LES CYBER-CONFLITS, UNE RÉVOLUTION GÉOPOLITIQUE?

PAR

JEAN-LOUP SAMAAN (*)

Au cours des derniers mois, des événements à travers le monde ont concouru à la prise en considération de ce qu'il est désormais convenu d'appeler les «cyber-conflits». L'attaque contre les serveurs gouvernementaux d'Estonie, au printemps 2007, les infiltrations asiatiques répétées au sein des réseaux militaires américains ou encore la découverte d'un gigantesque réseau de cyber-espionnage, appelé «Ghostnet», visant les relais de la cause tibétaine sont autant de nouvelles relayées par les médias, qui contribuent à alimenter la spéculation autour des tenants et aboutissants du «cyber-espace».

Le terme lui-même, «cyberespace», est aujourd'hui devenu un mot commun. Or, dans le même temps, il semble échapper à une terminologie qui serait internationalement reconnue. Certes, de nombreuses définitions ont été suggérées au sein de la communauté des ingénieurs, informaticiens, officiers militaires et stratégistes travaillant sur le sujet. Parmi d'autres, le Département à la Défense américain le définit comme un «*domaine caractérisé par l'usage de l'électronique et du spectre électromagnétique pour stocker, modifier et échanger des données* via *des systèmes en réseaux et les structures physiques qui y sont attachées*» (1). Bien que souvent jugée incomplète – car exclusivement orientée sur les caractéristiques du contenant et non du contenu –, la définition de l'armée américaine reste la référence du débat stratégique. Ce domaine peut également être circonscrit. Les experts en sécurité des réseaux distinguent trois strates fondatrices du cyberespace : la strate physique (infrastructures, câbles routeurs), la strate syntaxique (standards et protocoles) et la strate sémantique (l'information diffusée) (2).

Dans le même temps, force est de constater, au cours des dernières années, que, en dépit de l'incertitude ambiante sur ce que recouvre exactement le cyberespace, la problématique de son avènement et de son éventuel encadrement politique s'est progressivement insérée au premier plan de l'agenda international. De nombreux forums existent désormais au sein de

(*) Chargé de mission à la Délégation aux affaires stratégiques (DAS) du ministère français de la Défense.

(1) *National Military for Cyberspace Operations*, 2006.

(2) Martin C. LIBICKI, *Conquest in Cyberspace : National Security and. Information Warfare*, Cambridge. University Press, New York, 2007.

la sphère académique comme au sein de la sphère décisionnelle (entre autres, les séminaires réguliers organisés par la National Defense University à Washington ou encore les tables rondes du Global Internet Governance Academic Network). En outre, paraît un nombre impressionnant d'articles consacrés au «cyber-phénomène». Toutefois, ces travaux soulignent surtout les implications technologiques et les défis sécuritaires du domaine. Ainsi, passée la généalogie nécessaire mais non suffisante du cyberespace, leur apport analytique reste modeste. Dans le même temps, on ne dénombre que très peu de tentatives pour concevoir le «cyber» comme un espace socio-politique, soit une sphère produisant des enjeux de pouvoir qui lui seraient propres (3). Autrement dit, nous disposons aujourd'hui d'un nombre conséquent de travaux sur les technologies du cyberespace et leurs potentialités, mais nos connaissances restent parcellaires en ce qui concerne la caractérisation des acteurs, la compréhension de leurs motivations et l'appréhension des conséquences dans la distribution du pouvoir à l'échelle internationale.

En se fondant sur les événements des dernières années, cet article entend reprendre à son profit quelques outils classiques de la sociologie des mobilisations (4) pour attester de leur valeur ajoutée quant à la compréhension du cyberespace. En effet, ceux-là nous permettent d'appréhender la façon dont le «cyber» altère les vieilles grilles de la géopolitique entre les Etats et les individus. Ils permettent également de comprendre comment les acteurs décident de passer à l'acte de cyber-piraterie ou de lancer une cyber-guerre.

«Cyberchamp» : l'altération de la vieille géopolitique

Se référer au cyberespace comme sphère sociale signifie qu'il est possible de concevoir celui-là comme un secteur autonome – mais non indépendant –, où les acteurs (tant les individus que les organisations) interagissent et luttent pour la conquête de capitaux (politiques, sociaux ou financiers). Il s'agit là d'une vue classique, inspirée des travaux originels de Pierre Bourdieu sur les multiples «champs» qui constituent la société (5).

Si on considère l'exploitation croissante du cyberespace par les acteurs sociaux – qui n'incluent pas seulement les individus mais aussi les Etats, les organisations non gouvernementales, les compagnies privées et autres entités –, il n'est pas déplacé de considérer qu'il est devenu une sphère autonome avec ses propres processus, ses propres règles et ses propres enjeux.

(3) Un cas intéressant est le travail mené en 2007-2008 par la National Defense University : Frank Kramer/Stuart Starr/Larry Wentz, *Cyberpower and National Security*, NDU Press, Washington, 2009.

(4) Entre autres, Sidney Tarrow, *Power in Movement*, Cambridge University Press, Cambridge, 1998; Charles Tilly, *The Politics of Collective Violence*, Cambridge University Press, Cambridge, 2003.

(5) Entre autres, Pierre Bourdieu, *Questions de sociologie*, Editions de Minuit, Paris, 1980, *Raisons pratiques : sur la théorie de l'action*, Seuil, Paris, 1994, et *Les Règles de l'art : genèse et structure du champ littéraire*, Seuil, Paris, 1998.

