La cyberguerre

La cyberguerre remet en cause tous les schémas traditionnels de l'art de la guerre. Il n'y a plus d'attaque frontale, l'ennemi agit masqué. De même, les Etats ne sont plus les seules cibles : la sphère privée fait elle aussi l'objet d'attaques, notamment dans le cadre de la guerre économique.
Toutes les armées du monde se doivent d'intégrer cette nouvelle donne dans la conception de leur stratégie militaire.

par Nicolas ARPAGIAN*

Nous allons pour commencer préciser un point de vocabulaire relatif au mot de « cyberguerre ». Un débat a agité les experts en polémologie pour savoir si l'on pouvait ou non utiliser le terme de « guerre » pour décrire les usages offensifs de l'Internet et des technologies de l'information. La guerre désignant couramment la confrontation de forces armées sur un théâtre d'opération, avec à la clé un possible engagement de la vie humaine.
S'il ne s'agit certainement pas de contester l'intérêt d'une réflexion sémantique à ce propos, on peut reconnaître néanmoins l'efficacité du mot « cyberguerre ». Facilement compréhensible, il permet à un large public de prendre conscience des enjeux stratégiques que revêtent les territoires numériques auxquels nous confions un peu plus chaque jour de notre autonomie : données financières, médicales, industrielles, militaires…
On devrait davantage parler de *cyberguerilla,* dans l'esprit de la stratégie du faible au fort de Thomas E. Lawrence fondée sur le harcèlement, le faible obligeant le fort à mobiliser des forces importantes pour faire face aux multiples assauts émanant d'individus ou de groupes disséminés.
Il convient, au préalable, de préciser que la « cyberguerre » repose sur deux piliers :
• les « tuyaux », avec la capacité à espionner, altérer, suspendre ou interrompre les systèmes de communication et d'information de la cible visée ;
• les contenus, avec une capacité à agir sur l'information disponible en menant des campagnes de dénigrement, en prenant le contrôle de données stockées ou en rendant celles-ci inaccessibles.

Cette « cyberguerre » des années 2000 est un enfant de la RMA – *Revolution in Military Affairs*, cette doctrine du Pentagone qui désigne l'adaptation du système militaire aux technologies numériques, avec cet objectif : Regarder de l'autre côté de la montagne.
Cette Révolution Technologique Militaire date des années 1970 et prend sa source dans l'ex-URSS.
En effet, des théoriciens soviétiques parlent alors de « nouvelles méthodes tactiques » et pensent les nouvelles technologies de l'information et de la communication (NTIC) comme un changement de paradigme.
Au seuil des années 1990, des spécialistes étatsuniens reprennent le thème et lancent le slogan de la RMA. Pour résumer, cette RMA est le complément de la révolution numérique dans la société civile et incarne le passage à l'économie de l'immatériel.
Les militaires étaient déjà très présents : Internet étant la continuité d'ARPANET, le réseau de communication né de la guerre froide.
Cette introduction croissante des technologies de l'information vise à « Dissiper le « brouillard de la guerre », si cher à Clausewitz.

* Rédacteur en chef de la revue *Prospective Stratégique*, Nicolas Arpagian est Directeur scientifique du cycle « Sécurité Numérique » à l'Institut National des Hautes Etudes de la Sécurité et de la Justice (INHESJ). Il est également Chargé de cours à l'Institut des Relations Internationales & Stratégiques (IRIS). Ses récents ouvrages sont : *La Cybersécurité* (Collection *Que Sais-Je ?* – Presses Universitaires de France, paru en septembre 2010). *L'Etat, la Peur et le Citoyen – Du sentiment d'insécurité à la marchandisation des risques* (Vuibert, 2010), *La Cyberguerre – La guerre numérique a commencé* (Vuibert, 2009) ou *Liberté, Egalité… Sécurité* (Dalloz, 2007). Site Internet : www.arpagian.net

Pourtant, cette cyberguerre va mettre à mal des principes établis par ce même Clausewitz.

A commencer par sa définition de la guerre, qu'il présente comme « un acte de violence destiné à contraindre l'adversaire à se soumettre à notre volonté ».

Avec Internet, on va s'attacher à convaincre son ennemi de renoncer à faire la guerre.

Par exemple, lors du conflit russo-géorgien de l'été 2008, l'aviation géorgienne (18 appareils) a été clouée au sol, victime d'une attaque informatique préalable. « Autrefois », ces appareils auraient été abattus en vol… L'usage de la violence n'est donc plus forcément la règle.

