LA CYBERGUERRE

par Laurent Murawiec

Le cyberespace

Le cyberespace constitue aujourd'hui une dimension à part entière de l'activité humaine, à l'égal de la terre, de la mer, de l'air et de l'espace. Mieux, le cyberespace enveloppe les autres dimensions; il en conditionne la marche et en restructure de plus en plus les activités.

Né d'une triple révolution technologique survenue au cours du dernier quart de siècle - électronique, informatique et télécoms - le cyberespace est le "continent" virtuel constitué par les millions de communications numériques qui relient à chaque instant les centaines de millions de microprocesseurs qui équipent les satellites, les téléphones, les ordinateurs, mais aussi les ordinateurs qui contrôlent l'industrie, les infrastructures de transport aérien, ferroviaire et routier, l'énergie à tous ses stades, le système bancaire, financier et boursier, etc. Avec la fédération planétaire des réseaux d'ordinateurs qu'est Internet, le cyberespace est devenu un maillage véritablement permanent de la planète.

A la différence des autres dimensions, le cyberespace est dématérialisé (sauf pour son infrastructure): il est constitué de paquets d'électrons voyageurs, et non de matière solide. Il est déterritorialisé: la position géographique des participants est indifférente. Il est modulaire et décentralisé, ne dépendant d'aucun "centre" ni d'aucun central: par définition, son haut degré de redondance le met à l'abri de la destruction d'un nombre élevé de ses nodes. Sans hiérarchie, ses structures sont aplaties: il se passe des étages intermédiaires jusque là indispensables. Il tisse une connectivité généralisée entre toutes les sortes d'acteurs qui y participent. Et, nouveauté renversante dans l'histoire humaine, c'est en temps réel ou quasi réel que se passe tout cela.

Les prochaines étapes de l'essor du maillage cyberspatial profiteront de l'extrême miniaturisation des microprocesseurs et de l'élévation concomitante de leurs performances (mémoire, vitesse d'exécution, puissance de calcul, etc.) pour les intégrer directement à un éventail très large d'objets, et en les y insérant dès la fabrication: du four à micro-ondes à l'ordinateur répondant au doigt, à l'œil et à la voix, du réfrigérateur rendu "intelligent" et capable de passer commande pour remplacer ce qui a été consommé aux pièces d'aviation placées sous surveillance continue par des réseaux serrés de puces préimplantées pour en mesurer l'usure et les autres paramètres de performance et de sécurité, il ne s'agira plus de microprocesseurs isolés et incommunicants, ni même de boucles locales, mais d'une mise en réseau généralisée des hommes, des processus qu'ils orchestrent et des objets qu'ils manipulent, leur branchement universel sur Internet.

Le cyberespace ré-agence les autres dimensions, qu'il pénètre et réorganise: grâce aux instruments satellitaires, il devient par exemple système capacitant de l'agriculture et de la pêche, il est consubstantiel à la quasi-totalité des industries, des moyens de transmission et de communication, en bref, de toute activité qui dépasse la simple subsistance.

Du point de vue stratégique, et du point de vue militaire, toute dimension substantielle de l'activité humaine, *a fortiori* une dimension d'une telle envergure, est **un enjeu et un champ d'intervention**. Il faut l'observer, la reconnaître, s'y protéger, y intervenir. La militarisation de l'air commença par l'observation avant de passer à la défensive et à l'offensive pendant la Première Guerre Mondiale, et à une grande diversification des fonctions et missions militaires de l'aviation par la suite; de même, l'espace a initialement été exploité à des fins d'intelligence, de surveillance et de reconnaissance avant d'être militarisé par les missiles qui le sillonnent, avant que des armes spatiales ne soient

mises en place, défensives d'abord (ASAT), puis armes d'attaque. Le cyberespace traverse le même cycle, à une vitesse accélérée, ce qui est tout normal, puisque ce sont des paquets d'énergie organisée qui y circulent à vitesse électronique.

La guerre cyberspatiale

La cyberguerre sera donc l'ensemble des activités d'ordre et d'importance militaires qui ont lieu au sein de cette dimension nouvelle.