Alors, l'objet de notre recherche ne doit pas être de montrer comment les gouvernements ont perdu le contrôle du cyberespace, mais de caractériser les interactions et les comportements des compétiteurs, de comprendre ce qui se joue «dans» le cyberespace.

Processus, règles et enjeux

La spécificité des formes d'interaction dans le cyberespace est aujourd'hui source de fascination populaire. Les réseaux sociaux comme Facebook, Twitter, Live Journal, Viadeo ont créé une nouvelle façon de rencontrer les gens à distance. Cela a ainsi redéfini les modalités fondamentales de l'échange entre les individus. Par définition, le cyberespace n'est pas confronté aux limites naturelles (en termes géographiques comme temporels) comme peuvent l'être d'autres espaces sociaux. Ainsi que le rappelle Laurent Murawiec, un analyste du Hudson Institute, le «*cyberespace n'a pas attendu que les hommes le découvrent, l'explorent et l'exploitent : il est une invention humaine*» (6).

A l'exception des infrastructures physiques soutenant le cyberespace, celui-là est donc tout bonnement hors des règles de notre monde. On touche ici au défi originel du cyberespace : parce que celui-là dispose de ses propres règles, les acteurs dominés dans d'autres «champs» peuvent devenir dominants dans le «cyber-champ». Défi de pouvoir, mais aussi défi d'analyse : comment peut-on comprendre et systématiser un savoir sur un environnement évolutif par essence ? Autrement dit, si le cyberespace est une invention inédite et incomparable, quels outils d'analyse peuvent lui être associés ? Quelles analogies peuvent-elles s'avérer pertinentes ?

Les règles du cyberespace pourraient être résumées par deux mots : libre et économe. Libre, parce que le spectre électronique a été conçu par des gens préoccupés par la liberté et non par des questions de sécurité (7). Econome parce qu'il se développe de la façon la plus rapide dans l'histoire de la technologie. Si l'économie est la science de la rareté, l'étude du cyberespace est l'exact opposé.

Pour comprendre cela, jetons un coup d'œil au marché militaire international : le coût unitaire d'un char d'assaut avoisine les 15 millions d'euros, celui d'un hélicoptère dépasse les 30 millions d'euros, celui d'un avion de combat oscille autour de 100 millions de dollars, un système satellitaire vaut plus d'un milliard de dollars et un navire de guerre plus de 3 milliards de dollars. Par contraste, il y a des milliards d'utilisateurs du «cyber» à travers le monde : une connexion Internet coûte environ 40 dollars par mois, un bon ordinateur peut être obtenu pour 600 dollars et un

(6) Laurent MURAWIEC, *Aristotle in Cyberspace : Toward a Theory of Information Warfare*, RAND, nov. 2001, p. 62.

(7) Frédérick DOUZET/Jean-Loup SAMAAN/Alix DESFORGES, «Les pirates du cyberespace», *Hérodote*, n° 3, 2009, p. 180.

logiciel sophistiqué peut être créé par une personne unique ou téléchargé gratuitement à partir d'Internet.

Aux règles de liberté et d'économie du cyberespace, s'ajoute un facteur proprement technologique : la rapidité exponentielle de son développement. Face à celle-là, les organisations humaines devraient être capables de changer leurs structures aussi vite que le cyber s'étend.

Historiquement, cela s'est rapidement avéré difficile pour d'énormes institutions – qu'il s'agisse de bureaucraties gouvernementales et grandes firmes. Le décalage est criant au sein des armées, entre, d'un côté, des technologies de l'information et de la communication qui innovent de manière radicale en moins de cinq ans et, de l'autre, des équipements militaires dont les cycles d'exploitation restent programmés sur trente ans. En 2010, les équipements-phares de l'armée française (char Leclerc, hélicoptère Tigre, l'avion polyvalent Rafale et le porte-avions à propulsion nucléaire Charles-de-Gaulle) ont tous été choisis par la loi de programmation militaire... en 1986.

A l'inverse, le cyber-champ a ouvert une fenêtre d'opportunité pour de petites organisations (dans les affaires, en politique mais aussi en matière de crime et de terrorisme) (8). Cela souligne clairement le nouvel équilibre des pouvoirs que le «cyber» établit entre les acteurs politiques.

Redéfinir la distribution de puissance dans le cyberespace

A ce stade de la réflexion, qu'est-ce que la notion de «cyber-champ» implique pour les manières classiques de circonscrire les activités politiques ? Le cyberespace, plus particulièrement Internet, ne connaît pas de limite à ses activités. Evidemment, ce phénomène a conduit à la production de nombreuses affirmations euphoriques sur les implications probables pour les théories des relations internationales. En raison de cette tendance technologique, les universitaires en sont venus à affirmer que les concepts traditionnels de géopolitique comme les territoires allaient devenir inadaptés. Puis, les anciennes notions de frontières et de souveraineté nationale – avec le dispositif régalien qui les accompagne – allaient perdre leur pertinence à l'ère électronique. Certains ont soutenu que la puissance de la rapidité allait surpasser la valeur de l'espace et que, par conséquent, la géographie allait être de plus en plus dimensionnée par la vitesse et non le territoire. Il est vrai que le cyberespace modifie la «vieille» géopolitique, mais il ne la remplace pas. Martin Libicki explique sagement, dans un article de 1996 : «*aussi longtemps que l'humanité utilisera des instruments connectés à des médias lents – c'est encore le cas pour le transport aérien ou maritime –, la plupart de ce que nous savons à propos de la géographie et de la géopolitique continuera à s'appliquer. Cependant, avec tout nouveau média,*

(8) Thomas Rid/Marc Hecker, *War 2.0 : Irregular Warfare in the Information Age*, Praeger, Westport, 2009.

vient une nouvelle logique géographique; alors que l'importance des nouveaux médias grandit, leur logique transformera celle des anciens» (9).

