Tout commence par une « Révolution Technologique Militaire ». L'expression date des années 1970 : des théoriciens soviétiques parlent de « nouvelles méthodes tactiques »[1]. Ils pensent les Nouvelles Technologies de l'Information et de la Communication (les fameuses « NTIC ») comme un changement de paradigme. Au seuil des années 90, les spécialistes américains reprennent le thème et lancent le slogan de *Revolution in Military Affairs*, (RMA, Révolution dans les Affaires Militaires), le sigle qui restera. Cette approche converge avec un courant d'idées, futurologues, annonciateurs de la société postindustrielle, spécialistes de l'ère numérique et autres Troisièmes Vagues, influent aux États-Unis en général, dans l'armée et l'administration en particulier. Pour eux, la RMA est le complément de la révolution numérique dans la société civile et traduit le passage à une économie de l'intangible. La stratégie ne subira pas moins que l'économie ou la culture le choc numérique.

RMA résumerait donc les bouleversements tendanciels que subit l'art de la guerre. Tout cela débouche sur des spéculations sur l'emploi de panoplies « civiles »[2] (ordinateurs, satellites, Internet) et sur les perspectives politiques qui en découlent. Le tout pourrait se résumer en une équation : R.M.A. = 1991 (fin de la guerre froide) + NTIC = Nouvel Ordre Global.

Si « RMA » est supposée désigner une phase historique, la « guerre de l'information » constitue plutôt le modèle théorique des conflits futurs, une option stratégique ou plutôt un ensemble d'hypothèses. Comme il se doit, les experts ne sont d'accord ni sur le stade de la RMA qui est ou sera bientôt atteint, ni sur les formes et puissances de la guerre de l'information. Dans le débat, sur ce qui est technologiquement réalisable, les attitudes oscillent entre le scepticisme (« tous ces gadgets connaîtront le même sort que ceux de la guerre des étoiles de l'époque Reagan ») et

---

[1] Karber P.A., *The tactical Revolution in Soviet Military Doctrine*, Carlisle Barrakcs, U.S. Army War College, 1983

[2] La notion de technologie « civile » est relative si l'on songe que satellites et fusées descendent des V2 de la seconde guerre mondiale, que l'informatique a été en grande partie inventée par les cryptologues qui travaillaient à casser les codes secrets nazis, qu'Internet est né d'Arpanet de la guerre froide, un réseau d'ordinateurs de la guerre froide interconnectés de telle façon que la capacité de communication américaine ne soit pas détruite en cas d'attaque atomique, etc ;.....

l'enthousiasme (pour d'autres tous ces objectifs seront bientôt à la porté du pouvoir global U.S. : « *global reach, global power* »[3]).

La description de l'infoguerre, vire au catalogue avec floraison de sous-catégories. Ainsi, Laurent Murawiec inclut dans la guerre informationnelle, d'une part une guerre « capacitante » qui consiste à compliquer ou disloquer le processus décisionnel adverse, à brouiller, leurrer, détruire les capteurs, et d'autre part une guerre informationnelle « conditionnante » ? Cette dernière est à base de tromperie stratégique et guerre psychologique, de désinformation, d'atteinte au moral adverse, etc.[4]. Deux autres théoriciens de la Rand Corporation, Arquilla et Ronfeldt, séparent d'une part la *cyberwar*, cyberguerre strictement militaire, de la netwar, net guerre. La cyberguerre c'est « conduire des opérations militaires suivant des principes relatif à l'information. C'est-à-dire détourner ou détruire l'information et les systèmes de communication adverse ». La netguerre, ce sont des « conflits à grande échelle entre nations ou sociétés. Ce qui suppose s'efforcer de changer ou pervertir ce qu'une population cible sait ou croît d'elle-même ou du monde qui l'entoure »[5]. D'autres distinguent cinq ou sept [6] sous-catégories[7], sans parler de phraséologies concurrentes comme « hyperguerre[8] » ou « guerre de quatrième génération »...). A croire que les premières victimes de la guerre de l'information sont les stratèges qui ne parviendront bientôt plus à se comprendre.

Enfin, il faut tenir compte de la dimension utopique de la RMA, le rêve de remplacer la guerre de manœuvre et de massacre par une guerre de la connaissance et de la domination sans effusion de sang. Comme le note Alain Joxe : « Le concept de la RMA s'est banalisé. Il signifie tout : la recherche de l'application des innovations technologiques aux inventions militaires ; la dérive de

---

[3] Sur les différentes « écoles » de la RMA voir O'Hanlon M., *Technological Change and the Future of Warfare*, Washington D.C., Brookings Institution Press, 2000, p 11 et sq.

[4] Murawiec, L., *La guerre au XXIe siècle*. Paris, Odile Jacob, 2000

[5] Arquilla J. & Ronfeldt D., *Cyberwar is Coming*!, Comparative Strategy, 12:2 (Avril juin 1993): 141-165

[6] Par exemple : 1) guerre de contrôle et de commandement, 2) guerre d'intelligence 3) guerre électronique 4) opérations psychologiques 5) guerre de pirates informatiques, 6) guerre de l'information économique 7) Cyberguerre proprement dite...

[7] Le meilleur résumé de ces discussion scolastiques se trouve dans (article : Shunning the Frumious Bandersnatch: Current Literature on Information Warfare and Deterrence, Août 2000 Geoffrey S. French) http://www.terrorism.com

[8] Voir Arnett *Welcome to Hyperwar* http://www.bullatomsci.org/issues/1992/s92/s92.arnett.html voir aussihttp://www.airpower.maxwell.af.mil/airchronicles/battle/chp5.html

la pensée stratégique vers la guerre virtuelle et le cyberspace ; la recherche d'armes non létale destinées à maintenir l'ordre sans grands massacres. La "pensée de la RMA" est devenue l'équivalent du politically correct pour la défense, aux Etats Unis. »[9]

Cette confusion terminologique recouvre en réalité deux phénomènes. D'une part l'accroissement des possibilités offensives est immense. Il ne s'agit pas de raisonner sur une nouveauté technologique (comme le tank ou la bombe atomique) mais sur des systèmes technologiques imbriqués (pas forcément militaires) et sur des principes nouveaux, certains déjà effectifs, d'autres supposés, qui touchent ou toucheront tous les aspects de l'offensive : organisation, coordination, intelligence, frappe, manipulation de l'opinion, altération des perceptions adverses, etc… D'autre part l'infoguerre ouvre aussi l'éventail des objectifs : il ne s'agit plus seulement de vaincre des corps d'armée mais aussi de s'en prendre à des infrastructures civiles et, plus largement, à l'esprit de populations entières. Si l'on raisonne en termes de fragilités et de dangers, on peut donc assimiler à l'infoguerre toutes les formes de sabotage, prédation et falsification *high tech,* fussent-elles criminelles ou économiques. Ainsi, le grand spécialiste civil américain de l'*infowar*, Winn Schwartau, distingue-t-il trois « classes » : la guerre d'information privée qui touche à la « vie privée électronique », tous les malheurs qui peuvent arriver à un particulier du fait de cybercriminalité, la guerre d'information d'entreprise, tout ce qui menace les systèmes d'information d'une société et enfin la « guerre globale de l'information » dite de classe III, tout ce qui toucherait à la sécurité nationale, des infrastructures sensibles à la compétitivité économico-technologique d'un pays[10].

