Mythes et réalités des cyberguerres

par **Jean-Loup Samaan**

Jean-Loup Samaan, ancien *Visiting Scholar* à la RAND Corporation (Washington D.C.), a publié *Les Métamorphoses du Hezbollah* (Paris, Karthala, 2007).

On peut aujourd'hui identifier les niveaux physique, syntaxique, et sémantique, qui constituent le cyberespace. Pour autant, il est plus difficile de spécifier la cyberguerre, notion qui semble recycler des conceptions stratégiques assez classiques. Même si le *big bang* qui nous renverrait hors de l'âge informationnel reste un mythe, il faut se préparer à des opérations utilisant les moyens constitutifs du cyberespace. Et pour ce faire, la coopération avec le secteur privé est essentielle.

politique étrangère

Il y a plus de vingt ans, lorsque William Gibson publia son roman *Neuromancien* – sur un informaticien pourchassé dans l'espace virtuel, le *cyberspace* –, les choses semblaient bien confuses et en laissèrent perplexe plus d'un[1]. Or, à l'automne 2007, la perplexité a apparemment laissé place aux convictions, et l'US Air Force a annoncé en grande pompe la création de son tout nouveau Cybercommand, un commandement composé d'environ 600 officiers. De son côté, le dernier *Livre blanc sur la défense et la sécurité nationale* français annonce que « dans la mesure où le cyberespace est devenu un nouveau champ d'action dans lequel se déroulent déjà des opérations militaires, la France devra développer une capacité de lutte dans cet espace[2] ».

Aujourd'hui, le terme de « cyberespace » fait donc partie du langage commun et le Département de la Défense américain en a même une définition propre : « 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[3] ».

1. W. Gibson, *Neuromancien*, Paris, J'ai Lu, 2001. Voir sur cette généalogie, le blog du magazine américain *Wired* : <blog.wired.com/defense/2008/05/pentagon-define.html>.
2. *Défense et sécurité nationale : Le Livre Blanc*, Paris, éditions Odile Jacob/La Documentation française, 2008, p. 53.
3. US Department of Defense, *National Military Strategy for Cyberspace Operations*, Washington D.C., Département de la Défense, 2006.

On peut tenter de circonscrire ce domaine. Les experts en sécurité des réseaux reconnaissent trois strates constitutives du cyberespace : la strate *physique*, la strate *syntaxique* et la strate *sémantique*. La strate physique se compose des infrastructures, des câbles, des routeurs et commutateurs : il s'agit de la face la plus concrète du cyberespace. La strate syntaxique met en liaison les deux autres strates en formatant les informations contenues dans le cyberespace, en leur conférant des standards, des protocoles – tel le TCP/IP sur lequel repose Internet. Enfin, la strate sémantique désigne les données brutes véhiculées par le cyberespace et exploitées par les humains ou les machines. Ces informations peuvent aller du simple courriel reçu, jusqu'aux images de reconnaissance transmises par un drone aérien à sa station de contrôle en Irak.

Par quel truchement le cyberespace est-il donc passé de la science-fiction à la science militaire ? Théorisés avec plus ou moins de bonheur dans les années 1990, les concepts qui entourent cette notion se sont véritablement imposés sur le devant de la scène au printemps 2007 dans le sillage d'attaques informatiques ciblant les serveurs du Pentagone et de ce qui, au même moment en Estonie, sera bientôt identifié comme la « première cyberguerre ».

Le 26 avril 2007 à 10 heures, à Talinn, une vague inhabituelle de messages électroniques arrive sur l'ensemble des sites Internet gouvernementaux, provoquant un encombrement tel qu'une *emergency response team* est déployée dans les heures qui suivent. En vain : le premier jour, on compte 1 000 attaques par heure, le lendemain on monte à 2 000. Les sites sont progressivement fermés, certains pour quelques heures, d'autres pour plusieurs jours. Les dernières attaques ont lieu le 18 mai, concluant trois semaines de blocage au total.