Avant d'examiner ce qu'est effectivement la cyberguerre, précisons ce qu'elle n'est pas: on utilise souvent à contresens le terme spécieux de "guerre de l'information", à la fois pour mal traduire le terme américain d'*information warfare*, et pour exciter les foules autour de "guerres" inexistantes, mais aux effets dramatiques sonores. En anglais, *Information* ne se réfère pas aux "nouvelles" (*news*), mais aux technologies de l'information, aux processus qui en dérivent et à leurs contenus cognitifs. *Information warfare* sera donc, si l'on veut, la guerre informationnelle et informatique, mais pas du tout "guerre de l'information".

En l'occurrence, parler de guerre est un abus de langage: on confond concurrence, rivalité, conflit et guerre: on prend la métaphore pour la réalité. Quand on parle de "guerre de la saucisse" ou de "guerre de la morue", à part quelques pièces de charcuterie ou de poisson tombées au champ d'honneur, on saura bien qu'il s'agit de rivalités commerciales où charcutiers et harengères des deux camps se crêpent le chignon, sans pour autant faire appel aux chars d'assaut ou aux croiseurs lance-missiles pour vider la querelle.

Les cris d'orfraie poussés pendant des années par tel ancien dignitaire de la République sur le thème "nous sommes en guerre", l'abus journalistique du terme ("guerre commerciale", etc.) ne doivent pas permettre que les mots s'imposent à la pensée et la déterminent à la faveur d'une montée aux extrêmes de la dramatisation. Ne pensons pas par slogans, nous finirons par penser comme des slogans. Il n'y a pas aujourd'hui de "guerre de l'information". Il y a les **méthodes, stratégies et moyens de guerre informatique et électronique**, **de guerre informationnelle et de guerre psychologique**, dont l'ensemble constitue la cyberguerre, traduction appropriée de l'*Information warfare*.

Première forme de cyberguerre, **l'attaque informatique** lancée pour dé-

grader, désarticuler, neutraliser ou détruire l'infrastructure militaire de l'ennemi, et plus précisément ses capacités de **C4ISR**: commandement, contrôle, communications et calcul d'un côté, intelligence, surveillance et reconnaissance de l'autre. Au lieu d'envoyer des chasseurs-bombardiers furtifs éradiquer la capacité radar et transmission d'un ennemi, on utilisera des moyens informatiques offensifs qui sèment le chaos dans les circuits et dans les ordinateurs, mâchant et broyant les logiciels, créant failles et ruptures incapacitantes dans le dispositif ennemi. Virus, ver, cheval de Troie, bombe logique: que l'agent informatique soit dormant et réveillé sur signal, ou injecté au moment voulu, l'objectif est d'empêcher la circulation des signaux, des données et des informations chez l'ennemi, de la corrompre afin de dégrader sa conscience situationnelle, au niveau des Etats-majors aussi bien que des unités, et à tous les échelons intermédiaires.

On opacifie ainsi le champ de bataille aux sens de l'ennemi, on le rend sourd, muet et aveugle, et donc paralytique. La cyberguerre le transforme en aveugle de Breughel, en maréchal de Soubise.

Deuxième forme de cyberguerre, l'attaque dirigée contre l'infrastructure civile de l'adversaire: créons **le chaos chez l'ennemi**. Puisque l'amont de la bataille, amont scientifique, technologique, industriel et logistique, communicationnel et informationnel est de plus en plus prépondérant dans la conduite de la guerre, paralyser l'amont ennemi et y semer la confusion est un mode d'action militaire hautement productif: c'est couper l'aval militaire de ses bases, comme un MacArthur tranchant net le lien entre bases japonaises au cours de la guerre du Pacifique.

Les **cibles** visées sont principalement:

1/ les infrastructures de transport: contrôle du trafic aérien, centres de contrôle, lignes et nodes de circulation de l'information qui organisent le trafic ferroviaire, mécanismes de gestion de la circulation routière et urbaine et périurbaine, des tunnels, etc.;

2/ la gestion et la distribution de l'eau, du gaz et de l'électricité, les centrales nucléaires, thermiques et hydroélectriques, les lignes à haute tension, les stations qui gèrent les ressources hydriques, etc.;

3/ les réseaux de télécoms, centraux téléphoniques, réseaux cellulaires, moyens hertziens, moyens et liaisons satellitaires**;**

4/ les circuits bancaires et financiers, du *clearing* aux distributeurs de billets, les transferts de fonds nationaux et internationaux par voie électronique, les bourses et les marchés monétaires et financiers;

5/ les capacités nationales d'émission hertzienne, radio et télévision, réseaux et circuits informatiques, le câble, le satellite…