Pour le dire autrement, la question de la guerre revient au premier plan par un double mouvement d'idées. Celles des civils qui décrivent en termes martiaux les périls criminels, terroristes, économiques liés aux nouvelles technologies. Pour eux, l'infoguerre recouvre des

---

[9] Alain Joxe *Représentation des alliances dans la nouvelle stratégie américaine*. http://www.ceri.com

[10] Winn Schwartau. *Information Warfare,* Thunders Mouth Press. Disponible sur Amazon.Com en livre numérique. Celui-ci y affirme notamment : « Nous découvrirons hélas qu'un adversaire décidé et doté de moyens financiers importants aura la capacité - j'insiste sur le mot capacité - de faire de mener des guerres contre des Etats Nations et des sphères d'influence politiques ou économiques comme jamais auparavant. Nous verrons que le conflit international sur les autoroutes mondiales de l'information comme sur nos structures nationales d'information. Dès maintenant nous devons commencer à nous défendre. »

risques d'atteinte à la sécurité voire d'effondrement de nos sociétés. Et l'autre mouvement est celui des penseurs militaires qui décrivent une guerre basée précisément sur les technologies et les principes civils de l'ère de l'information.

Barouf dans le cybervillage

Les stratèges les plus audacieux acceptent désormais plusieurs postulats qui donnent une singulière interprétation du slogan du *1984* d'Orwell. : « La paix c'est la guerre ». Il nous semble que ces postulats soient les suivants :

a) L'armée, comme la société civile, subit le choc technologique de l'information mais aussi le choc organisationnel : elle doit fonctionner en réseau, comme l'entreprise.
b) La guerre repose sur les mêmes infrastructures de l'information que l'activité économique, réseaux, Internet. Corollairement, les infrastructures civiles critiques (tout comme les médias ou tout ce qui peut agir sur le moral de la population) deviennent autant de cibles.
c) Les conflits opposeront de moins en moins des États Nations mais feront intervenir des guérillas, des mafias, des terroristes, des fondamentalistes, des puissances financières, des ONG, etc. Ces acteurs seront parfois difficiles à identifier mais leur structure de fonctionnement non hiérarchique et non centralisée renforceront cette logique de dispersion.
d) La gamme des actions offensives ou dissuasives s'est tellement étendue, de l'usage de virus à celui de missiles en passant par des actions sur l'opinion publique, que tout un chacun peut entrer dans le jeu à un niveau correspondant à ses capacités. Le passage de la guerre à la paix devient une frontière impalpable entre sabotage, contrainte, pression, sanction, etc. Nombre de nouveaux stratèges[11] raisonnent en terme de « spectre des conflits » : une échelle d'intensité, avec à une extrémité l'emploi explosif de la puissance militaire et, à l'autre, des formes d'attaques qui ressemblent davantage à des manipulations politiques ou à des délits informatiques.

[11] En particulier les gurus de la Rand corporation réunis dans *In Athena's camp*

e) À l'ère des réseaux tout conflit local concerne toute la planète et il n'y a plus vraiment d'affaires intérieures et d'affaires internationales (les Américains ont forgé le néologisme d'affaires « intermestiques » à la fois internationales et domestiques).

f) En somme guerre et paix seraient une affaire de supériorité informationnelle, l'une et l'autre opposent le modèle de société dominant culturellement, économiquement, technologiquement ses adversaires qui sont aussi des ennemis idéologiques. À l'extrême, la dominance par les technologies de l'information, aboutit à l'intelligence parfaite et à la prévision/prévention de toute violence. L'information devient un substitut au conflit : les maîtres du réseau sont les maîtres du monde et font régner la *pax numerica*. La politique étrangère devient le monitoring de la planète.

Une utopie « cybernétique »[12] de la communication est née après 1944, avec pour dessein d'empêcher le « retour de la barbarie ». L'information c'était la paix ; il se pourrait qu'il nous faille maintenant affronter que « l'information, c'est la guerre ».

Dans cette perspective, on comprend mieux comment les chantres de l'infoguerre se la représentent concrètement.

Pour l'ordre, distinguons à la louche trois types ou trois stades de l'utopie infoguerière :

- Une stratégie d'amplification : ajouter aux forces armées des machines à communiquer ou traiter qui en accroissent l'efficacité (observation, coordination, traitement de l'information en temps réel, simulation, armes « intelligentes), mieux faire avec les technologies modernes ce qui se faisait autrefois avec des pigeons voyageurs, des photos aériennes, des radios : c'est une guerre conventionnelle assistée par ordinateur. La gestion de l'information est un facteur d'économie de temps et de force. Le volet civil est la poursuite par des moyens numériques

[12] Du grec *keubernêtiké*, science de gouverner. La cybernétique, science inventée par la mathématicien Wiener, se proposait d'étudier le contrôle et la communication chez les animaux et les machines. Son projet de créer une science du maintien des équilibres optimaux aboutissait explicitement sur une utopie de régulation pacifique des sociétés humaines. Voir Wiener Norman *1950 The Human Use of Human Beings, Cybernetics and society,* trad. fr.; *Cybernétique et société* UGE, , 1954,. Plusieurs travaux, notamment ceux de Philippe Breton (voir Breton P., Proulx S. *L'explosion de la communication* , Paris La Découverte, 1989 et Breton P. *L'utopie de la communication,* Paris La Découverte, 1992) en font même un des mythes annonciateurs de notre présente idéologie de la communication.

d'activités d'espionnage, dénigrement, démoralisation, intoxication, etc. L'infoguerre démultiplie les armes.

- Une stratégie de réemploi : des techniques qui n'ont rien de martial en leur principe servent à des fins de destruction ou de contrainte. Ainsi l'application guerrière ou délictueuse de l'informatique (atteintes à la confidentialité ou à l'intégrité de données) : intrusion via Internet, virus, chevaux de Troie, usurpation d'identité électronique, etc... Corollairement chaque technologie de communication implique des fragilités et des dépendances. Un Intranet est un objectif plus tentant qu'un bureau de poste pour un saboteur, civil ou militaire. Une rumeur électronique est plus difficile à arrêter qu'un distributeur de tract. Du coup, certains rêvent de remplacer raids aériens ou débarquements par l'usage de logiciels ou d'illusions médiatiques. L'information produit une perturbation ciblée plutôt qu'une destruction massive. L'infoguerre succède aux armes[13].

- Une politique de dominance informationnelle : la dissymétrie des moyens d'acquisition, circulation ou traitement de l'information permet de contrôler ce que savent et ce que croient les forces pouvant influer sur le conflit. Cette prévention totale s'en prend aux intentions mêmes de l'adversaire. L'infoguerre supprime la guerre.