L'enquête aura bien du mal à identifier un responsable particulier, l'origine des attaques ayant été localisée dans plus de cinquante pays. Néanmoins, faut-il voir une simple coïncidence dans le fait que l'offensive électronique contre l'État estonien se soit produite en pleine controverse autour de la statue du « soldat de bronze » soviétique, héros de la Seconde Guerre mondiale que le Parti de la réforme estonien, vainqueur des élections la même année, entendait déplacer ? Il n'en fallut pas plus pour voir dans les « cyberattaques » du printemps 2007 la main invisible du Kremlin – le secrétaire américain de l'US Air Force Michael Wynne s'empressant alors de déclarer que « la Russie, notre *nemesis* de la guerre froide, semble être la première à s'être engagée dans la voie de la cyberguerre ». Jaak Aaviksoo, ministre de la Défense estonien, renchérit en évoquant « la Troisième Guerre mondiale passée inaperçue[4] ».

4. Communiqué de presse du ministère estonien de la Défense, « Internet : xxist Century Battlefield », 16 juin 2007.

Parce que les déclarations politiques se mêlent ici à des constats stratégiques parfois approximatifs, il importe de comprendre plus exactement les enjeux qui se cachent derrière l'actualité. Que détermine le cyberespace et dans quelle mesure peut-il être conçu comme un espace conflictuel autonome ? Qu'y a-t-il là de nouveau ? Quelle est, à l'heure actuelle, la faisabilité stratégique de la cyberguerre ? Et quels doivent être les chantiers prioritaires pour les décideurs publics ?

L'incertaine genèse de la *cyberwar* à l'américaine

Si ARPANET, l'ancêtre d'Internet, date de la fin des années 1960, la problématique du cyberespace émerge dans la littérature stratégique au lendemain de la guerre froide, alors que la dynamique entre acquisition du renseignement et action militaire se précise sur le terrain de la guerre du Golfe grâce aux innovations en matière de technologies de l'information et de la communication (TIC) développées dans les décennies précédentes[5]. Les années 1990 voient proliférer les travaux aux accents messianiques sur cette révolution dans les affaires militaires (Revolution in Military Affairs, RMA), où l'exploitation des interfaces électroniques ne figure que comme une composante parmi d'autres. De la révolution informationnelle des futurologues Alvin et Heidi Toffler à l'étrange « guerre néo-corticale » de l'iconoclaste colonel Richard Szafranski, le Pentagone se met à lire et écrire sur la guerre à l'âge de l'information. L'*information warfare* est née[6]. À ce titre, il importe de constater une fois encore comme notre logique stratégique demeure tributaire de la littérature américaine : les débats entre stratégistes de Washington sur les cyberguerres irriguent les orientations décisionnelles en France, comme dans la plupart des pays de l'Organisation du traité de l'Atlantique nord (OTAN).

C'est en Californie, en 1993, que deux chercheurs de la RAND – John Arquilla et David Ronfeldt – publient l'article intitulé « Cyberwar is Coming! » dans la revue académique *Comparative Strategy*[7]. Derrière un titre devenu emblématique, les auteurs avancent que la cyberguerre, fondée et axée sur l'information à travers des interfaces électroniques, est en passe de provoquer une véritable refonte des organisations militaires.

---

5. J.-P. Maulny, *La Guerre en réseau au XXIe siècle : Internet sur les champs de bataille*, Paris, éditions Le Félin, 2006.
6. On trouve les prémices du concept d'*information warfare* chez Th. Rona, *Weapons System and Information at War*, Chicago (IL) Boeing Aerospace, juillet 1976.
7. J. Arquilla, D. Ronfeldt, « Cyberwar is Coming ! », *Comparative Strategy*, vol. 12, n° 2, printemps 1993, p. 141-165.

Cet article fondateur contient en lui-même l'ambiguïté première qui ne cessera d'entourer les réflexions sur les cyberguerres. La « cyberguerre » est-elle le moyen ou la fin de la conflictualité à venir ? Pour J. Arquilla et D. Ronfeldt, c'est assurément un moyen, qui permet de décentraliser les armées, d'assouplir les chaînes de commandement, et donc de consacrer la figure emblématique du « caporal stratégique[8] ». En quelque sorte, la cyberguerre serait l'expression technique de la guerre en réseau, formule qui décrit la nature des conflits futurs.