Dès lors, la vraie question est la spécificité de cette transformation.

Un nouvel outil de mobilisation socio-politique

Comprendre le crime et la guerre dans le cyberespace reste complexe, mais l'étude scientifique des mouvements sociaux et de l'action collective peut nous délivrer quelques outils d'analyse précieux. Si les acteurs rationnels tendent à chercher l'arène la plus efficace pour promouvoir leurs vues et conquérir des ressources, le cyberespace semble être devenu une de ces arènes dans le monde contemporain. Comme nous disions auparavant, le cyberespace est une sphère autonome du monde social, mais non indépendante. Cela signifie qu'il peut être défini comme une arène où les conflits sociaux advenant dans d'autres champs peuvent migrer. C'est la raison pour laquelle, au cours des dernières années, les *mass medias* ont été fascinés par ce nouveau vecteur de protestation.

Par exemple, les journalistes ont récemment évoqué la «révolution Twitter» en Moldavie, en référence à l'exploitation d'Internet au cours des mobilisations sociales contre les autorités politiques en avril 2009. Le 6 avril, alors que le Parti communiste moldave revendique une victoire électorale, des allégations sur une vague de fraude dans les urnes circulent dans la capitale Chisinau. Alors que le parti au pouvoir est déjà accusé de la faillite du modèle économique national, ces allégations déclenchent un massif mouvement de contestation parmi les étudiants. En l'espace de quelques heures, des manifestations gigantesques s'organisent dans les rues de Chisinau, les organisateurs communiquant entre eux très souvent à partir des outils du Web 2.0.

Ces événements dans l'ancienne République soviétique de Moldavie nous donnent l'illustration pertinente de la façon dont le cyberespace a modifié le mode opératoire des mouvements sociaux, les voies et les moyens des acteurs non étatiques pour défier les autorités traditionnelles. Soutenus par des outils de réseaux sociaux comme Twitter, LiveJournal et Facebook, les manifestants ont mené une campagne agressive de protestation contre le gouvernement actuel. Nathan Hodge, du magazine américain *Wired*, a observé que des «tweets», e-mails, «blog posts», des vidéos, des photos et des messages sur Facebook arrivaient chaque seconde, livrant des actualités immédiates sur l'évolution de la manifestation (10).

(9) Martin Libicki, «The emerging primacy of information – A Debate on Geopolitics», *Orbis*, print. 1996, p. 261.

(10) Nathan Hodge, «Inside Moldova's Twitter revolution», *Danger room*, 8 avr. 2009.

La motivation politique derrière les événements en Moldavie était évidente et revendiquée, mais ce n'est pas toujours le cas. Par exemple, l'usage de «spams», de virus, d'intrusions électroniques, pour nuire aux utilisateurs ou pour les voler n'implique pas obligatoirement de signification politique. Ce sont typiquement ce que nous appellerions des armes de nuisance massive ou, dit autrement, de «la cyber-piraterie». Afin de donner un aperçu précis de l'étendue des mobilisations dans le cyberespace, nous avons besoin de détailler les outils en question.

Cyber-outils de mobilisation

Il y a plusieurs façons d'interagir avec des acteurs à travers le cyberespace, mais nous considérerons ici uniquement trois outils offensifs pouvant le plus souvent être exploités.

Les *Bot*-(une contraction de robot)-*networks* ou *botnets* sont constitués d'un vaste nombre d'ordinateurs infectés et commandés à distance pour opérer, de concert, à travers des ordres envoyés *via* Internet. Ils sont utilisés pour bloquer ou couper les ordinateurs d'organisations ciblées – action dite de «déni de service» – ou pour distribuer des «spams», des virus et autres codes frauduleux.

Le *phishing* est la forme la plus commune de «*online scam*». Cela implique des millions d'e-mails, apparemment en provenance d'une société légitime telle qu'une banque en ligne ou un marchand, annonçant un problème avec le compte du client. Les messages trompent les utilisateurs en leur demandant de cliquer sur un lien qui apparaît pointer vers un site commercial légitime, mais qui, en fait, conduit l'utilisateur vers un site imposteur, contrôlé par l'attaquant et conçu pour ressembler à un site de commerce en ligne. Le site demande à l'utilisateur son nom et son mot de passe ou l'information d'un autre compte, que le logiciel de l'attaquant mémorise à des fins frauduleuses ou criminelles. On comptabilise plus de 100 000 sites de *phishing* sur Internet et des millions d'e-mails de *phishing* sont envoyés chaque jour (11).

Enfin, on trouve les *malwares*. Les chevaux de Troie, les *spywares* et *adwares* sont des formes de logiciels malicieux (*malicious softwares*) qui peuvent clandestinement infecter un ordinateur, enregistrer des informations sensibles stockées par l'ordinateur ou mémoriser les mots de passe pour les transmettre ensuite *via* Internet à un emplacement temporaire où ils seront réutilisés pour des fins frauduleuses par une tierce personne.