Autre recommandation énoncée par Clausewitz : « connais ton ennemi ». La particularité de ces cyberconflits est que précisément on ne peut pas être certain de l'identité de l'attaquant. On peut en avoir l'intuition, la conviction…, mais on ne dispose pas de preuve formelle et indiscutable.

Lors de l'attaque informatique de grande ampleur menée contre l'Estonie au printemps 2007, les autorités de l'OTAN ont renoncé à appliquer l'article 5 du Traité de l'Atlantique Nord. Comment, en effet, désigner avec certitude l'assaillant ?

La vraie rupture de cette RMA est que l'on passe d'une logique de « Faire la guerre qui correspond à ses armes » – la règle générale non écrite de l'Histoire de la guerre, puisque ce n'est généralement qu'après l'acquisition d'une arme qu'est définie la tactique lui correspondant – à la logique de « Fabriquer les armes qui correspondent à la guerre » (que l'on veut mener). C'est là une percée majeure dans l'histoire de la préparation de la guerre.

L'autre spécificité de cette cyberguerre est la forte imbrication existant entre le Public et le Privé.

Une firme comme Google, fondée en 1998, traite désormais d'égal à égal avec un Etat comme la Chine.

Et les Etats investissent le champ des entreprises privées. Par exemple, en octobre 2009, la CIA investit via son fonds *In-Q-tel* dans la veille de médias sociaux, en établissant un partenariat avec la firme *Visible Technologies*, qui est un fournisseur de solutions de gestion de marques et d'analyse des contenus de médias sociaux.

Il s'agit pour l'agence étatsunienne de disposer de ses propres outils de veille pour assurer le suivi des conversations échangées sur les réseaux sociaux, *blogs* et autres plateformes d'échanges.

Dans un discours (1) du 29 mai 2009, Barack Obama a indiqué que les entreprises participaient pleinement à la sécurité nationale, surtout dans le domaine des technologies de l'information. Cette position a de nouveau été clairement exprimée dans la *US National Security Strategy* de mai 2010 (qui comporte un important volet cybernétique : le *Cyberspace Policy Review (2)*). A qui ira, en priorité, la fidélité de ces prestataires privés ? A leurs clients, ou aux autorités de leur pays ?

La capacité d'un pays à disposer d'une industrie informatique performante participe donc de sa stratégie de souveraineté nationale.

A l'avenir, les conflits opposeront de moins en moins les Etats-nations, mais feront intervenir des guérillas, des réseaux mafieux, des mouvements terroristes, des militants, des puissances financières, des organisations non gouvernementales… Ces acteurs seront parfois difficiles à identifier et leurs structures de fonctionnement, non hiérarchiques et non centralisées, renforceront cette logique de dispersion.

Comme le disait Ou-Tsé, on fait la guerre pour l'une des cinq raisons suivantes :

- l'amour de la gloire,
- l'envie d'acquérir,
- la perversion,
- l'anarchie intérieure,
- le désespoir.

Tous ces sentiments peuvent conduire un individu ou un collectif à mener des cyberattaques, sans, par ailleurs, avoir été préalablement identifié par les services de sécurité nationaux. Cette cyberguerre va donner l'occasion à chacun (activiste, militant, minorité…) de devenir acteur de cet affrontement asymétrique.

On ne se bat plus entre acteurs de même nature juridique (Etat/Etat, Entreprise/Entreprise…) ni de même taille. On systématise la logique du judo, où un plus petit peut faire vaciller un plus gros.

Ainsi, en décembre 2009, Washington (3) a reconnu que les activistes irakiens avaient été en mesure d'intercepter les transmissions d'images émises par les drones *Predator,* avec un logiciel comme *SkyGrabber*, qui coûte 26 $. Ou comment l'utilisation judicieuse d'une technologie à bas prix a pu contribuer à mettre en échec des équipements représentant, à l'unité, des millions de dollars. En l'espèce, l'idée que des Irakiens puissent accéder à ces données non cryptées n'avait, semble-t-il, à aucun moment effleurer l'esprit des brillants stratèges de l'état-major étatsunien.