Les premiers échos de l'article sont plutôt mauvais, et la thèse des auteurs est accueillie par un très large scepticisme. Ce n'est que lorsque certains officiels du Pentagone – comme le capitaine Dick O'Neill, alors au cabinet du secrétaire à la Défense – se laissent séduire qu'Arquilla et Ronfeldt voient leur travail reconnu.

Pour certains, cet article aurait eu un impact certain sur la doctrine militaire américaine. Si le document programmatique *Joint Vision 2010*[9] supervisé en 1995 par le général John M. Shalikashvili, alors chef d'état-major, ne mentionne guère l'*information warfare* ou le *cyberspace*, le document *Joint Vision 2020*[10], publié cinq ans plus tard, souligne que « le développement continu et la prolifération des technologies de l'information changent la conduite des opérations militaires[11] ».

À la suite d'Arquilla et Ronfeldt, deux notions centrales de l'art opératif militaire émergent : la guerre réseau-centrée et le système de systèmes[12]. Développés au sein même du Pentagone, ces concepts articulent l'arrivée des innovations technologiques des décennies précédentes avec une refonte fondamentale des modes d'action des armées. Grâce à l'ensemble des systèmes d'information et de commandement reliés entre eux, le soldat moderne s'insère dans une architecture en réseaux dont il devient lui-même un « système ».

Tout semble alors conduire à un inventaire à la Prévert, où se mêlent les termes d'*information warfare*, *information-aged warfare*, *noopolitik*, *swarming*

8. L'expression entend souligner l'imbrication des niveaux autrefois cloisonnés de la stratégie et de la tactique, du fait de l'exploitation des nouvelles technologies sur le champ de bataille. Le terme ne passera à la postérité que six ans plus tard avec l'article du général C. C. Krulak, « The Strategic Corporal: Leadership in the Three Block War », *Marines Magazine*, vol. 28, n° 1, janvier 1999, p. 32.
9. US Department of Defense, *Joint Vision 2010, America's Military Preparing for Tomorrow: Quality People Trained, Equipped and Ready for Joint Operations*, Washington, D.C., Joint Chiefs of Staff, 1995.
10. US Department of Defense, *Joint Vision 2020*, Washington, D.C., Joint Chiefs of Staff, 2000.
11. Voir R. Grant, *Victory in Cyberspace*, Airlington, rapport spécial de l'US Air Force Association, octobre 2007, p. 15, disponible sur <www.afa.org/media/reports/victorycyberspace.pdf>
12. A. Cebrowski, J. Gartska, « Network-centric Warfare, its Origin and Future », *Proceedings*, vol. 124, n° 1, janvier 1998 ; Amiral W. Owens, « The Emerging U.S. System-of-Systems », *Strategic Forum*, n° 63, février 1996.

warfare, *netwar*, *network-centric warfare*, etc. L'une des conséquences les plus claires de la fin de la guerre froide est probablement l'inflation de paradigmes dits « nouveaux », de concepts, de théories, d'idées en tous genres, qui font passer de vieilles croyances pour des révolutions et donnent l'impression que la communauté stratégique entend désormais concurrencer le monde des publicistes et concepteurs en marketing.

Placée devant un tel magma, l'administration militaire américaine fut bien en peine d'établir une cohésion intellectuelle susceptible de consolider un nouveau savoir stratégique. Le Pentagone décida d'inclure désormais sous le vocable des *information operations* les opérations psychologiques, les ruses militaires, la sécurisation des opérations[13], les opérations informatiques en réseau et la guerre électronique. Cette fusion d'éléments hétérogènes n'allait qu'ajouter à la confusion ambiante[14].