Ce rapide aperçu des cyber-outils de mobilisation laisse entrevoir combien il est difficile de qualifier les nouvelles formes de mobilisations qu'ils induisent. Des techniques d'intrusion dans les réseaux informatiques, comme le

(11) Edward Skoudis, «Information security issues in cyberspace», *in* Franklin Kramer/Stuart Starr/Larry Wentz (dir.), *op. cit.*, p. 175.

phishing, le *spaming* ou les attaques de déni de service, peuvent être perçues soit comme des actes frauduleux isolés, soit comme des actes politiques impliquant un objectif stratégique agressif.

Des différents types de mobilisation

Il est nécessaire de distinguer deux différents types de mobilisations : la cyber-piraterie et les cyber-conflits. En quoi sont-ils différents ? Leur forme est similaire : le déni d'accès, le *phishing*, le *spaming* peuvent être utilisés pour les deux. La seule façon de les différencier est la motivation derrière l'action.

Nous pouvons en énumérer trois types. La motivation frauduleuse caractérise la cyber-piraterie classique (comme les attaques sur les sites bancaires, le vol d'identité). La recherche clandestine d'acquisition de données renvoie au cyber-espionnage, que ce soit dans la sphère politique ou commerciale. Enfin, la volonté de détruire l'ennemi de sorte qu'il soit affecté au-delà du cyberespace correspond à ce que nous appellerons la cyber-guerre.

Si cette brève typologie permet d'avoir un aperçu du spectre de mobilisations sociales dans le cyberespace, quelques questions fondamentales restent toutefois sans réponse et freinent tout progrès pour une analyse rigoureuse des cyber-conflits.

Attribution, intentionnalité et rationalité des attaques

Regardons de près trois problématiques : l'attribution des attaques, leur intentionnalité et la rationalité collective.

Les cyber-outils de mobilisation contournent toute possibilité technologique de retracer un acte de piraterie ou de guerre. L'utilisation de *botnets* renvoie à un détournement d'ordinateurs qui peuvent se trouver dans d'autres pays, voire sur d'autres continents. C'est pourquoi les autorités ne peuvent pas être certaines d'attribuer une attaque à une organisation terroriste ou à un Etat, excepté si celui-là revendique l'attaque – ce qui n'est jamais arrivé à ce jour. Les attaques du printemps 2007 contre l'Estonie avaient parfois pour provenance des ordinateurs localisés en Californie. De même pour le réseau Ghostnet, dont certaines sources, mais pas exclusivement, étaient chinoises.

Etablir le spectre des motivations pour des attaques dans le cyberespace nécessite la compréhension de celles-là lorsque les attaques adviennent. Est-ce qu'un cyber-guerrier – ou un cybercriminel – attaque une infrastructure critique (un système bancaire ou un réseau énergétique) pour entrer en guerre ou uniquement pour nuire ? A nouveau, sans revendication, il est presque impossible d'en avoir la certitude. S'ajoutant au problème de

l'attribution, cela rend clairement difficiles les choix politiques pour les décideurs. D'un point de vue légal, est-ce un acte de guerre ou non ?

Même si nous sommes capables de retracer une attaque et nous savons qu'un groupuscule d'Asie centrale avec un agenda politique est derrière celle-là, comment peut-on évaluer sa rationalité ? Les auteurs sont-ils liés à une organisation gouvernementale ? S'agit-il d'un acte isolé de *hackers* psycho-pathétiques ou, au contraire, d'un mouvement de «proxy» ? A ce titre, l'analyse du US Cyber Consequences Unit (US-CCU) sur la cyber-campagne contre la Géorgie est particulièrement instructive. Retraçant les attaques, les experts américains ont pu constater que la provenance était essentiellement civile et non militaire. Les attaquants étaient ainsi des individus recrutés *via* des réseaux sociaux électroniques. Néanmoins, l'US-CCU est convaincu d'une convergence évidente entre les intentions de ces groupes de *hackers* et l'armée russe, tant les attaques des premiers suivaient le rythme de la campagne militaire conduite par Moscou : «*les organisateurs des cyber-attaques avaient une connaissance* a priori *des intentions militaires russes et bénéficiaient d'informations précises sur l'avancée des opérations avant que celles-là soient menées*», écrivent ainsi les auteurs (12). Les experts occidentaux restent plus mesurés en ce qui concerne les «hackers» chinois ayant perpétré, au cours des dernières années, les assauts informatiques contre les réseaux du Département de la Défense américain. D'après les rapports techniques non classifiés, les capacités à la disposition des attaquants attestent d'un niveau de sophistication élevé, pouvant suggérer un appui étatique. Pour autant, le lien entre programmeurs clandestins (*black hat programmers*) et l'armée populaire chinoise reste ténu (13).

Ces trois problématiques soulignent combien le cyber-champ reste difficile à appréhender. Cela étant, parce que la sphère politique ne peut supporter l'incertitude, les cyber-conflits ont souvent été résumés d'une façon simpliste avec des expressions telles «le Pearl Harbor électronique», «les hackers djihadistes», le «cyber-terrorisme». En dépit du fait que rien dans l'histoire, à ce jour, ne peut étayer ces scénarios, les événements des dernières années (les cyber-attaques en Estonie, au Kirghizstan ou encore les intrusions dans les réseaux militaires américains, français, britanniques, parmi d'autres) ont conduit à placer la cyber-défense sur l'agenda des forces armées.

(12) John Bumgarner/Scott Borg, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, US-CCU Special Report, août 2009.

(13) Bryan Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman (US-China Economic and Security Review Commission), oct. 2009, pp. 6-7.