Attention, d'ailleurs, à ne pas verser dans le mirage technologique. La guerre ne peut et ne pourra se résumer à une simple accumulation d'outils *high tech.* La situation en Afghanistan le démontre amplement : la détention de matériels très sophistiqués ne peut en aucun cas garantir la victoire. Dans leur ouvrage *La guerre ne fait que commencer (4)*, le criminologue Alain Bauer et l'universitaire Xavier Raufer racontent la manière dont, au Kosovo, « le climat, la ruse paysanne et les leurres grossiers ont mystifié les armements de haute technologie de l'OTAN ». Et d'évoquer comment il suffisait aux Serbes de brancher deux minutes

(1) Disponible sur le site de la Maison Blanche : http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

(2) Accessible sur http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

(3) *Insurgent hack US Drones* par Siobhan Gorman, Yochi J. Dreazen et August Cole, *The Wall Street Journal*, 17 décembre 2009. http://online.wsj.com/article/SB126102247889095011.html

(4) *La guerre ne fait que commencer,* d'Alain Bauer et Xavier Raufer, 2002, Editions Jean-Claude Lattès.

leurs radars avant de les éteindre pour que les missiles de croisière supposés les détruire soient désorientés, pour, *in fine,* rater systématiquement leur cible. Il en a été de même lorsque de vieux poêles disséminés dans des champs ou des carcasses de camions à peine repeintes ont pu faire croire à des radars de dernière génération qu'il s'agissait d'affûts de canons ou de chars, mobilisant ainsi les troupes de l'OTAN, l'aviation, ainsi que d'importants stocks de munitions.

De quoi incarner la prédiction des colonels de l'armée chinoise MM. Quiao Liang et Wang Xiangsui, qui, dans leur essai *La Guerre hors limites (5)* (1999), prédisaient que « Sur les champs de bataille du futur, les forces numérisées risquent fort de se retrouver comme le grand cuisinier qui excelle à préparer des homards au beurre. Face à des guérilleros qui s'obstinent à manger des épis de maïs, elles n'auront plus que leurs yeux pour pleurer ».

Les « Sociétés de l'information » devaient réduire les risques, les conflits… bref, les incertitudes. Or, plus il existe de moyens de savoir et de transmettre, plus il y a, comme le souligne l'universitaire François-Bernard Huyghe, de risques de dissimulation et de falsification. Depuis la fin des années 1990, on annonce un « Pearl Harbor informatique » ou un « Waterloo Digital ». Juste avant la prise de fonction du Président Obama, le FBI a communiqué sur la menace d'un *Cybergeddon*, sorte d'*Armageddon cybernétique*, en référence au Livre de l'Apocalypse de la Bible. Et le secrétaire d'Etat adjoint américain à la Défense révèle, en 2010, sur le site Internet (6) de son ministère, que lorsqu'on lui demande ce qui l'empêche de dormir, il répond immédiatement : « les cyberattaques ». Avec l'infoguerre s'ouvre l'éventail des objectifs : il ne s'agit plus seulement de vaincre des corps d'armées, mais, aussi de s'en prendre à des infrastructures civiles et, plus largement, à l'esprit de populations entières.

Les équipements informatiques contaminés dès l'origine !

Au mois de mai 2008, plusieurs institutions de la défense des Etats-Unis (l'Ecole navale, le Centre de guerre aéronavale, la principale base aérienne américaine en Allemagne (à Spangdahlem) …), mais également la firme *Raytheon,* qui fabrique, notamment, le missile *Patriot* rendu célèbre pour son efficacité contre les *Scuds* irakiens pendant la première Guerre du Golfe, ont été alertées par le FBI sur les fortes présomptions (7) pesant sur les serveurs *Cisco Systems* et autres équipements informatiques achetés dernièrement par ces honorables entités, qui seraient en fait des contrefaçons d'origine chinoise. Plus grave encore, ces équipements *high tech* contiendraient des logiciels facilitant l'intrusion et la navigation dans les réseaux informatiques auxquels ils sont reliés. Ils constituent ainsi une porte d'entrée hors pair dans les coulisses de la défense des Etats-Unis.

En juin 2009, Pékin a souhaité, au nom de la lutte contre la pornographie, que tout ordinateur fabriqué en Chine soit équipé d'un logiciel filtrant les contenus pornographiques, le logiciel *Green Dam (*le « barrage vert d'escorte de la jeunesse »), avec le risque de voir inclus dans les listes des sites bloqués pour obscénité des contenus sensibles sur le plan politique. Face au tollé international, c'est la règle du volontariat qui a finalement été retenue.

Au printemps 2010, la polémique rebondit en France avec les interrogations pesant sur l'intégrité des clés 3G commercialisées par les équipementiers chinois ZTE et Huawei.