Parce que la genèse des cyberguerres nous enseigne qu'il n'y a pas, à ce jour, de savoir consensuel sur le sujet, on peut mieux saisir comment les années 1990 et l'*information warfare* anticipaient déjà les errements conceptuels contemporains. Arquilla et Ronfeldt ne se reconnaissent plus dans ce que le Département de la Défense américain – et par extension les alliés transatlantiques – présente sous ce vocable. Tout d'abord, le rôle central de l'information dans le conflit n'est pas une idée neuve : avec un peu de chance, une page prise au hasard de *L'Art de la guerre* de Sun Tzu[15] nous le rappelle. Comme souvent, il s'agit moins ici d'une révolution que de l'arrivée à maturation de nouveaux modes de communication et de transmission de l'information.

Les usages tactiques de l'information pour tromper l'adversaire ou le démoraliser n'ont pas attendu que Szafranski fasse du cortex de l'ennemi le centre de gravité des nouveaux conflits. A-t-on vraiment besoin de créer l'expression « guerre néo-corticale » pour comprendre que la première cible dans un combat est le moral de l'adversaire ? Enfin, la guerre électronique – variante de la *cyberwar* – n'a pas attendu la fin de la guerre froide pour exister : elle l'avait précédée[16]. Qu'un ennemi puisse brouiller des communications, décoder des messages cryptés et sérieusement endommager les infrastructures par ce biais n'est pas nouveau.

---

13. Ou processus d'identification d'informations critiques susceptibles de mettre en danger les troupes. Par exemple, l'armée américaine a retiré durant l'opération *Iraqi Freedom* certaines informations non classifiées du site Internet public du Département de la Défense, estimant que les militaires irakiens pouvaient les exploiter.
14. Nous sommes redevables à Peter Wilson de nous avoir rappelé cet élément.
15. Sun Tzu, *L'Art de la guerre*, Paris, Flammarion, 2008 (rééd.).
16. Voir A. Price, *The History of US Electronic Warfare*, Alexandria, AOC, 1984.

Or tous ces éléments combinés semblent entretenus par la littérature alarmiste sur les cyberguerres. Parce qu'elle part d'hypothèses trompeuses, l'idée de cyberguerre débouche sur des analyses disproportionnées, dont celle de la menace « imminente » d'une cyberattaque de grande ampleur.

La réalité opérationnelle des cyberattaques

Les métaphores et analogies ne manquent pas pour nous convaincre de la pertinence stratégique du cyberespace. Beaucoup évoquent outre-Atlantique la peur d'un « Pearl Harbor numérique » ; certains comparent même la création du Cybercommand à celle de l'US Air Force un demi-siècle plus tôt[17]. Mais si le cyberespace constitue un espace de bataille au même titre que l'air, l'eau ou la terre, on peut en déduire que les vieilles règles de l'art de la guerre peuvent s'y appliquer : l'attaque, la défense, la dissuasion.

C'est exactement ce que dit le général James Cartwright, commandant de l'US Strategic Command, le 21 mars 2007 devant le Comité des forces armées de la Chambre des représentants : « l'histoire nous apprend qu'une posture purement défensive pose toujours des risques et par conséquent la meilleure défense dans le cyberespace est l'attaque[18] ». Mais l'application consciencieuse de grilles de lecture stratégiques classiques est-elle véritablement convaincante ? Comparons pour cela deux conflits, l'un dans le monde « réel » et l'autre dans le cyberespace.

Le 12 juillet 2006, dix jours après l'enlèvement du caporal Gilad Shalit dans la bande de Gaza, le Hezbollah lance un raid à la frontière libano-israélienne, capture deux soldats israéliens et en tue huit autres. Immédiatement, le Premier ministre israélien Ehoud Olmert accuse le Liban de s'être livré à « un acte de guerre[19] » tandis que le chef d'état-major israélien, le général Dan Haloutz, indique que Tsahal va ramener le Liban « vingt ans en arrière ». S'ensuit une guerre de 34 jours, durant lesquels le Hezbollah lancera plus de 4 000 roquettes sur le sol israélien et utilisera plus de 1 000 missiles antichars. Tsahal lance la plus importante campagne aérienne jamais menée hors OTAN, avec plus de 7 000 cibles : centres de commandement du mouvement chiite, ponts, aéroport, bâtiments civils. Bilan humain : 43 civils israéliens, 116 soldats de Tsahal, entre 650 et 750 hommes du Hezbollah et entre 850 et 1 191 civils libanais périssent.