La militarisation croissante du cyberespace

Le cyberespace n'implique pas seulement de nouveaux modes d'expression politique, mais aussi un nouvel art de la guerre. Dans la plupart des pays développés, les forces armées étendent de plus en plus leur dispositif institutionnel devant couvrir le cyber-champ. En France, le Livre blanc sur la défense et la sécurité nationale, publié en 2008, explique : «*dans le domaine informatique plus que dans tout autre milieu, il faudra, pour se défendre, savoir attaquer*» (14). Depuis lors, cette déclaration a été suivie d'actes, avec la création, en 2009, de l'Agence nationale de sécurité des systèmes d'information (ANSSI), une agence exécutive en charge de la sécurité des systèmes d'information au sein du gouvernement français. Aux Etats-Unis, au printemps 2009, le président Obama a mandaté une revue de soixante jours conduite par Melissa Hathaway, avec pour but de définir une stratégie en matière de cyber-sécurité.

En fait, la sensibilité grandissante des pays occidentaux est apparue au premier plan, après la fameuse «première cyber-guerre» en Estonie, au printemps 2007. Le 26 avril 2007, un flux hors du commun de messages électroniques fut envoyé aux sites gouvernementaux, provoquant une congestion électronique telle qu'une équipe d'urgence fut déployée au cours des heures suivantes. En vain : les sites Internet furent progressivement fermés, certains pour quelques heures, d'autres pour plusieurs jours, ce qui aboutit finalement à un «cyber-blocus» total de l'Estonie pendant trois semaines. L'enquête qui suivit fut décevante parce qu'il était difficile de déterminer une entité clairement responsable. En effet, l'origine des attaques se trouvait dans plus de cinquante pays. Pour autant, devons-nous voir comme une simple coïncidence le fait que cette attaque électronique contre l'Etat estonien est arrivée, en pleine controverse sur la statue du soldat de bronze soviétique, héros de la Seconde Guerre mondiale, que le Parti de la réforme, vainqueur des dernières élections, avait promis de déplacer ? Pour certains observateurs, ce mobile était suffisant pour qu'on voie la main invisible du Kremlin derrière les attaques. Quelques semaines après celles-là, le Secrétaire de l'Air Force, Michael Wynne affirme en tout cas que «*la Russie semble être la première à s'être engagée dans la cyber-guerre*» (15). Et Jaak Aaviksoo, ministre estonien de la Défense, va plus loin en évoquant «*la véritable troisième guerre mondiale*» (16).

(14) *Défense et sécurité nationale : Le Livre blanc*, Odile Jacob, Paris, 2008, p. 207.
(15) Rebecca Grant, *Victory in Cyberspace*, Air Force Association, 2007.
(16) Estonian Ministry of Defense, «Internet : XXI Century Battlefield», Communiqué de presse, 16 juin 2007.

D'une certaine façon, les réactions aux événements en Estonie n'ont fait qu'exacerber la préoccupation des armées à l'égard du cyberespace. Leur long investissement en la matière tend bien à le prouver.

Les armées modernes intègrent les cyber-outils à leurs arsenaux

Si le cyberespace est initialement la progéniture de l'armée américaine (avec Arpanet, l'ancêtre d'Internet, construit au cours des années soixante par la DARPA) la problématique des cyber-conflits fait son apparition dans le débat stratégique au lendemain de la Guerre froide. A l'époque, la première guerre du Golfe offre l'illustration spectaculaire de l'accélération du processus entre collecte du renseignement et conduite des opérations, grâce à des innovations dans le champ des technologies de l'information et de la communication mises en œuvre au cours des décennies précédentes. Pendant les années 1990, toute une littérature stratégique se développe autour de la fameuse Révolution dans les affaires militaires, au sein de laquelle l'exploitation d'interfaces électroniques n'était qu'une composante parmi d'autres (17).

Si les Américains réfléchissent depuis deux décennies au «cyber», ils n'en sont pas pour autant plus avancés en matière de responsabilités institutionnelles. Entre la fin de l'administration Bush et le début de l'administration Obama, plusieurs déclarations d'officiels militaires haut placés (le *chairman of the joint Chiefs of staff* l'amiral Mullen ; le *vice-chairman of the joint Chiefs of staff*, le général Cartwright ou encore le Directeur de la communauté du renseignement, l'amiral Blair) sur l'enjeu de sécurité nationale que représente le cyberespace (18) ont mis en évidence le fait que le sujet devait désormais être directement traité au sein de la Maison-Blanche. Cette reprise en main du dossier au plus haut niveau de l'exécutif fait suite à diverses critiques : le manque de moyens du Department of Homeland Security (19) et la captation inachevée de la cyber-défense par l'US Air Force (USAF) dans le cadre de son Cybercommand. Ce dernier semble aujourd'hui faire figure de grand perdant des luttes bureaucratiques : lancée par Michael Wynne, l'ancien secrétaire de l'Air Force limogé par Robert

(17) Pour un aperçu des débats autour de la Révolution dans les affaires militaires, *cf.* Richard Hundley, *Past Revolutions. Future Transformation : What can the History of Revolutions in Military Affairs Tell Us About Transforming the US Military?*, RAND Corporation, Santa Monica, 1999 ; Stuart Johnson/Martin Libicki (dir.), *Dominant Battlespace Knowledge*, NDU Press Book, Washington, 1995 ; Arthur K. Cebrowski/John J. Garska, «Network-centric warfare : its origin and future», *Proceedings Magazine*, vol. CXXIV, n° 1, janv. 1998, pp. 28-35 ; Eliot Cohen, «A revolution in warfare», *Foreign Affairs*, vol. LXXV, n° 2, mars-avr. 1996, pp. 37-54 ; Michael Mazzarr, *The Military-Technical Revolution : a Structural Framework*, Center for Strategic and International Studies Press, Washington, 1993 ; William Odom, *America's Military Revolution : Strategy and Structure after the Cold War*, American University Press, Washington, 1993.