On assiste ainsi à de nouvelles formes d'attaque, comme ce fut le cas avec le piratage du projet de chasseur américain *F-35 Joint Strike Fighter*. Le *Wall Street Journal* a découvert, en 2009, que des *hackers* étaient parvenus à voler des informations concernant le programme de développement de l'avion de chasse F-35, en profitant de failles de sécurité dans les réseaux informatiques de plusieurs entreprises partenaires du projet (*Lockheed Martin*, *Northrop Grumman* et *BAE Systems*). En réaction à l'évocation de l'origine chinoise de ces attaques, l'ambassade de Chine à Washington a répondu que le pays « bannit toute forme de cyber-délit ».

Là encore, on constate que l'offensive porte sur les équipements et se déroule bien en amont d'un éventuel conflit. On cherche à s'insérer dans les infrastructures informatiques pour – le moment venu – exploiter cette connaissance intime du système de défense de l'adversaire.

Global par nature, le réseau des réseaux ne dispose pas d'un cadre juridique international à la mesure du caractère planétaire de la Toile. En effet, il n'existe pas à proprement parler, aujourd'hui, de droit international du Net.

C'est une juxtaposition de droits nationaux voire régionaux, comme, par exemple, au sein de l'Union européenne.

Le seul texte de dimension internationale est la Convention sur la cybercriminalité de Budapest en date du 23 novembre 2001 du Conseil de l'Europe. Mais, là encore, il faut s'intéresser à la réalité matérielle de ce texte. Si quarante-trois Etats l'ont déjà signée, on constate cependant que de grandes démocraties, comme l'Autriche, la Belgique, l'Espagne, la Grèce, la Pologne, le Royaume-Uni ou la Suisse, n'avaient toujours pas ratifié ce texte en 2010. Soit près d'une décennie plus tard…

Ensuite, les différentes organisations internationales se sont décidées à traiter partiellement le sujet de la cybersécurité en se dotant de déclarations ou d'entités dédiées. C'est, par exemple, le cas de l'OTAN, qui a ouvert un centre d'analyse sur le sujet à Tallinn (capitale de l'Estonie), du G-8 qui a créé un dispositif d'alerte 24 h sur 24, de l'ONU qui a organisé, en 2003 et 2005,

(5) Quiao Liang et Wang Xiangsui, *La Guerre hors limites*, édition originale 1999. Traduction française, 2003, Editions Payot & Rivages.

(6) http://www.defense.gov/news/newsarticle.aspx?id=57871

(7) *FBI : China may use counterfeit Cisco routers to penetrate US networks,* 15 mai 2008, www.worldtribune.com

des Sommets mondiaux sur la société de l'information (sommets dont les résultats restent néanmoins limités), de l'OCDE, qui fut la première en 1982 à signaler les risques d'infractions informatiques… et jusqu'au Secrétaire général de l'Union Internationale des Télécommunications, qui, lors du Forum de Davos en 2010, a eu l'idée d'un traité international contre les cyberattaques. Une initiative jugée sympathique… mais restée sans suite.

De son côté, l'Union européenne a donné naissance, en 2004, à une agence dédiée à la sécurité des systèmes d'information : l'ENISA (8). Fait curieux, on ne lui a accordé, dès sa naissance, qu'une durée de vie de cinq ans ! Pas de quoi motiver les fonctionnaires qui ont été détachés à Heraklion en Crête, où se trouve le siège de l'agence. D'autant plus qu'avec seulement huit millions d'euros de budget annuel, elle ne pouvait que mener des actions d'ampleur limitée. En 2008, son existence a été prolongée jusqu'au 13 mars 2012. Avec de telles échéances à courte vue, on comprend aisément que le sujet ne sont pas jugé prioritaire par les Etats membres.

Il s'agit pour les états-majors d'intégrer ces technologies de l'information dans le management des troupes, à l'instar des *milblogs*, ces sites personnels tenus et rédigés par des militaires, où ils y livrent leurs ressentis sur leur vie au quotidien, que ce soit ou non en opération. Par ailleurs, en 2010, l'armée israélienne a été obligée d'annuler une intervention suite à l'annonce qu'en avait faite un jeune appelé sur sa page *FaceBook*. En mai 2010, l'hebdomadaire allemand *Der Spiegel* a expliqué comment le Hezbollah avait créé sur *FaceBook* le profil d'une demoiselle nommée Reut Zukerman, qui aurait convaincu deux cents soldats ou réservistes israéliens de devenir ses « amis ». Ils auraient ainsi communiqué des noms de soldats, apporté des précisions sur le jargon militaire, décrit des bases militaires… A l'inverse, les Israéliens reconnaissent avoir utilisé la plateforme de *microblogging Twitter* et *FaceBook* pour recruter des informateurs palestiniens dans la bande de Gaza. Une unité *FaceBook* a été également constituée au sein de Tsahal, l'armée israélienne, afin de mieux gérer les réseaux sociaux.