A l'énoncé de cette liste, on conçoit aisément l'immense champ d'action ouvert à cette forme de guerre informationnelle, et les chocs paralysants qu'elle est susceptible d'infliger, non seulement à des pays et à des économies hautement développés, mais aussi à des pays apparemment moins vulnérables car plus primitifs et moins équipés électroniquement et informatiquement. Rien n'est moins sûr. Car le haut de gamme des capacités modernes de ces pays est ultra dépendant. Chaos urbain provoqué par la manipulation du système de gestion de la circulation automobile dans des mégapoles, anéantissement des capacités de phonie cellulaire; tout ce haut de gamme indispensable transite par le cyberespace. En intervenant contre l'amont cyberspatial ennemi, nous réduisons, nous neutralisons peut-être sa capacité militaire.

Troisième composante de la cyberguerre, la **guerre psychologique**, qui lancera des attaques visant la conscience situationnelle et la conception du monde de la population de l'adversaire. En ce sens, la cyberguerre se fait ici guerre informationnelle.

L'histoire de la guerre psychologique est ancienne et riche d'expériences. Son objectif est de créer et d'implanter chez l'ennemi une fausse réalité, une pseudo réalité: ayant réduit, distordu ou détruit son contact avec la réalité, l'action que nous menons contre lui dans cette réalité est d'autant plus efficace: l'ennemi voit des fantômes, la population ennemie craint les spectres que nous avons suscités: c'est le *Psychological Warfare Executive* et d'autres instances du renseignement anglais et américain, créant l'"homme qui n'existait pas", le 5ème Bureau français créant la "bleuite" pendant la Guerre d'Algérie, c'est la *desinformatsiya* soviétique suscitant la psychose de la bombe à neutrons, "la bombe capitaliste qui détruit les gens pas les bâtiments" dans certains pays européens. L'intox, en bref, veut faire perdre le Nord, elle veut désorienter - le langage a bien raison d'utiliser ces termes spatiaux. La population ennemie, ayant perdu ses repères, sera déboussolée. Et, bien sûr, notre attaque sera menée avec les formidables moyens que les technologies de l'information mettent entre nos mains.

Le but du jeu sera donc de saper la confiance qu'accorde une population à ses repères traditionnels, l'Etat et ses organes au premier chef. Moins une société est évoluée, plus l'Etat y occupe une position centrale, moins la société civile y est autonome. Or, les nouvelles technologies de l'information opèrent un **décentrement de l'Etat,** qui est bouté hors de sa position traditionnelle, telle la Terre par Copernic, et renvoyé en orbite extérieure: les monopoles traditionnels sont brisés. Dans l'URSS stalinienne, les postes de radio étaient préréglés sur une, deux ou trois fréquences. Dans l'URSS brejnevienne, on ne pouvait choisir qu'entre l'un et le même, entre la *Pravda*, *Izvestiya*, TASS, Radio Moscou, et leurs relais ou éditions locaux. Mais graduellement les radios étrangères devinrent la référence en matière d'information: la référence - BBC ou *Radio Free Europe* - était désormais située à l'extérieur du système, sapant la crédibilité des media officielles, institutionnalisant et légitimant l'existence du dissensus. Le totalitarisme repose sur le consensus abêti. Le remède n'est pas souverain, mais il est important. Le fax joua un rôle significatif pour soutenir et fédérer le *Solidarnosc* polonais, de même que le mouvement dissident et démocratique dans la Chine du Printemps de Pékin. Aujourd'hui, *Voice of America* expédie à des dizaines de milliers d'adresses e-mail en Chine des paquets d'information que ne peuvent filtrer les sbires du régime: les exigences de la modernisation empêchent de tout filtrer sans tout casser.

Mais cela, c'est de l'information et de la propagande "blanche". A côté, on trouve les opérations "grises et noires" qui ressortent de la manipulation et de la tromperie. La fausse nouvelle et la rumeur biaisée sont vieilles comme le monde, ou comme la guerre: Ulysse se sert de la ruse, *to stratagèma* en grec. La télédiffusion satellitaire directe en multiplie les moyens, avec ses centaines de chaînes. Les forums de discussion d'Internet servent déjà de chambres d'écho pour l'injection de campagnes de fausses nouvelles ou de rumeurs.