(18) A titre d'exemple, dans son *Annual Threat Assessment*, en date du 12 février 2009, l'amiral Blair, actuel Director for National Intelligence, souligne la nécessité urgente de mettre en œuvre une stratégie de cyber-sécurité.

(19) En atteste la démission du Directeur de la cyber-sécurité du DHS, Rod Beckström, en mars 2009.

Gates, cette structure a été finalement absorbée par le Space Command de l'USAF.

Devant le besoin de centralisation, les autorités militaires américaines ont alors opté pour un Cybercommand assimilé à un Combatant Command, sur le modèle du Strategic Command (STRATCOM), déjà en charge, entre autres, de la dissuasion nucléaire et de la défense antimissiles. L'idée est donc bien de dépasser l'écueil de la désignation d'un corps d'armées (en l'occurrence l'Air Force) qui bénéficierait de la primauté dans le cyberespace, pour souligner qu'il s'agit, au contraire, d'un domaine interarmées.

Notons cependant que, en confiant la gestion du Cybercommand au lieutenant-général Alexander, jusqu'ici directeur de la National Security Agency, la Maison-Blanche a clairement fait comprendre que le nouvel arbitrage était plus favorable à l'expertise de la communauté du renseignement qu'à celle revendiquée par les armées (20). Ce choix, en apparence bénin, aura de fortes implications tant dans la formation des personnels que dans les axes d'effort mis en œuvre par ce nouveau commandement.

Certains experts, tels que James Carafano de la Heritage Foundation, s'inquiètent de cette dynamique. Pour Carafano, la centralisation institutionnelle induit une vulnérabilité de la chaîne décisionnelle, elle fait planer le risque de plaquer une gestion stricte et verticale sur un objet, le «cyber», par définition transversal et en constante évolution. Enfin, la centralisation, au niveau de l'exécutif signifie surtout que le Congrès aura un faible droit de regard en termes d'investigations potentielles sur les pratiques de la Maison-Blanche (21).

En France, outre l'ANSSI, les compétences sont encore éclatées entre de multiples acteurs. La cybercriminalité est suivie au ministère de l'Intérieur par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. La problématique des réseaux militaires est quant à elle gérée par la Direction générale des systèmes d'information et de communication au sein du ministère de la Défense. Et, depuis la parution du Livre blanc en 2008, des réflexions sont en cours pour créer une structure interarmées, sur le modèle américain.

Une doctrine encore embryonnaire

Comme mentionné plus haut, la Révolution dans les affaires militaires a conduit à des déclarations parfois baroques et douteuses de la part de *defense intellectuals*. Certains ont tenté de comparer le «cyber» à des domaines militaires existants : d'autres, citant Aristote ou Sophocle d'une façon peu convaincante pour mélanger rhétorique grecque et évolution technologique moderne, ont affirmé qu'une révolution copernicienne était

(20) Ellen NAKASHIMA, «Gates creates Cyber-Defense Command», *Washington Post*, 24 juin 2009.
(21) Entretien avec l'auteur, print. 2009.

en cours. Pourquoi tant d'affirmations étranges sur le cyberespace, les cyber-conflits ? D'où peut provenir cet ésotérisme ?

Tout cela semble rappeler ce que l'épistémologue Thomas Kuhn appelait «*une phase de science extraordinaire*». Dans son livre *The Structure of Scientific Revolutions*, Kuhn montre que la science n'est pas une évolution naturelle vers un progrès inexorable dans la connaissance. La communauté scientifique rencontre régulièrement des crises avec des phénomènes empiriques qui défient leurs idées centrales, leur paradigme fondamental (22). Puis vient la fameuse phase de «science extraordinaire», où tout, y compris des théories étranges, originales, voire douteuses, sont explorées afin de trouver un nouveau paradigme. En raison des trois problématiques (attribution, intentionnalité, rationalité collective) mentionnées plus haut, cette phase de «science extraordinaire» est la phase sur laquelle les forces armées dans le monde butent, face au cyberespace, depuis les quinze dernières années.

La même chose pouvait être dite de la littérature nucléaire publiée dans les années 1950 et 1960. A cette époque, personne ne pouvait nier les potentialités des armes nucléaires, telles que démontrées à Hiroshima et Nagasaki, mais, dans le même temps, personne non plus ne pouvait dire exactement ce que cela modifiait dans l'équilibre des forces de la Guerre froide. Cela prit des années et plusieurs travaux audacieux (de Bernard Brodie, Herman Kahn ou Albert Wolhstetter) pour édifier un savoir cohérent sur la stratégie nucléaire (23).

Jusqu'où la comparaison avec les cyber-conflits peut-elle aller ? Aujourd'hui, le cyber-champ n'a pas été dompté par les acteurs politiques. Certes, au cours des derniers mois, plusieurs publications officielles ont attesté d'un travail ambitieux de mise en œuvre d'une cyber-doctrine. En mai 2008, le colonel Williamson de l'Air Force publie un article vivement critiqué dans la revue *Armed Forces Journal* sur la création de *botnets* militaires à des fins offensives (24). Pour les ingénieurs en informatique, une telle posture offensive ne répond pas à la question initiale de la vulnérabilité des systèmes de communication américains.