Le tout forme un discours programmatique voire « futurocratique[14] ». très contesté. Parfois qualifiée d'utopie dangereuse, la RMA fait débat surtout aux U.S.A. Les critiques portent sur l'effectivité du changement et répètent que « ça n'existe pas » ou qu'il n'y a pas vraiment de révolutions militaires mais des évolutions. D'autres en contestent l'efficacité sur le thème « ça ne marchera jamais. ». Cette guerre trop propre, trop politiquement correcte (guère de victimes ou

---

[13] Voir à ce propos un très intéressant point de vue de l'analyste suédois E. Anders Erikson du Centre d'études pour la non-prolifération : « *Information warfare, hype or reality ?* » disponible sur http://cns.miis.edu/pubs/npr/eriksn63.htm

[14] Nous proposons le néologisme de "futurocratie" pour désigner le système d'autorité qui se fonde sur la prétention en une conformité supposée aux tendances du réel, et prône une soumission à une inévitable loi tendancielle cachée, que ne distingueraient encore que quelques-uns ; et cela en dépit (à cause ?) d'un terrifiant taux d'erreurs avérées. Nous vivons en futurocratie en ce sens qu'à chaque instant, bien plus qu'à la force de la tradition ou à la légitimité de l'autorité, nous sommes appelés à nous soumettre au pouvoir d'anticipations présentées comme inéluctables et scientifiques et qui peuvent aussi bien porter sur la technologie, l'écologie, l'économie, la démographie, etc.

de violence visible), trop mode et trop technocratique fait ricaner les pessimistes. Ils trouvent mille raisons, contradictions ou facteurs humains pour en dénoncer l'irréalisme et la fragilité. Beaucoup considèrent que l'obsession de réduire ses pertes désarmera moralement une armée infoguerrière face à des adversaires rustiques prêts à tuer et à mourir[15].

Des sceptiques décrivent la future infoguerre comme celle de l'arroseur arrosé : dans un monde de réseaux interconnectés, comment être certains que les agressions informationnelles (actes de piratages, intoxication, etc.) dont on ne saura plus identifier la source ni contrôler la diffusion ne frappent pas leur auteur ? Ou un allié par un phénomène d'information « fratricide » ? Que l'on s'en prend bien à celui que l'on vise ou que l'on réplique à celui qui vous attaque ? Qu'un système aussi fragile n'est pas à la merci de la panne la plus stupide ou de l'erreur la plus contagieuse ? Surtout, comment dissuader à l'ère numérique ? Un gouvernement comprend le risque si on le menace de bombes atomiques ou de raids de B52, mais peut-on le menacer d'un cyber sabotage, d'une intoxication ou d'une campagne médiatique ?

La guerre de l'information n'est pas seulement une hypothèse d'intellectuels. Elle semble avoir acquis le statut de programme officiel de la première puissance du monde[16]. Le seul fait que ces hypothèses remplissent les cartons du Pentagone mérite examen. L'infoguerre ressemble à un plan en trois étapes .

Dominer la bataille

La RMA suppose d'abord des outils pour améliorer la protection, la mobilité, l'intelligence, la coordination des armées. Pour éviter la liste de gadgets (voir l'encadré « armes intelligentes et méchantes puces »), on les classera par buts recherchés :

---

[15] Voir en particulier une critique de la RMA sous forme de fiction par Charles Dunlap « *How we lost the High Tech War of 2007 : a Warning from the Future* » Washington D.C, Weekly Standard, 29 janvier 1996

[16] Un rapport de 1997 du Department of Defense américain intitulé « Joint vision 2010 » est généralement considéré comme le signe que l'infoguerre a un statut de quasi doctrine officielle aux USA.

Repérage des positions, mouvements et messages ennemis : vision, écoute, thermodétection, piratage et capteurs en tout genre, des satellites aux terminaux informatiques que portera chaque soldat.

Représentation par simulation numérique de l'environnement afin d'entraîner les troupes, préparer et décider les offensives. S'ajoutent des robots ou engins intelligents délégués là où il fallait autrefois risquer une vie. Donc guerre dans le virtuel.

Furtivité, capacité de se rendre indétectable, grâce à des formes high tech de camouflage (électromagnétique p. e.), par des modes de communication sécurisés, soit en détruisant les moyens de détection adverses et en l'éblouissant.

Guidage ultra précis des forces destructives, dosage de la violence appliquée au point le plus efficace, demain peut-être par des armes à énergie dirigée ?).

Supériorité dans la vitesse et le transport par des véhicules ou vecteurs rapides soutenus par des relais ou plate-forme allant de la station orbitale au porte-avions

Maîtrise des espaces, mer et l'air, espace stratosphérique voire cyberespace, pour être partout et frapper de partout.

Cette énumération qui évoque une liste de pouvoirs magiques (invisibilité, omniscience, omniprésence, invulnérabilité, etc. des anciennes mythologies,) se tend donc à l'élimination du délai, de l'incertitude et de l'aléa

Une ligne de force se dessine. S'affranchir de l'espace physique, et des obstacles de la distance : il fallait autrefois transporter ses troupes, explorer un environnement physique inconnu, découvrir péniblement où allait l'adversaire, se risquer au front, etc. Il s'agit maintenant de s'engager dans l'espace des signes : tout savoir, disposer de toutes les données en chaque point, ne pas émettre de signaux, rendre l'autre incapable de transmettre. L'idée est de traiter l'espace physique comme un espace sémantique : remplacer la lutte des hommes par la gestion des données implique un changement organisationnel à la mesure du changement technologique.

Tout cela suppose une coordination des connaissances, messages et décisions si totale et si instantanée que l'armée entière, hommes et machines réunis, semble obéir à un seul cerveau. Les

corps de troupe deviennent un corps mystique dont chaque membre participe de l'intelligence totale. Tout élément engagé sait tout (il bénéficie instantanément de toutes les données), communique tout (il est relié), peut tout (la puissance de frappe globale est à sa disposition). La hiérarchie militaire fondée sur la circulation verticale des informations et des commandements est remise en cause. Les futurologues conçoivent une armée « en réseau ». On parle maintenant de « réseau de combat »[17] par opposition avec la structure traditionnelle hiérarchique de l'armée traditionnelle, où l'information remonte au sommet et les ordres descendent. La décentralisation du pouvoir se traduirait en vitesse et souplesse de réaction, capacité de mieux faire circuler l'information, meilleure adaptation à un adversaire qui peut lui-même être constitué de petits groupes d'insurgés ou terroristes. Quand il n'y a plus de champ de bataille, et que les objectifs sont des éléments interconnectés en systèmes, le modèle du réseau s'impose donc également pour l'attaque comme pour la défense.

La RMA est parfois décrite comme une théorie du « système des systèmes » ce qui exprime à la fois l'interdépendance de tous ses éléments, et le fait que le réseau tend à avoir son centre partout et sa circonférence nulle part. Le champ des opérations apparaît lui-même comme un système intégré pensé également en termes de réseaux. Des mouvements de troupes adverses aux communications téléphoniques, tout est devenu flux et connections, non plus forces ou territoires.