17. Voir Major General Worden, « Developing Twenty-First-Century Airpower Strategists », *Strategic Studies Quarterly*, vol. 2, n° 1, printemps 2008.
18. B. Brewin, « Cybersecurity Defense Requires a Good Offense », *Federal Computer Week*, 22 mars 2007, disponible sur *Fcw.com*.
19. Déclaration d'E. Olmert, 12 juillet 2006.

De son côté, la « cyberguerre » en Estonie du printemps 2007 a duré 22 jours, n'a fait aucun mort et les structures physiques du pays sont restées intactes. On pourrait certes mesurer des dégâts économiques ou politiques, mais s'agit-il là d'une guerre ? Non, si l'on en croit Napoléon Bonaparte : « À la guerre comme en amour, pour en finir il faut se voir de près ».

Certains dans les années 1990 n'avaient pas hésité à comparer la cyberguerre à la guerre nucléaire imaginée au début de la guerre froide. Mais aujourd'hui, les stratégistes américains les plus modérés révoquent cette comparaison entre les outils d'une cyberguerre et les armes de destruction massive, et préfèrent parler plutôt, dans le cas des cyberattaques, « d'armes de nuisance massive ». Comme le confie l'expert nucléaire Roger Molander, « qu'une bande de hackers mette à plat votre système informatique c'est affreux, mais ça n'équivaudra jamais à une arme qui rase New York ».

La cyberguerre d'Estonie a duré 22 jours, mais est-ce une guerre ?

Que recouvrent exactement les cyberattaques ? Si l'on se réfère aux différentes couches constitutives du domaine virtuel, les attaques contre sa strate sémantique consistent à voler, modifier ou supprimer les informations contenues dans l'interface virtuelle. Les attaques contre les strates syntaxiques entendent endommager la diffusion des données *via* des virus ou autres outils de brouillage. Enfin, les attaques contre la strate physique recouvrent des pratiques plus classiques, ciblant des infrastructures réelles et impliquant donc un déploiement physique de l'ennemi.

Créer des outils en matière de cyberattaques tels que virus, chevaux de Troie et interdictions d'accès s'avère aujourd'hui plus simple et moins coûteux que de se munir d'artillerie ou d'obusiers. On oublie pourtant que tout acte de guerre est lié à un contexte spatio-temporel, et que par définition les outils actuels d'une cyberguerre peuvent produire une nuisance mais non l'annihilation de la cible. À moins d'imaginer le scénario d'un ennemi omnipotent attaquant simultanément l'ensemble des structures, il est encore possible de réagir une fois attaqué – en tout cas beaucoup plus sûrement que si un missile balistique explose sur une capitale.

Admettons qu'un ennemi décide effectivement de mettre à terre tous les moyens civils et militaires de fonctionnement de son adversaire. En 2006, la Commission européenne a identifié les infrastructures dites « critiques », susceptibles de faire l'objet d'une attaque terroriste : les

industries nucléaire et chimique, les systèmes financier, alimentaire, énergétique et sanitaire, le trafic routier, les réseaux de transport. Parce que toutes ces infrastructures sont aujourd'hui intrinsèquement liées à l'interface informatique et qu'en outre elles fonctionnent sur un mode civil et non militaire, leur vulnérabilité semble importante face à une cyberattaque.

Considérons pourtant la dimension logistique qu'une telle hypothèse induit. Lancer une attaque contre ces centres de gravité sociétaux demanderait d'investir des sommes colossales tant en matière de technologies offensives que de veille constante de cibles évolutives. Le cyberespace et les systèmes de sécurité changent effectivement si rapidement que l'actualisation des techniques d'intrusion et de destruction devient un travail extrêmement coûteux, rendant une cyberattaque terroriste de grande envergure peu probable.