De son côté, le général Chilton, à la tête du *Strategic Command*, défendait récemment dans une revue de l'Air Force, *Strategic Studies Quarterly*, l'idée d'une lutte informatique intégrée à l'architecture de dissuasion américaine au XXI^{e} siècle (25). Or, l'idée d'une cyber-dissuasion reste aujourd'hui imprécise. Sans capacité d'attribution d'une attaque, comment pourrait s'organiser un arsenal informatique de riposte ? En l'absence d'ennemi clai-

(22) Thomas KUHN, *The Structure of Scientific Revolutions*, University of Chicago Press, Chicago, 1970.
(23) Fred KAPLAN, *The Wizards of Armageddon*, Simon and Schuster, New York, 1983.
(24) Colonel WILLIAMSON, «Carpet bombing in cyberspace», *Armed Forces Journal*, mai 2008.
(25) Kevin CHILTON/Greg WEAVER, «Waging deterrence in the twenty-first century», *Strategic Studies Quarterly*, print. 2009.

rement identifiable, où placer le curseur ? Par conséquent, une cyber-dissuasion ne serait ici pas tous azimuts, mais tout simplement sans azimut.

Par ailleurs, compte tenu des rythmes d'innovation des outils informatiques, l'armée américaine reste partagée quant à l'efficacité d'une démonstration de capacités de contre-attaque. Celle-là tendrait à donner une indication précise des avancées technologiques du Département de la Défense. «*Nous ne pourrions disposer de cette capacité de démonstration, donc de dissuasion, qu'à partir du moment où nous disposons d'un avantage technologique inégalé et inégalable*» confie un officier supérieur américain, dans l'anonymat.

Dans les deux cas, la cyber-dissuasion semble devoir attendre une rupture technologique (par exemple pour tracer les intrusions) que les Américains n'identifient pas encore, mais qui pourrait accélérer les réflexions actuelles.

Malgré ces limites, le Pentagone poursuit ses efforts de doctrine. Mentionnons une idée importante défendue par le général Chilton : l'incertitude quant aux effets d'une contre-attaque dans le cyberespace pourrait devenir en soi un élément de dissuasion. Le chaos assuré par une riposte dissuaderait ainsi tout attaquant. Chilton écrit : «*les inquiétudes d'un rival quant aux conséquences non-intentionnelles pourrait renforcer les effets de notre dissuasion s'il souhaite maîtriser l'escalade militaire ou s'il craint les répercussions sur ses propres opérations*» (26). Soit la logique MAD (*Mutually Assured Destruction*) revisitée, en quelque sorte.

Pour sa part, l'armée populaire chinoise est prolixe en matière de réflexion doctrinale, y intégrant la dimension cybernétique. Depuis le fameux opuscule des deux colonels Qiao Liang et Wang Xiangsui, *La Guerre hors limites* (27), les attaques informatiques sont l'objet d'une intense littérature à Pékin. L'APL a ainsi adopté une stratégie de «guerre électronique intégrée», qui consiste à prendre le contrôle du flux d'informations de l'adversaire et à maintenir son info-domination sur le théâtre d'opération. Pour les stratèges chinois, la lutte informatique est donc devenue à la fois une phase préalable de campagne militaire et une option préemptive contre les systèmes d'information de l'ennemi (28). Les deux grands documents stratégiques de l'APL, *La Science de la stratégie militaire* et *La Science des campagnes*, présentent la supériorité informatique comme un moyen décisif de contrôler les milieux aérien et maritime. A cet égard, le mode opératoire se rapproche fortement de la pratique russe au cours de l'affrontement en Géorgie, en août 2008.

(26) *Ibid.*, p. 40.

(27) Liang QIAO/Xiangsui WANG, *La Guerre hors limites*, Payot/Rivages, Paris, 2003.

(28) Bryan KREKEL, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman (US-China Economic and Security Review Commission), oct. 2009, pp. 6-7.

A l'échelle internationale, l'OTAN a déjà placé le «cyber» sur son agenda, avec l'établissement de son Cooperative Cyber Defence Centre of Excellence (CCDCOE) à Tallinn. Les moyens du CCDCOE sont encore modestes et des incertitudes subsistent quant aux implications de l'OTAN en cas de cyber-attaques : l'article 5 du Traité de l'Atlantique-Nord s'applique-t-il si une des nations de l'Alliance fait face à de telles attaques ?

Du côté de l'Union européenne, si la European Network and Information Security Agency (ENISA) apparaît comme l'organisme idoine à l'échelon européen pour la sécurité des systèmes d'information, aucune réflexion politique ne semble avoir été engagée à Bruxelles sur la lutte informatique. Qui plus est, entre les initiatives otaniennes et européennes, ne risquerions-nous pas de rencontrer dans le cyberespace les mêmes dilemmes que dans d'autres secteurs ? Autrement dit, peut-on prédire des risques d'incohérence en matière de capacités de lutte informatique entre OTAN et UE comme il en existe, par exemple, entre la NATO Response Force et les Groupements tactiques de l'UE, au niveau de la génération de forces ?

Enfin, à un niveau global, comment les Nations Unies peuvent-elles être impliquées ? L'Organisation devrait-elle redéfinir son corpus juridique délimitant les «actes de guerre» pour inclure les cyber-conflits ?