La guerre du Golfe fut souvent comparée à un jeu vidéo. La vision qu'en donnait CNN, avec gracieuses traces de missiles dans le ciel et jolies lumières vertes sur Bagdad évoquait un produit Sega. La RMA sera plutôt un jeu où chaque G.I. Jo jouera en réseau et 3D avec tous ses copains. Ils seront connectés et disposeront de données en temps réel. Ils ne regarderont plus le viseur de leur fusil, mais l'écran de leur portable. Et si les choses tournent mal dans la réalité (IRL, *In real life,* comme disent les internautes), le secours tombera du ciel au grand dam des *bad guys*.

La doctrine militaire intègre manœuvre médiatique et manœuvre diplomatique. La RMA reflète la « judiciarisation » de la guerre et son évolution vers la guerre policière de contrôle et

[17] Arquilla and Ronfeldt, 1993 *Combat networks, Superior ability to gather, process, and disseminate information is key in preventing a war from arising*, sur le site de la Rand Organization précité.

prévention des troubles : en témoigne l'emploi d'armes non létales adaptées au maintien de l'ordre et du médiatiquement correct. Les guerres du futur mobiliseront reporters sans frontières, médecins sans frontières et gendarmes sans frontières.

Par hypothèse, une partie bénéficie d'une transparence intégrale et se bat à distance. On raisonne en supposant une disproportion totale, pour ne pas dire l'omnipotence des U.S.A. La phrase célèbre de Clausewitz selon laquelle, à la guerre, la seule chose dont un général soit certain est sa propre position deviendrait fausse[18]. La violence effective se ferait démonstration : vous êtes vu, vous avez perdu, preuve surabondante administrée à un destinataire un peu abruti, en somme. Quand les bombes sont considérées plus comme des messages que comme des moyens de tuer les gens, il s'est bien produit une révolution.

Contrôler l'adversaire

« Sans donner de bataille, tâchez d'être victorieux. » conseillait Sun Tse[19]. Vingt-cinq siècles plus tard, les stratèges modernes reprennent l'idée. La RMA bascule de la guerre high-tech à la « supériorité informationnelle : une « infodominance » telle que l'adversaire soit hors d'état de combattre. Il s'agit maintenant d'altérer ce que croit ou sait l'autre, tout en se préservant d'une attaque symétrique. Le principe est de « choquer et sidérer » (*shock and awe*) la partie adverse, civils compris, au point qu'elle s'effondre psychologiquement.

A priori, l'idée ne paraît pas très neuve : on se serait douté qu'il n'est utile de s'en prendre aux moyens de communication de l'ennemi, qu'il est de bonne guerre de manipuler, désorganiser, plonger l'autre dans l'ignorance, l'incohérence ou l'illusion. À ce compte, les ruses d'Ulysse ou les fourberies de Scapin valent bien des traités de stratégie.

---

[18] Les partisans de la RMA se présentent volontiers comme des « anticlausewitziens », bien davantage inspirés par les ruses du Chinois que par les célèbres catégories du Prussien, considéré comme un penseur typique de l'ère industrielle.

[19] Sun Tse Art III

La nouveauté est plutôt la façon dont ces principes sont mis en œuvre grâce aux instruments actuels. Les futurologues militaires rêvent désormais d'opérations psychologiques (*Psyops*) et cyberterrorisme.

Les Psyops, « opérations psychologiques » déjà évoqués, visent à la manipulation de l'opinion, celle des forces adverses et des civils. C'est la version ultramoderne de procédés bien connus : utiliser la radio pour persuader une population que ses dirigeants la trahissent, envoyer des tracts sur le thème « rendez-vous, toute résistance est inutile » ou infiltrer des agents pour saper le moral ennemi.

Or, plus de moyens techniques ne signifient pas nécessairement plus de puissance d'illusion. La seule psyops qui ait vraiment fait du bruit jusqu'à présent, c'est celle qu'ont menée quatre membres du « 4th Psychological Operations Group » de Fort Bragg, North California lorsqu'ils se sont fait repérer par la presse comme infiltrés à CNN[20]. Pour le moment l'efficacité des psyops est surtout douteuse.

Même incertitude quant aux actions orientées non pas vers la falsification de l'information adverse mais vers la suppression de ses outils de communication. Ici le but est bien le chaos[21]. La cyberguerre pure et dure se pratique par destruction physique des canaux et vecteurs (faire sauter des antennes, ou radars, détruire des nœuds de communication) mais surtout elle altère des flux immatériels. Une fois encore, virus, saturation, chevaux de Troie, faux messages, perturbations des circuits monétaires, destruction des bases de données, tous les sabotages auxquels un pirate peut se livrer à petite échelle contre une entreprise ou un particulier seraient ici réalisés à l'échelle d'une grande armée.

Dans ce cas théorique, l'attaquant emploie la force entropique de l'information contre l'infrastructure, l'organisation, les composantes qui servent à la transporter, collecter,

---

[20] Voir Abe de Vries, 25 Fev 2000 : « Specialists in 'psyops' worked for CNN » et *Army psyops at CNN* WorldNet Daily 3 Mars 2000 via http://www.zdnet.com

[21] Voir le chapitre VIII

transmettre et traiter. L'objectif, les nœuds par où circulent des énergies, des ressources, des informations à la fois moyen de production et facteur d'organisation

D'où trois conséquences :

- Pour que l'attaque sur la structure de l'information réponde au modèle des réseaux, ce qui suppose qu'ils existent, une cyberguerre contre l'Internet somalien ne serait pas très efficace. En outre, le système échanges est visé, y compris les infrastructures civiles imbriquées dans les systèmes militaires. Les civils ont vocation à être les principales victimes d'une infoguerre qui ne connaîtrait ni arrière ni champ de bataille. Du coup certains se demandent si l'infoguerre ne constituerait pas une forme de crime de guerre¨.
- Le raisonnement se retourne. L'infoguerre est à double tranchant. Plus un pays est doté de techniques sophistiquées, plus il est interconnecté, plus il est menacé.

- Il n'y a aucune raison que ce type de guerre soit réservé à des acteurs étatiques comme à l'époque où le conflit consistait à trouver un million de jeunes gens pour remplir des tranchées. La cyberguerre peut être une guerre privée.

Maîtriser la guerre

La « guerre par d'autres moyens » (WBOM, *War By Other Means* en jargon du Pentagone). Elle est un mélange des antiques stratagèmes de la Chine et des double-clics. Elle repose sur le postulat que toute forme d'action militaire classique est dépassée. Longtemps vaincre consista à détruire des choses ou des gens, occuper des territoires ou des positions, interdire des mouvements adverses. Désormais, ce serait désorganiser des structures, contrôler des réseaux et des perceptions, paralyser des volontés.

Le stade suprême de la guerre de l'information devient la prévention de toute guerre : la supériorité informationnelle. L'infoguerre se fait régulation de l'équilibre politique global, si ce

n'est avec plan de paix perpétuelle, pour ne pas dire direction du monde. On ne parle plus de gadgets électroniques, mais de » noopolitique », d'» intelligence absolue », de « *softpowe*r », diverses manières de dire que le modèle économique, politique, culturel et communicationnel de la société la plus avancée s'imposerait et suffirait à prévenir l'éclatement de conflits[22]. Les fauteurs de troubles subiraient un « *monitoring* » mondial : « substitut aux façons traditionnelles, de combattre ... remplacement de la force pure par la subversion ou une nouvelle forme de dissuasion »[23]. Le postulat est exprimé avec délicatesse par l'US Army[24] : ce serait « la capacité du gouvernement des États-Unis d'influencer la perception et la décision des autres. ». Les U.S.A. pourraient désarmer toute volonté offensive de paralyser à l'avance la velléité de lancer une attaque. La surveillance et la prédominance idéologique garantiraient contre toute surprise stratégique La Révolution dans les Affaires Militaires se fait révolution dans les affaires diplomatiques[25].

