-t-on « vivre avec » les armes cybernétiques ? C'est tout l'enjeu de la Convention proposée par Roche & Blaine. Après la signature de plusieurs

massif de la cyberpiraterie ». Dans ces conditions, on comprend que ces pratiques soient considérées comme « une alternative très intéressante aux moyens militaires classiques notamment car elles sont discrètes. Il est en effet très difficile de prouver l'origine des attaques, aussi dévastatrices soient-elles » (Sauné, 2014).

[41] F. Douzet (2009).

Conventions internationales portant des objets divers[42], cette nouvelle *Convention* d'intérêt mondial a-t-elle quelque chance de voir le jour ?

Les sceptiques ne manqueront pas. Certains remarqueront que l'organisation des Nations unies (le « machin » comme le qualifiait de manière méprisante le Pt. Charles de Gaulle[43]) a suffisamment de causes de blocages bureaucratiques et politiques dans son fonctionnement pour en ajouter une ; parce qu'il s'agit de la seule organisation au monde à accueillir près de 200 pays membres « et autant de visions des affaires internationales »[44]. Ils diront aussi que la proposition de réflexions autour d'une convention témoigne d'un optimisme démesuré, voire d'une certaine naïveté tant le sujet est difficile, inséparable d'obstacles considérables, tant politiques que techniques. On n'imagine évidemment pas que les pirates et terroristes de tous bords soient intéressés, ce qui, de fait réduit considérablement le champ d'application d'une Convention dont seraient extérieurs les acteurs les plus pernicieux. On peut craindre aussi que les acteurs plus puissants sauront s'entourer de secrets en sélectionnant des activités à dissimuler impérativement ; qu'ils seront plutôt intéressés à mettre sur pied, comme l'OTAN, des équipes de réaction rapide pour protéger leurs systèmes informatiques[45]. Le scepticisme est peut-être une réaction réaliste en la matière. Pourtant, l'immobilisme ne serait pas une solution tant les enjeux sont important. Même si les Etats démocratiques et leurs organisations dédiées[46] parvenaient seuls à s'entendre et signer cette Convention, l'avancée serait déjà considérable. Les diplomates ont donc du travail devant eux pour faire avancer significativement ce dossier difficile.

---

[42] Depuis le Traité de Strasbourg (1675) signé par la France et le Saint Empire Romain Germanique pour limiter l'utilisation de boulets empoisonnés, divers accords internationaux ont tenté de contrôler la prolifération d'armes chimiques et biologiques. Citons aussi le « Traité sur les principes régissant les activités des Etats en matière d'exploration et d'utilisation de l'espace extra-atmosphérique » *(http://www.oosa.unvienna.org/pdf/publications/STSPACE11F.pdf).*

[43] « Le machin qu'on appelle l'ONU » : c'est ainsi que le général De Gaulle qualifiait les Nations Unies (10 septembre, Nantes, 1960).

[44] Attias Richard (2013), « L'ONU: une grosse machine imparfaite... mais indispensable », 24 septembre, *http://www.huffingtonpost.fr/richard-attias/nations-unies-international_b_3975885.html*

[45] *01net.com*, 4 sept. 2014, *http://www.01net.com/editorial/596753/cybersecurite-l-otan-se-dote-d-une-cyberforce-de-reaction-rapide/*

[46] Par exemple le Centre canadien de réponse aux incidents cybernétiques (CCRIC) qui « veille à ce que les nombreux services utilisés chaque jour par les Canadiens soient sécuritaires. Il aide à sécuriser les systèmes cybernétiques des provinces, des territoires, des municipalités et des organisations du secteur privé, et collabore étroitement avec les partenaires, y compris les homologues et les fournisseurs en technologie de l'information à l'échelle internationale » *(http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-fra.aspx*, consult. 5 sept. 2014)

REFERENCES

ABRIAL, Général Stephane (2011), « NATO Builds Its Cyberdefenses », 27 feb., *http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html?_r=5&*

ARPAGIAN Nicolas (2011), « Cyberguerre & cybercriminalité. Internet : combien de divisions ? », voir : *GDD* (2011).

BAKIS Henry (1987), *Géopolitique de l'information*, Que sais-je ?, Presses universitaires de France.