Comme ce rapide tour d'horizon en atteste, les avancées doctrinales portant sur le «cyber» restent très embryonnaires, tant au niveau des Etats que des organisations internationales. D'où la nécessité de mettre en œuvre de véritables axes de recherche.

Pistes pour un agenda de recherche

Le fait que les décideurs civils et militaires aient besoin de clarté et de certitudes minimales est entièrement compréhensible, mais les calendriers politique et académique sont deux choses différentes : le premier ne doit pas précipiter ni parasiter le second.

Lors de nos recherches sur le cyberespace, un ingénieur informaticien confiait : «*les cyber-conflits sont un dossier trop sérieux pour le laisser aux nerds*». A nouveau, la stratégie nucléaire fut conçue après une longue bataille entre les scientifiques et les *defense intellectuals* quant à la légitimité des seconds sur le sujet. Dans les années 1940 et 1950, l'idée selon laquelle les politologues seraient compétents en matière de doctrine nucléaire semblait candide. Les sciences humaines et sociales étaient perçues comme tellement éloignées des réalités scientifiques et opérationnelles qu'elles devaient se limiter à des sujets mous (comme les ressources humaines dans l'armée). Nous faisons aujourd'hui face au même défi sur les cyber-conflits. Une fenêtre d'opportunité est ouverte pour un agenda de recherche sur le

cyberespace qui représenterait une vraie valeur ajoutée. Mentionnons ici deux axes qui pourraient figurer sur la feuille de route :

Examiner le phénomène de radicalisation à travers le cyberespace

La sociologie des mobilisations collectives devrait se tourner vers le cyberespace pour évaluer la façon dont celui-là modifie et devrait modifier, dans les années à venir, les processus de radicalisation pour les organisations sociales ou terroristes. Les événements autour des dernières élections en Iran ou les protestations en Egypte, pendant la guerre de Gaza, en décembre 2008 (29), ont montré que le cyberespace altère considérablement les formes de contestation. Qui sont sociologiquement ces acteurs ? Quelle est l'étendue de leurs cyber-compétences ? Représentent-ils une communauté émergente munie de sa propre identité ? Peut-on retracer des filières spécifiques de recrutement ? (30)

Intégrer les cyber-conflits dans une approche fluide des conflits contemporains

Comme nous l'avons explicitement dit ici, les cyber-conflits en eux-mêmes ne seront pas l'« Armageddon » de demain – contrairement à ce que serait une guerre nucléaire. Toutefois, ils peuvent constituer la première phase d'une campagne militaire plus étendue (comme les cyber-attaques russes en Géorgie, en août 2008). Ils peuvent être utilisés comme contournement de la puissance, à la manière des guérillas de la Guerre froide, comme affrontement de basse intensité dissuadant une montée aux extrêmes. Dans ce contexte, la cyber-guerre est une composante évidente du débat plus large sur la montée des «*guerres hybrides*» (31). A la suite des guerres en Iraq et en Afghanistan et plus particulièrement *via* le phénomène contre-insurrectionnel, les études stratégiques sont en train d'évoluer de manière à concevoir à la fois des formes classiques de conflits avec des formes irrégulières. Par conséquent, il est nécessaire de revenir sur des concepts pertinents : les postures offensive, défensive, dissuasive au regard des modalités conflictuelles dans le cyberespace. Des efforts majeurs ont déjà été accomplis. Dans un article de la revue *Politique étrangère*, en 2005, Aline Lebœuf soulignait déjà le défi analytique recouvert par l'interpénétration de multiples modes de conflit : «*le monde du conflit fluide se caractérise aussi par le nombre important de systèmes conflictuels observables simultanément. De façon banale, on peut aujourd'hui relever la coexistence de*

(29) Samantha SHAPIRO, «Revolution, Facebook-style», *New York Times*, 22 janv. 2009.

(30) *Cf.* le travail programmatique de Hsinchun CHEN/Wingyam CHUNG/Jialun QIN/Edna REID/Marc SAGEMAN/Gabriel WEIMANN, «Uncovering the dark web : a case Study of Jihad on the Web», *Journal of the American Society for Information Science and Technology*, vol. LIX, n° 8, pp. 1 347-1 359.

(31) Frank HOFFMAN, *Conflict in the 21st Century : The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2008.

conflits interétatiques classiques, de guerres civiles, de systèmes conflictuels mixtes (inter-et intra-étatiques). Mais, au-delà, la nouveauté est que les systèmes conflictuels combinent les caractéristiques de conflits jusque-là strictement séparés dans nos classifications guerrières» (32).

C'est dans ce spectre mouvant de la conflictualité que la cyber-guerre doit être pensée. Cet effort intellectuel permettra non seulement de mieux définir les modes de conflit contemporains, mais aussi de dégager des conclusions opérationnelles quant aux déterminants d'une cyber-défense efficace.

A l'heure où l'Internet Corporation for Assigned Names and Numbers (ICANN), l'organisme en charge de l'assignation des adresses Internet, est en passe d'être privatisée par l'administration Obama (33), la question de la gouvernance du cyberespace et, plus particulièrement, des aspects sécuritaires et militaires est donc ouverte. A ce titre, elle représente une réelle opportunité de collaboration entre décideurs et chercheurs : des agendas différents n'induisent pas des objectifs différents.

(32) Aline Lebœuf, «Les conflits fluides : concepts et scénarios», *Politique étrangère*, sept. 2005, p. 637.
(33) Laurent Chicola, «Le contrôle de l'ICANN : un enjeu diplomatique», *Le Monde*, 29 sept. 2009.