Et si cela ne suffisait pas, une gamme de punitions contraindrait les fauteurs de trouble : sanctions économiques, blocus technologique, pressions médiatico-diplomatiques, soutien aux forces d'opposition ou de guérilla, sanctions juridiques, ou encore raids aériens de représailles, campagne militaire internationale, occupation d'une zone par des soldats de la paix, cyberguerre. La « RMA » ressemblerait finalement plutôt la « R.A.P. », traduisez révolution des affaires pacifiques, politiques ou psychologiques, comme vous l'entendrez. Le fantasme du contrôle absolu confond art militaire, management planétaire, et sanction judiciaire.

---

[22] Le lecteur ne s'étonnera pas que toutes ces idées naissent et soient propagées une fois encore dans le cadre de la Rand. Voir http://www.rand.org/publications/MR/MR880

[23] Geoffrey S. Frenchl *Shunning the Frumious Bandersnatch* : Current Literature on Information Warfare and Deterrence, Août 2000, publié sur http://www.terrorism.com, un site très riche pour toutes les questions d'infoguerre

[24] Document FM 100-06 I Information operations, cité in Adams J. , *The Next World War*, New York, Simon and Schuster, 1998 p. 300

[25] Notion qui est très explicitement développée dans *In Athena's camp : Preparing for Conflict in the Information Age*, Santa Monica, Californie, Rand Monograph Report, Rand,. (sous la direction de Arquilla J. et Ronfeldt D) , véritable manifeste politicio-stratégique des penseurs U.S. les plus représentatifs de l'infoguerre, de la RMA et de la société de l'information. Bref de la « Troisième Vague » inspirée par les futurologue Toffler.

Le marchand

Le soldat de la RMA n'a rien d'un reître balafré. À rebours d'une tradition millénaire qui dressait des hommes pour le combat et pour la mort, le nouveau guerrier gère le sang comme les informations, en bon manager. Par contraste, c'est l'économie qui paraît martiale avec ses infoguerriers et ses batailles de l'opinion. « Le commerce, c'est la guerre » dit un proverbe japonais. Cet entrepreneur, aussi habile au négoce qu'au combat, a des ancêtres. La conquête de territoires et le développement des économies-mondes se fit souvent brutalement. Des associations de marchands, telles les Hanses germaniques ou la V.O.C., compagnie des Indes Orientales hollandaise, menaient des guerres, appliquaient la peine de mort, avaient une diplomatie autonome. Il arrive que telle multinationale soit suspectée d'aider à renverser des gouvernements, de subventionner des groupes armés ou d'avoir de véritables services d'espionnage, mais il n'existe pas de bombardiers aux armes de Coca-Cola. Sony ne fait pas pendre les employés qui divulguent ses secrets et Bill Gates ne répond pas comme les dirigeants de la V.O.C. à leur propre gouvernement[26], qu'il a le droit de traiter avec l'ennemi si tel est son intérêt.

La nouvelle économie a pourtant popularisé la version civile de l'infoguerre. Ici ce terme désigne tantôt une forme d'intelligence économique plus ou moins illégale, tantôt il se réfère à divers dangers d'Internet pour l'entreprise, tantôt enfin c'est un synonyme de guerre économique, de conquête par des moyens agressifs et planifiés.

Guerre angélique, économie militaire

L'infoguerre économique souvent décrite du point de vue de l'entreprise assiégée ou victime correspond à trois cas de figure.

---

[26] Voir Huyghe E. et F.B., *Les coureurs d'épices,* Paris, J.C. Lattès, 1995, p 246 sq.

A : Des entreprises ou des officines spécialisées - parfois le crime organisé, parfois des États - tentent de s'approprier des informations vraies et pertinentes, inventions et techniques, ou indices sur la stratégie des victimes, données diverses.

B : Ces mêmes entreprises ou officines attaquantes, mais aussi des "amateurs" appartenant à diverses tribus, *hackers*, *crackers*, *cyberpunks* et *cypherpunks*[27],, obéissent, eux à des pulsions ludiques ou nihilistes, s'introduisent dans le système d'information des victimes. Ils introduisent des virus, vers, chevaux de Troie et autres moyens de contrôle ou destruction des systèmes, des données et de leurs moyens de traitement. L'information pénétrante détruit l'information archivée, lui retire intégrité, fiabilité ou cohérence. Ici le procédé ressemble au vieux sabotage. La source de l'attaque est inconnue, le résultat visible.

C : Les agresseurs diffusent une information préjudiciable à la victime : bruits, rumeurs, prétendu mouvement d'opinion négatif, contestation de la fiabilité de ses produits, attaques contre son image de marque, lobbying "négatif", la discréditer, vrai, tendancieux, exagéré ou faux.

Les attaquants recourent à des relais humains conscients ou non, associations politisées, protestataires, experts, institutions, médias voire simples groupes de discussion, rumeurs ou bobards peuvent paniquer des actionnaires ou indigner l'opinion. Des relais techniques interviennent – tels des logiciels "renifleurs" analysant ce qui se dit sur les forums afin de repérer où lancer une opération de dénigrement. But ultime: la perte de marchés, la réprobation de l'opinion publique, la sanction d'autorités morales, juridiques, ou la paralysie des forces de la victime par inhibition et désordre. Tout cela rappelle ce que l'on nommait propagande noire, désinformation ou influence pendant la guerre. Avec la puissance d'amplification que donne à tout bruit Internet.

---

[27] Spécialistes du déchiffrement et du cassage de codes, mélange des mots *cypher* (chiffre au sens code secret et de punk)

L'économie de l'immatériel augmente la valeur de l'information, celle de son monopole ou de son antériorité, mais elle rend aussi la rivalité plus féroce. C'est le passage de la concurrence comme recherche de l'avantage au conflit, poursuite de la suprématie par tous les moyens. La globalisation offre un champ d'action à des acteurs menant une stratégie planétaire, d'autant que la fin du monde bipolaire permet la « reconversion » des moyens et des énergies.

Symétriquement, un fantasme se répand : le chaos, l'énorme machine paralysée par une attaque indécelable en son point de fragilité, virus, action d'une poignée d'informaticiens terroristes.

La concurrence se militarise. Économie et guerre s'inscrivent dans un même dessein géostratégique et recourent souvent aux mêmes méthodes d'utilisation dommageable de l'information. Des États conduisent l'affrontement économique avec autant de détermination qu'une expédition militaire, et tournent des moyens d'intelligence et d'agression vers la conquête des marchés.