Il est intéressant de noter que les doctrines des armées, en la matière, évoluent. Ainsi, en mars 2010, l'*US Army* donne à nouveau le feu vert à l'accès aux réseaux sociaux à partir des ordinateurs de l'armée, après l'avoir interdit à partir de l'été 2009. Ses principales motivations étaient à l'époque les suivantes : empêcher l'intrusion de logiciels malveillants et éviter aux militaires concernés de divulguer publiquement des informations confidentielles.

Le *Department of Defense* américain autorise donc à nouveau les militaires à accéder à des sites comme *Twitter, FaceBook* ou *Youtube*, sous réserve que « l'utilisation de ces platesformes Web 2.0 ne compromette pas la sécurité des infrastructures et ne permette de révéler aucune information confidentielle ». Toutefois, afin d'être en mesure de protéger les réseaux militaires contre la prolifération de virus informatiques et les attaques de *hackers*, le Pentagone se réserve le droit de « limiter temporairement » l'accès à ces réseaux sociaux « afin de maintenir la sécurité lors des opérations militaires ou pour préserver la bande passante ».

Dans la mesure où la cyberguerre ne se limite pas à espionner ou à chercher à prendre le contrôle des équipements adverses, mais vise également à rivaliser sur le terrain de l'information disponible sur la Toile, cela suppose d'y consacrer d'importants moyens, notamment humains. La Chine dispose, par exemple, de milliers d'internautes rémunérés pour délivrer en sa faveur des commentaires « positifs » et orienter ainsi les débats sur le Net.

Face à de tels facteurs d'insécurité, les Etats-Unis réfléchissent à la mise en place d'un réseau Internet qui leur serait propre. En octobre 2009, la DARPA (*Defense Advanced Research Projects Agency*), l'agence de recherche de l'armée américaine, a annoncé avoir confié à plusieurs entreprises le développement d'un protocole de réseau militaire (MNP, « Military Network Protocol ») distinct du protocole TCP/IP actuellement utilisé sur Internet. Parmi les prestataires, on trouve *Lockheed Martin*, *Juniper Networks*, *Microsoft*, mais également l'université de Stanford. Le projet devrait disposer d'un financement de quelque 31 millions de dollars. Ultra-sécurisé, ce nouveau protocole réseau offrira un système de priorités accordées aux utilisateurs et aux machines connectées et sera capable d'allouer dynamiquement la bande passante disponible entre les utilisateurs ou les groupes d'utilisateurs. Une sorte d'Internet II donc, mais réservé aux militaires (un retour aux sources en quelque sorte !).

On estime que les dépenses des autorités fédérales américaines en matière de sécurité informatique atteignent aujourd'hui les 10 milliards de dollars (7,1 milliards d'euros) par an. Cette demande de sécurité informatique ne concerne plus seulement le Pentagone, mais s'étend également aux organismes de santé, aux agences de l'énergie et aux autres éléments essentiels de l'infrastructure nationale.

La diversité des types d'attaques possibles et la créativité qu'il convient de développer pour élaborer des ripostes ou des contre-mesures adaptées vont obliger les armées à diversifier leurs modes de recrutement. Ainsi, les Etats-Unis ont lancé en juillet 2009 un *US Cyber Challenge (9)*. C'est un concours national destiné à recruter de jeunes informaticiens appelés à constituer la cyberdéfense du pays. Le programme est ambitieux ; le concours ouvert en 2009 prévoyait le recrutement de dix mille recrues. L'opération devrait être renouvelée régulièrement : rien de mieux pour identifier les bons profils susceptibles d'intéresser les autorités étatsuniennes.

Cette cyberguerre revêt donc des aspects multiples (managériaux, informationnels, technologiques…) et

(8) Son site Internet : http://www.enisa.europa.eu/

(9) http://www.uscyberchallenge.org/

se situe à la croisée des chemins universitaire, industriel, militaire, politique et diplomatique. Autant de composantes qui exigent une réflexion sur cet environnement où certains opérateurs commerciaux disposent d'une puissance supérieure à celle de bien des Etats. A l'instar du nucléaire, qui fut doté, en son temps, de doctrines d'emploi, il serait souhaitable que les Etats se donnent les moyens de bâtir un tel *corpus* pour cet univers cybernétique. L'enjeu est planétaire et le calendrier s'accélère, au fur et à mesure que nous nous abandonnons à une certaine dépendance numérique.