BARLOW John Perry (1996), *A Declaration of the Independence of Cyberspace*, février, *http ://homes. eff.org/barlow/Declaration-Final.html*

BOCKEL Jean-Marie (2012), *La cyberdéfense : un enjeu mondial, une priorité nationale.* Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées, n° 681 (2011-2012) - 18 juillet.

BOYER, Commandant Bertrand (2011), « La cyberguerre ou le mythe du *blitzkrieg* numérique », voir : *GDD* (2011).

BOYER, Commandant Bertrand (2012), *Cyberstratégie, l'art de la guerre numérique,* 238 p. Coll. La Pensée stratégique, Nuvis.

BOYER, Commandant Bertrand (2014), *Cybertactique : Conduire la Guerre Numerique*, Nuvis.

DESFORGES Alix (2013), « Les frontières du cyberspace », pp. 101-112 in Douzet F. & Giblin B. (dir.), *Des frontières indépassables, Des frontières indépassables ? des frontières d'Etat aux frontières urbaines,* 320 p. Armand Colin, Paris.

DOUZET Frédérick (1997), « Les enjeux géopolitiques du cyberespace », *Netcom*, vol. 11, n° 1, pp. 181-216.

DOUZET Frédérick (2009), « Les pirates du cyberespace », Hérodote, 3 (n° 134). *http://www.cairn.info/zen.php?ID_ARTICLE=HER_134_0353#no83*

DOUZET Frédérick (2013), "La course aux cyberarmes est en marche", *Le Monde Economie*, 25.02.2013, Propos recueillis par Chloé Hecketsweiler.

DOUZET Frédérick, DESFORGES Alix & LIMONIER Kevin (2014), *Géopolitique du cyberespace: « territoire », frontières et conflits, http://www.gis-cist.fr/wp-content/uploads/2014/02/douzet-desforges-limonier.pdf*

GDD (2011), « Géopolitique de l'information », *Les Grands Dossiers de Diplomatie*, 6 avr 2011, n°2, avril-mai 2011. 100 pages, AREION Group/CAPRI, Paris.

MATTELART Tristan (2014), « Les enjeux de la circulation internationale de l'information », *Revue française des sciences de l'information et de la communication*, 5, *http://rfsic.revues.org/1145*.

MOUSSU Nelly (2011). *2011 - Cyberdéfense, enjeu du 21e siècle*, *http://www.defense.gouv.fr/actualites/dossiers/la-cyberdefense/dossiers/2011-cyberdefense-enjeu-du-21e-siecle/international*, 8 août.

ROCHE Edward M. & BLAINE Michael J. (2014), « Convention Internationale sur l'utilisation pacifique du Cyberespace », *Netcom*, vol. 27, n° 3-4, sept. Version originale : « International Convention for the Peaceful Use of Cyberspace », *Orbis: A Journal of World Affairs*, Spring 2014, Vol. 58 Issue 2 pages 282-296. Voir *: http://www.fpri.org/articles/2014/04/international-convention-peaceful-use-cyberspace*

SAUNE Julien (2014), « Les cyberattaques bientôt considérées comme acte de guerre par l'OTAN », 4 septembre, La Tribune, *http://www.latribune.fr/actualites/economie/international/20140904trib000847402/les-cyberattaques-bientot-considerees-comme-acte-de-guerre-par-l-otan.html*

SOPPELSA Jacques (1980), *Géographie des armements*, Masson, Paris, 279 pages

USA. DEPARTEMENT OF DEFENSE (2013), *ANNUAL REPORT TO CONGRESS. Military and Security Developments Involving the People's Republic of China 2013, http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf*

01NET.COM (2014), « Cybersécurité : l'OTAN se dote d'une cyberforce de réaction rapide », 4 sept., *http://www.01net.com/editorial/596753/cybersecurite-l-otan-se-dote-d-une-cyberforce-de-reaction-rapide/*

01net.com (2014), « Cybersécurité : l'OTAN se dote d'une cyberforce de réaction rapide », 4 sept., *http://www.01net.com/editorial/596753/cybersecurite-l-otan-se-dote-d-une-cyberforce-de-reaction-rapide/*