De même, il semble régner quelque confusion sur la question des infrastructures critiques. Martin Libicki, expert à la RAND, explique que « la question n'est pas de savoir si c'est difficile d'atteindre les infrastructures critiques mais de le faire réellement, en entraînant de véritables conséquences ». George Smith, journaliste spécialisé en sécurité informatique, ajoute : « On entend toujours cette hypothèse selon laquelle des usines chimiques pourraient exploser, la fourniture d'eau être polluée – toutes ces choses qui sont déjà difficiles à effectuer dans le monde réel sont soudainement supposées élémentaires du fait de l'importance d'Internet[20] ».

En juillet 2001, le Naval War College a organisé un *wargame* imaginant une attaque massive contre les infrastructures critiques américaines. Suite à l'exercice, il a été conclu qu'« une telle attaque nécessiterait une organisation extrêmement lourde bénéficiant au moins de 200 millions de dollars, de cellules de renseignement dignes d'un pays et de cinq ans de préparation[21] ».

En outre, sur le plan tactique, à l'ère des munitions intelligentes et précises, une cyberattaque semble beaucoup trop incertaine en matière de ciblage. Si les cibles fonctionnent en réseau, jusqu'où le maillage remonte-t-il, et dans quelles proportions la destruction d'un nœud endommagera-t-elle des stations « collatérales » ? Sur ce point, il est rapporté qu'en 2003 le cabinet de Donald Rumsfeld aurait refusé de lancer une cyberattaque contre le système financier irakien car ce dernier se trouvait être connecté à un réseau de communications financières localisé en Europe. La destruc-

20. J. Green, « The Myth of Cyberterrorism », *Washington Monthly*, novembre 2002.
21. *Ibidem.*

tion du système irakien aurait ainsi pu entraîner la mise à mal de systèmes informatiques bancaires et de distributeurs automatiques d'argent européens[22]. Déjà, au milieu des années 1990, la première fois que des représentants de systèmes financiers furent invités par les militaires américains à un *wargame* où des terroristes attaquaient les réseaux bancaires, les convives se tournèrent vers les officiers en s'exclamant : « Excusez-nous, mais avez-vous la moindre idée de ce que représente réellement le système financier mondial ?!...[23] »

La nuisance d'intrusions informatiques pouvait être réelle, mais leur caractère stratégique, qui autoriserait à les qualifier de cyberattaques – au sens proprement militaire – reste à ce jour peu convaincant, tant au niveau de l'investissement conséquent qu'il exigerait, que de l'impact supposé sur le « champ de bataille » considéré.

Au fond, le mythe du *big bang* informatique qui nous renverrait à l'âge de pierre ne nous induit-il pas en erreur ? La guerre réseau-centrée doit-elle vraiment être cyber-centrée ? On en revient au premier des malentendus énoncé plus haut à l'égard de la guerre réseau-centrée et de son affiliation systématique aux capacités technologiques. Le chercheur David Ronfeldt se remémore la consécration du concept : « À partir du moment où deux, trois personnes au Pentagone ont commencé à définir la guerre en réseau sur un plan technologique *stricto sensu*, il est devenu quasiment impossible d'expliquer que le premier chantier était institutionnel, que la priorité restait les organisations humaines[24] ». La cyberguerre, comme finalité, est donc d'abord une surenchère technologique, qu'on pourrait résumer de façon sarcastique comme une « course aux ordinateurs ». À l'inverse, la cyberguerre, en tant que système de moyens, recouvre une plus haute ambition : en finir avec le modèle d'armée occidental et exploiter les capacités du cyberespace pour constituer de petites unités militaires souples dont la référence ultime serait les tribus mongoles du XIII^{e} siècle[25].

Surenchère technologique et dépassement du système d'armée occidental

Après les attentats du 11 septembre, le biais technologique s'est encore accru, la peur d'une cyberattaque d'Al-Qaida se faisant récurrente. À nouveau, on semblait ne pas saisir que le cyberespace était en réalité moins

22. C. Wilson, « Dominating the Electronic Spectrum: Information Operations and Cyberwar », *Military Technology*, vol. 31, n° 11, novembre 2007, p. 94.
23. Entretiens au Département de la Défense américain, hiver 2007.
24. Entretien avec D. Ronfeldt, RAND Corporation (Santa Monica), hiver 2007.
25. Sur l'histoire militaire mongole et son usage contemporain, voir T. May, *The Mongol Art of War*, Yardley, Westholme Publishing, 2007.

une cible qu'un support, et qu'en aucun cas – comme cela allait se vérifier dans les années suivantes – les terroristes ne pouvaient ambitionner de mettre à terre Internet. N'en sont-ils pas aussi dépendants en termes logistiques ? Ne l'exploitent-ils pas tout autant que les gouvernements en termes de propagande ?