Certes, les différences avec la « vraie » guerre sautent aux yeux :

- L'infoguerre économique échappe à la loi de la mort acceptée qui est celle de la vraie guerre ;
- La plupart des opérations d'infoguerre sont inavouées, illégales, clandestines et parfois même non décelées par les victimes, ce qui rapproche singulièrement plus de l'affrontement des services secrets que de la « vraie » guerre ;
- Elles se limitent parfois à une offensive ponctuelle et possède plus la brusquerie du raid que la continuité de la guerre.
- Certaines de ces « batailles », surtout via Internet, n'ont pas la clarté de celles qui opposaient des corps d'armée. Il est impossible de distinguer la source et la motivation des agressions, voire de mesurer un dommage qui peut être clandestin ou différé. En cas d'offensive, est-on en présence d'une opération militaire, d'une initiative d'un concurrent, d'un acte de vandalisme à motivation idéologique, d'un canular, d'un jeu[28]? Les victimes de bombardements ou d'une charge de cavaliers mongols avaient rarement de tels doutes.

[28] À titre d'exemple, en 1998, d'importantes intrusions logistiques contre des sites stratégiques US ont été détectées en pleine crise avec l'Irak et leur origine a été retracée jusqu'à un immeuble d'Abou Dhabi. Conclusion logique : Saddam Hussein lance une offensive cyberterroriste. Vérification faite, il se

La vraie question n'est guère de savoir si « guerre économique » ou « de l'information » sont le nom trop ronflant pour de vilaines pratiques. Elle est de comprendre en quoi les conditions d'une économie qu'on dit nouvelle favorisent aussi de nouvelles batailles.

La bataille pour le temps

Dès les années 70, une idée s'impose : l'information est une ressource stratégique. De l'idée que certaines informations sont précieuses, on passe à celle que les flux et systèmes d'information constituent les fondements de la richesse Pas seulement des connaissances nouvelles mais des modes de répartition et gestion de l'information...

Marc Guillaume parle d'un passage du fordisme au « toyotisme » dans l'entreprise « lorsqu'on a découvert qu'une information mieux gérée permettait de produire avec moins de délais, moins de stocks, moins de défauts et donc plus de qualité. »[29] Acquérir la « bonne » information, de type connaissance technologique de pointe, ou évaluation de l'environnement économique, mais aussi réguler la circulation de cette richesse, donc gérer les réseaux, deviennent l'alpha et l'oméga du management

Un modèle s'impose : l'entreprise virtuelle, mondialisée et décentralisée, éclatée par le télétravail ou en regroupements provisoires orientés vers un projet, toujours en réseaux, sans horaires fixes, reliant des groupes de créatifs en perpétuelle ébullition, échangeant des données. Cela ne ressemble guère à la vision traditionnelle d'une entreprise où, en des lieux et des moments appropriés, des gens disciplinés se collettent à la matière, et répètent les gestes appris, tandis que d'autres les dirigent et conçoivent. L'entreprise virtuelle, immatérielle, flexible aurait pour principes "ubiquité", "omniprésence" et "omnisciences »[30]. Ses performances supposeraient

---

révéla que dans l'immeuble en question, il y avait un routeur Internet et qu'en réalité, cette terrifiante première stratégique était l'œuvre de gamins aux U.S.A.

[29] Guillaume M., *L'Empire des réseaux*, Paris, Descartes, 1999 p103

[30] Ettighoffer D *L'entreprise virtuelle,* Paris, Odile Jacob 1992

innovations constantes, juste appréciation du marché, performances organisationnelles, confiance de capitaux internationaux.

La richesse dépendrait d'opinions et croyances (investisseurs persuadés de leur rentabilité, acheteurs convaincus de la modernité et de l'efficacité de leurs produits, des talents attirés par leur image de marque). Or, cette croyance est de plus en plus virtuelle. Ainsi les capitaux flottants exigent une rentabilité exceptionnelle basée sur d'hypothétiques conquêtes de parts de marché à venir. Quand le taux de rendement décolle de la réalité, toutes les tromperies et les menaces sont possibles. Voir la façon dont un escroc doué en informatique a fait baisser le cours de l'action Emulex par un faux communiqué, en a racheté à bas prix et a ainsi gagné 250.000 $ en un instant.

La nouvelle économie repose sur le monopole ou l'antériorité de données ou connaissances mais aussi sur des croyances. Telle l'appréciation positive sur l'image de la société, mais aussi, l'attention que le public est prêt à consacrer aux spectacles, productions imaginaires ou informatives, à la consultation de ressources de savoir ou de distraction. L'économie devient le négoce de la conscience : vendre des « états de conscience » aux consommateurs, mais aussi vendre aux entreprises la capacité de diriger la conscience des consommateurs. D'autres parlent d'une « économie de l'expérience », où chaque moment de la vie est « marchandisé », dans la mesure où « Dans la nouvelle économie, les gens consomment leur propre existence en en faisant l'acquisition par segments commercialisés »[31]. Demain peut-être, ce sera le passage prophétisé par certains[32] d'un système de marché où l'on vend et achète des choses et services en un lieu à un système de réseau : fournisseurs et utilisateurs échangent du temps. Il s'agit de temps d'usage ou d'accès à des services, bases de données, d'abonnements, de production et livraison ultra-rapide « *just in time* », de contrôle du « *lifetime value»* , la valeur de temps de vie des clients profilés et individualisés, etc...

---

[31] Rifkin J. *L'âge de l'accès,* Paris, La Découverte 2000 p.15 Le titre anglais est encore plus significatif : *The Age of Access. The New Culture of Hypercapitalism where All of Life is a Paid-for Experience* (New York, Putman's sons 2000)

[32] Jeremy Rifkin précité, par exemple. Voir aussi son long entretien avec Libération sur http://www.liberation .

Reprenant l'idée du prix Nobel d'économie Herbert Simon, Pierre Lévy fait remarquer que la cyberéconomie, inaugure une économie de l'attention[33] où il s'agit moins de fabriquer et vendre des choses que « d'attirer, de canaliser et de gérer des flux d'attention. »[34] car « dans le cyberespace, il est encore plus évident que ce sont les mouvements de notre attention qui dirigent tout. Nous n'avons même plus besoin d'acheter pour orienter l'économie, il nous suffit de diriger notre attention vers telle ou telle zone de l'esprit collectif. »[35] .

Toutes ces notions convergent autour de l'idée de temps. Nous entrons dans une économie du temps évalué (l'avantage concurrentiel consiste à exploiter une innovation technique, à occuper un créneau ou à anticiper une tendance avant la concurrence, à faire des économies de temps plutôt que d'échelle). Elle est aussi une économie du temps désiré (celui que les consommateurs sont prêts à consacrer au service ou au produit proposé), et du temps vendu (la sphère marchande prenant en charge chaque minute de la vie quotidienne par des réseaux de conseil, distraction, relation, etc.).

Tout cela peut s'interpréter en termes guerriers. Là où tous sont en compétition pour le temps, il est plus facile de voler ou d'altérer le temps du concurrent. L'infoguerre provoque des retards, une dispersion ou une perversion du temps de la victime handicapée par une période d'impuissance. Quand tout savoir et toute richesse circulent sous forme intangible, il est plus aisé de faire une razzia sur des électrons que sur des troupeaux de moutons : un réseau s'attaque plus facilement qu'une usine. Quand le monde est dirigé par les manipulateurs de symboles ou « analystes symboliques »[36] de la nouvelle classe dirigeante, et quand la circulation l'emporte sur la production, les luttes éclatent là où réside la puissance.