Se déprendre des sirènes de la cyberguerre ne signifie pas jouer les réactionnaires stratégiques. Si une bonne part des hypothèses actuelles de la littérature repose sur des mythes, les problèmes concrets demeurent, comme celui que posent les relations entre secteurs public et privé dans le cyberespace.

La synergie public-privé dans le cyberespace

L'un des aspects les plus novateurs, et complexes, du cyberespace est la dépendance exponentielle des structures militaires et, de manière parallèle, civiles vis-à-vis de ces technologies, qu'il s'agisse de la « numérisation du champ de bataille » ou de l'usage du courriel à des fins privées ou commerciales.

En ce sens, lorsque Gordon Moore, fondateur d'Intel, édicte en 1975 sa fameuse loi selon laquelle le nombre de transistors des microprocesseurs sur une puce de silicium double tous les deux ans, son intuition technologique ne peut concevoir la grande difficulté qui est dès lors celle des structures militaires modernes : comment absorber, assimiler, « endoctriner » les innovations si leurs capacités s'accélèrent constamment ?

Tout en évoluant, en se modifiant continuellement, le cyberespace a si vite envahi nos vies de tous les jours que l'on en vient à réaliser que contrairement aux dimensions terrestre, maritime et aérienne, les stratèges militaires n'ont pas réussi à capter le cyberespace afin d'agencer une thèse tangible s'apparentant à une sorte de *cyberpower*[26].

Par ailleurs, et c'est là que la faille potentielle paraît, les organisations militaires occidentales en général, et celles des États-Unis en particulier, sont devenues dépendantes de technologies développées par le secteur privé. Dans le domaine informationnel, le Département de la Défense a intensivement recours aux produits dits « sur étagère » (*commercial off the shelf*). En ce qui concerne, par exemple, les systèmes de communication embarqués sur les drones, l'Unmanned Systems Roadmap fait état d'une

26. Mentionnons néanmoins des efforts en ce sens aux États-Unis, notamment par le biais de travaux actuellement en cours à la National Defense University.

tendance grandissante à l'externalisation des liaisons de données, les deux avantages étant un coût plus faible pour le Pentagone et des cycles de développement accélérés[27].

L'exploitation de produits d'origine commerciale dans le domaine du cyberespace à des fins militaires est devenue une pratique courante pour des raisons budgétaires : pour les armées, développer par elles-mêmes des réseaux et des logiciels propres représenterait un coût exorbitant. Pour l'énorme programme Future Combat Systems, symbole pour l'US Army de la guerre réseau-centrée, Boeing est en train de créer un système opératoire reliant le fantassin aux véhicules de combats, capteurs, drones et centres de commandement. Pour ne pas augmenter les coûts de production, les ingénieurs de Boeing ont tout simplement décidé de se fonder sur le système d'exploitation à distribution libre Linux[28].

Les services de renseignement américains ont aussi recours à des contractants externes pour développer et exploiter des logiciels innovants en matière de détection d'information. Ils ont ainsi créé en 2006 Intellipedia, s'inspirant volontairement de Wikipedia, pour permettre la mise en commun des données[29].

Que l'on se rassure : dans le cas d'Intellipedia, ou du *software* de Boeing, les ingénieurs prennent soin d'identifier les technologies « critiques » et de modifier les interfaces de départ[30]. La tendance de long terme des structures militaires à se tourner vers les innovations civiles est néanmoins nette. Comme nous l'avons souligné précédemment, l'un des véritables aspects novateurs du cyberespace est la dépendance grandissante des structures militaires à l'égard du secteur privé. La recherche et le développement en matière de technologies de l'information ne sont ainsi plus guère financés par le Pentagone, qui a laissé les grandes compagnies prendre le relais. Il en résulte des dilemmes financiers, auxquels s'ajoutent des aberrations opérationnelles.

Ce choix économique coïncide avec l'usage de plus en plus complexe et intense du spectre électromagnétique. Comment le Pentagone peut-il rationaliser ses pratiques en la matière lorsque 80 % de sa bande passante est d'origine commerciale ?[31] Le résultat est que derrière les grandes

27. *Unmanned Systems Roadmap 2007-2032*, rapport du Département de la Défense, 2007, p. 49.
28. A. Klein, « The Complex Crux Of Wireless Warfare », *Washington Post*, 24 janvier 2008.
29. L. Wright, « The Spymaster », *The New Yorker*, 21 janvier 2008.
30. Cette démarche fait l'objet d'une directive spécifique, la « DoD Directive 8100.2: Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid », 14/4/2004.
31. « Unmanned and dangerous », *The Economist, Technology Quarterly*, 6 décembre 2007.

théories des stratégistes et les beaux documents promotionnels de l'US Air Force, le Département de la Défense se retrouve aujourd'hui en concurrence avec les opérateurs satellitaires privés pour l'allocation de fréquences radio. Pire, il a pu arriver en Irak que les communications de drones aériens soient brouillées non par des miliciens irakiens mais par des téléphones portables, dont l'opérateur utilisait la même fréquence.

80 % de la bande passante du Pentagone est d'origine commerciale

Plus que dans n'importe quel domaine, les militaires devront coopérer dans le cyberespace avec les civils. Les premiers doivent bénéficier des compétences des seconds, et ces derniers être sensibilisés aux enjeux militaires de leurs activités. D'une part, ce n'est pas sans raison que l'US Air Force recrute autant qu'elle peut ces *information warriors* venus des grandes entreprises des technologies de l'information, même si l'on peut douter que l'US Air Force puisse attirer en masse des ingénieurs grassement payés dans la Silicon Valley[32]. D'autre part, le secteur privé doit être accompagné dans une démarche sécuritaire à l'égard de ses infrastructures, qui peuvent représenter des cibles pour un ennemi potentiel, et donc des failles pour le bien public.

En ce sens, la controverse qui a éclaté à l'automne 2007 – qui a conduit la Maison-Blanche à bloquer le rachat de 3Com, une société créant du matériel de sécurité informatique, par le fonds d'investissement Bain Capital Partners et le consortium chinois Huawei Technology – rappelle combien la problématique technologique, avant d'être celle des affaires, devrait être celle du politique.

En 2002, Richard Clarke, alors assistant spécial du président George W. Bush sur le cyberterrorisme, estima devant un parterre d'industriels que seul 0,0025 % du revenu des entreprises américaines était consacré à la sécurité technologique. La *National Strategy to Secure Cyberspace* publiée en 2003 reconnaît que le secteur privé détient désormais un rôle crucial en matière de sécurité nationale car il entretient très largement les infrastructures critiques des États-Unis[33]. Mais ce document fait toujours aujourd'hui figure de vœu pieu tant Clarke et son équipe semblaient exiger des mesures allant vers une régulation du marché, idée que rejettent les entrepreneurs.

32. J. Lasker, « Air Force Recruits Techies from Area », *Tacoma News Tribune*, 15 octobre 2007.
33. *National Strategy to Secure Cyberspace*, Washington, Government Printing Office, 2003, disponible sur *Whitehouse.gov*.

Ainsi, il n'y a que l'US Air Force pour croire qu'elle pourrait prendre seule en charge le cyberespace ; si cyberguerre il y avait, celle-ci ne se déroulerait pas dans un espace virtuel réduit au champ électromagnétique. Il s'agirait au contraire d'une guerre bien réelle. Dans cette logique, le cyberespace doit d'abord être conçu comme une interface aux opportunités incontestables pour les structures militaires et civiles, les défis en termes de sécurité étant proportionnels aux opportunités. Des défis que ces mêmes acteurs ne pourront relever qu'ensemble.

MOTS CLÉS

Cyberguerre
Guerre réseau-centrée
États-Unis
Estonie