Facilité de l'attaque et enjeu de l'attaque donnent la prime au plus agressif. Dans un monde du contrôle à distance, on se bat à distance. C'est le durcissement de l'économie : dans un nouvel ordre mondial, ni la force des armes, ni l'influence des idéologies ne semblent plus décider du

---

[33] Voir http://www.firstmonday.dk/issues/issue2_4/goldhaber/

[34] Lévy P., *World Philosophie* , Paris, Odile Jacob, le champ médiologique, 2000, p. 131

[35] ibid. p. 132

[36] L'expression est de Robert Reich *The Work of Nations,* New York Random House,1982

sort de la planète. Le marché et les modèles techno-culturels déterminent les nouveaux rapports de force. Ici encore, la dominance suppose le contrôle des flux et des attitudes. La bataille touche aussi les règles (négociations de l'O.MC., décisions du FMI, choix des instruments monétaires, règles techniques ou éthiques de production comme pour les OGM ou les normes de pollution autorisée, ou simplement outils intellectuels d'analyse de l'économie, modèles de vie ou de conception de l'entreprise). Dans une économie ultra agressive, il n'est question que de raids boursiers, de fusions et acquisitions pharaoniques et où l'argent parcourant la planète en temps zéro se moque des pouvoirs locaux et récompense le « différentiel de déplacement ». L'affaiblissement des protections, de l'État, des frontières et situations acquises, sont autant de stimulants pour les prédateurs.

Le pirate

La troisième forme de la guerre de l'information est celle des particuliers. Ils la mènent ou la subissent : guerre de tous contre tous, pirateries en tout genre, guerre de Léviathan contre tous (le côté Big Brother) voire guerre de tous contre Léviathan (actions militantes).

Une telle guerre n'est pas seulement menée au service d'intérêts privés. Elle se déroule sur la frontière de la sphère privée et pour son existence même. Dans le pire des cas, dit Winn Schwartau « Votre vie peut être bouleversée si votre Moi numérique cesse d'exister. C'est un meurtre électronique dans le cyberespace : vous avez tout simplement disparu. »[37]. Voir vider ses comptes bancaires à distance ou devenir la victime de bases de données qui ne vous attribuent plus le bon numéro de sécurité sociale ni les bons diplômes, est un scénario kafkaïen auquel il faudra s'habituer.

[37] Winn Schwartau. Première publication dans "Information Warfare", New York, Thunders Mouth Press.1994 Disponible sur Amazon.Com

Mais on reste là encore dans le domaine des délits astucieux : vol, falsification de données, emprunt d'identité. Les particuliers risquent autant que les entreprises. Ici, ce qui est privé, c'est le dommage subi.

Le thème de la « fin de la vie privée »[38] ou du « comment on vous espionne »[39] fleurit partout et reflète un autre souci. Libertés publiques et autonomie psychologique des individus sont liées au contrôle de la technique. Interviennent ici la révolution numérique (qui tend à rendre chaque trait ou acte enregistrable), l'État (dont la souveraineté suppose aussi la régulation de la technique sur son territoire et la définition de la sphère privée), et les appétits économiques qui souhaitent des consommateurs prédictibles et maniables.

Les Nouvelles Technologies engendrent des militants eux aussi d'un type nouveau. Ils sont d'abord individualistes : l'État, les grandes organisations leur apparaissent à la fois comme nocifs et comme archaïques. Ils militent par et pour les techniques numériques afin d'échapper à toute forme de contrôle ou d'autorité. Les combats pour le droit à la cryptologie, l'initiative de diffuser gratuitement le logiciel PGP[40] dans l'espoir de rendre tout citoyen capable d'échapper aux services d'écoute, la lutte contre Echelon sont des signes avant-coureurs de ces mobilisations au nom d'une idéologie de l'autonomie. C'est une liberté sans objet ni projet précis qui est réclamée, hors de tout projet politique. C'est un « foutez nous la paix » pur et dur. Ainsi la très puissante Electronic Frontier Fondation proclame : « Nous devons déclarer nos alter ego virtuels inaccessibles à votre autorité, alors même que nous acceptions votre souveraineté sur nos corps. Nous nous répandrons à travers la planète et personne ne pourra stopper nos pensées. Nous créerons une civilisation de l'Esprit dans le Cybermonde. » [41]

---

[38] Paul Virilio *La fin de la vie privée* in *Penser le XXI° siècle*, Manière de voir N°21, Juillet Août 2000, Paris, Le Monde diplomatique.

[39] Voir par exemple le dossier très représentatif de Capital d'Octobre 2000

[40] Puissant logiciel de cryptologie dit Pretty Good Privacy, qui fut distribué à tous les internautes par Fred Zimermann, en 1991 au grand dam des autorités fédérales américaines. Le récit de cette aventure se retrouve dans Guisnel J., , *Guerre dans le cyberspace*, Paris, La Découverte 1997 et Dufresne D. et Latrive F., *Pirates et flics du Net,* Paris, Seuil, Contre-enquêtes, 2000

[41] Déclaration d'indépendance du Cybermonde de l'Electronic Frontier Foundation et John Perry Barlow in Dufresne et Latrive précités. L'EFF (http://www.eff.org) est sans doute la plus puissante

La nouvelle idéologie est aussi tribale. On voit se multiplier des communautés virtuelles qui se réuniront dans le cybermonde par affinités temporaires, pour jouer, commercer, créer des institutions, vivre une autre vie dans le virtuel[42]. Avec ses gourous comme Howard Rheingold[43] et Hakim Bey, cette mouvance aspire à l'utopie (u-topie qui veut dire situé nulle part est le mot parfait) voire à une insurrection numérique. Ainsi, se réclamant de l'exemple des pirates du XVIII siècle qui créaient sur leurs îles des zones soumises à leur seule loi, Hakim Bey proclame les droits au « nomadisme psychique », à l' « anarchie ontologique », à la « disparition »[44]. On peut juger que ce type de propos, avec ses références à Timoty Leary, pape du LSD des années 60, à Baudrillard ou aux soufis, reflète les obsessions d'intellectuels américains et que la force de frappe de ces révolutionnaires ne menace guère l'État. Pourtant, l'apparition de la net-idéologie vaut symptôme.

Les capacités de nuisance des NTIC n'est rien en soi. Pour qu'elle présente un réel danger, il faut la multiplication des motivations. Les raisons pour lesquelles un individu ou un groupe s'en prend par électrons interposés à l'État, à une entreprise, à une institution défient presque l'inventaire. Citons pêle-mêle : - recherche de la performance et du statut au sein de mini-groupes de cyberguerriers, *hackers* ou autres– sabotage au service de rivaux d'une firme-- guerres de « gangs » entre tribus de hackers ou de simples compétitions entre groupes – motivations « éthiques » proclamées (volonté de « punir » un gouvernement totalitaire ou une compagnie qui ne respecte pas l'environnement) – militantisme ou soutien à un mouvement de libération (Chiapas, mouvements anti-nucléaires, pro-kurdes, anti Mac Donald, etc.) - paranoïa (lutte contre les services secrets et le gouvernement assimilé à Big Brother) – crime organisé-terrorisme au service d'un gouvernement - entraînement d'apprentis»[45], – vengeance (par exemple d'employés licenciés) – chantage ou profit (créer un virus redoutable pour vendre le

---

des organisations de défense de la vie privée sur Internet. Voir aussi http://www.epic.org (Electronic Privacy information center) ainsi que http://www.privacyinternational.org, et http://privacy.net

[42] voir Quéau P. in coll. *L'Empire des techniques Nouvelles Images*, Paris, Points Seuil, 1997, p. 135

[43] Rheingold Howard, *Virtual Community*, New York Addison Westley, 1993

[44] Nombre de textes d'Hakim Bey (de son vrai nom Peter Lamborn Wilson) sont disponibles sur http://www.babelweb.org /virtualistes. En français voir : *TAZ.*, Paris, Éditions de l'Éclat, 1997

[45] Winn Schwartau dans *Cybershock* précité considère que les « script kiddies, wanabees, Push-Button hackers » et autres apprentis qui appliquent les recettes de piratage des autres (dont ils reprennent les scripts sur Internet) représenteraient 95 % des intrusions sur Internet.

conte poison) – vol (cyberescroquerie) - et parfois simple envie de maîtriser le fonctionnement des choses ou goût de la compétition intellectuelle.

Dans le cybermonde, les frontières entre crime, jeu et rébellion ne sont pas mieux fixées que les séparations entre bons et mauvais *hackers* (chapeaux blancs et chapeaux noirs, dans leur jargon)[46]. Ou celles qui différencient l'activisme (qui consisterait simplement à défendre une cause sur le Net), des opérations plus agressives (« *hacktivism* », disent les anglo-saxons, formant un nouveau mot avec *activism* et *hacker*) comme le blocage ou le détournement de sites adverses surtout à des fins de propagande et enfin le véritable cyberterrorisme capable de provoquer de sérieuses pertes économiques ou militaires[47].

• • • • •

L'imagination aux armées, des scénaristes au Pentagone ? C'est peut-être pour demain. De gourous de la « *soft-war* » comme le producteur De Caro, le personnage qui a inspiré *Des hommes d'influence*,[48] proposent donc aux militaires U.S. des séminaires « mensonges, viols et

[46] Pour se renseigner sur le jargon des *Hackers* et sur de multiples catégories et nuances que nous n'avons pas la place de développer ici, visiter le site http://fwi.ua.nl

[47] Outre les sites précités, on se fera une assez bonne idée des réalités du « hacktivisme » sur Internet en visitant ces adresses URL :
http://www.samizdat.net : hébergement de sites « alternatifs »
http://www.indymedia.org agence de presse
http://www.attac.org/indexfr.htm : ATTAC
http://www.assises.sgdg.org : assises pour un internet « non marchand »
http://www.privacyinternational.org : mouvement anti surveillance
http://www.iris.sgdg.org IRIS : Imaginons un Réseau Internet Solidaire
http://www.transfert.net Webzine
http://www.salon.com : revue US
http://www.monde-diplomatique.fr site du mensuel
http://www.homme-moderne.org/societé/socio :revue électronique
http://www.new-media-and-society.com : critique des médias
http://www.ctheory.com : revue critique en anglais
http://www.cryptome.org Centre d'information sur la surveillance en anglais
http://www.ecirioa.org/Observ.htm : Observatoire de la mondialisation

[48] Le thème du film (*Wag the Dog*) de Barry Jevinson était qu'un président des États-Unis embarrassé par une scandale sexuel, produisait une fausse guerre en Albanie, mise en scène par des spécialistes d'Hollywood. Voir http://www.wag-the-dog.com/

vidéos ». Les innombrables sites consacrés aux « *Psyops* »[49] fourmillent de synopsis dans le plus pur style d'un *Mission Impossible* revu par *Matrix*.

Ces hypothèses ont inspiré des essais de politique-fiction pleins d'humour[50]. Par contraste, les scenarii des spécialistes en « psyops », semblent d'une puérilité affligeante. Il s'agit le plus souvent de diffuser auprès des télévisions des images d'un homme politique recevant un pot-de-vin ou rencontrant des néo-nazis[51], ou de produire de séquences de Saddam Hussein en train de manger du porc afin de le déconsidérer auprès de son peuple[52]. Dans les armes supposées des brigades de Psyops ne manqueraient, dit-on, ni les hologrammes[53] destinés à faire des projections en trois dimensions sur le champ de bataille ni le contrôle de l'esprit à distance[54]. Il n'y manque surtout aucune idée qui n'ait été ressassée dans les bandes dessinées depuis un demi-siècle.

À voir ! Pour le moment, les seules images truquées qui aient joué rôle notable, et encore relatif, sont les photos caviardées de Trotski ou les faux reportage TV de Timisoara : pas d'images virtuelles qui aient changé la face de la Terre. Quant aux piratages de site sur Internet, ils existent, comme le montrent les exemples des tigres du Tamoul, du sous-commandant Marcos[55] ou de diverses batailles de courrier électronique pendant la guerre du Kosovo[56]. Mais leur efficacité réelle et surtout durable resterait encore à démontrer. Dessiner des moustaches sur un faux site de Haider est une chose, lancer les foules indignées dans la rue en est une autre.

Tous ces trucages s'inscrivent dans le cadre d'un projet : le « management de la perception » consisterait à contrôler toutes les représentations du réel de l'adversaire ou de la victime. Le concept est né chez les militaires, les spécialistes de la guerre économique l'ont repris à leur compte. L'idée est excitante : la victoire se gagnerait dans la tête de l'ennemi et non contre le

---

[49] Le site http://www.geocities.com/Pentagon/102/psyocrests.html donne la nomenclature des différents corps d'armée et des sections impliquées dans les Psyops aux U.S.A.

[50] Nous pensons au livre de Gérald Messadié G., *Vingt-neuf jours avant la fin du monde* Paris, Robert Laffont 1995, qui décrit un gigantesque cybersabotage mené par une secte zen.

[51] Ces deux exemples sont également empruntés à *Cybershock* p. 430

[52] Cette fois l'idée est dans Adams J., *The Next World War*, New York, Simon and Schuster, 1998

[53] http://www.sonic.net/~west/nsamindcontrol.htm

[54] Voir les exemples donnés par http://www.conspiracycafe.com/

[55] Voir une anthologie dans Destouche G., *Menace sur Internet- Des groupes subversifs et terroristes sur le Net*, Paris, Editions Michalon, 1999

[56] Voie P. Sabatier *Le Net arme de propagande* in Libération du 15 Avril 1999

corps de l'ennemi. Mais la réalisation est pour le moment encore discutable. Les cyberdisciples de Sun Tse ou les machiavéliens numériques ont beau répéter que le suprême raffinement consiste à s'en prendre aux plans ennemis ou se réclamer de la programmation neuro-linguistique, leurs performances ressemblent encore trop souvent à des jeux de potaches.