Plus puissamment, on s'intéressera à l'induction de mouvements culturels et politiques par ces moyens. Tout comme les Islamistes algériens utilisèrent une projection laser de versets du Coran sur des nuages bas à Alger, on utilisera la télédiffusion satellitaire directe comme moyen de guerre. Après mise hors d'état de nuire des émetteurs et relais de télévision hertziens d'un pays attaqué (par commodité, on prendra l'Irak comme exemple) par voie d'attaque informatique ou par bombardement, un satellite lancé pour l'occasion télédiffusera sur les fréquences désirées des images vidéomorphées montrant le dictateur moustachu en situation plus que pénible - avouant au Conseil de la Révolution sa criminelle incurie, son mépris du peuple et la tromperie sciemment infligée à

celui-ci. D'autres vidéomorphages le montreront dans des positions et se livrant à des activités vivement réprouvées par la morale et la religion locales. Depuis *Forrest Gump*, *Wag the Dog* ou *Jurassic Park*, on sait à quel point ces effets spéciaux sont l'enfance de l'art. Les vessies deviennent des lanternes. On peut faire croire au maréchal de Soubise qu'il a retrouvé son armée. Un extraordinaire **état de confusion** peut être créé. Peut-être ne durera-t-elle que quelques heures - assez peut-être pour créer des ruptures, pour sidérer, pour paralyser, comme un grenade immobilise des terroristes pour quelques instants cruciaux.

Essor, parades, perspectives

La cyberguerre, dans les formes diverses esquissées ici, ne remplace pas la guerre tout court. Elle la complète, elle la soutient, elle la réorganise. Le cyberguerrier ne remplace pas le guerrier, pas plus que le savant atomiste n'a remplacé le tankiste: les missions en sont cependant réorganisées.

Bien sûr, à chacune des formes de cyberguerre présentées existent ou existeront des parades et des contre-mesures. Rien que de très normal: l'essentiel, c'est d'être en avance plutôt qu'en retard, c'est de pouvoir frapper dans un temps et d'une manière dont l'ennemi ne peut se protéger ni se défaire. C'est, comme toujours à la guerre, le **différentiel** qui compte, et non la masse brute, l'initiative plutôt que l'abri.

Plus un pays est développé, plus il possède d'interfaces informatiques qui permettent et favorisent, comme autant de "ports" informatiques, la pénétration de pirates lançant des opérations offensives. Mais plus le pays est développé, plus il possède également de capacités informatiques permettant de monter sa propre défense: la cyberguerre est autant une guerre défensive qu'offensive.

Voyons aux Etats-Unis l'*Air Force Information Warfare Center,* situé sur la base aérienne de Kelly, près de San Antonio au Texas, dont l'une des principales fonctions est l'*Automated Security Incident Measurement* (mesure automatique des incidents affectant la sécurité, ASIM) dont s'occupe l'équipe de réaction informatique d'urgence: elle mène la chasse aux intrusions illicites et aux pirates informatiques qui s'attaquent aux réseaux de la défense américaine. L'Université nationale de Défense a lancé depuis plusieurs années un programme de formation des *Information Warriors*, les cyberguerriers, à savoir des officiers qui en sortent diplômés et nantis de capacités opérationnelles.

Le 609ème escadron de guerre informationnelle de l'armée de l'Air américaine est une unité de guerre informationnelle défensive opérationnelle qui accompagne désormais en campagne la 9ème *Air Force*. La Marine possède désormais son Centre de guerre informationnelle, le *FIWC*. La protection des flancs et des arrières informatiques est devenue essentielle: s'il est vrai que le centre de gravité des forces armées américaines est maintenant situé dans le cyberespace, c'est là que tout ennemi sérieux voudra attaquer, c'est là la dimension qu'il faudra défendre. Et c'est de là que partiront des assauts informationnels dirigés contre les œuvres informatiques vives de l'ennemi. Déjà existe à Norfolk, en Virginie, un Commandement de cyberguerre interarmes unifié (*Joint Services Information Warfare Command*, JSIWC).

Même si la cyberguerre n'en est qu'à ses débuts, que certains de ses concepts, certaines de ses procédures et opérations souffrent encore d'imprécision et de flottement, le rôle et l'importance croissants des technologies de l'information et des événements du cyberespace peuvent nous assurer que la cyberguerre ne fera que croître. Il n'est pas interdit de s'y préparer.

Laurent Murawiec, consultant auprès du Ministère de la Défense, enseignant à l'EHESS, a publié en 1999 chez Perrin une nouvelle traduction du De la Guerre *de Clausewitz. Son livre* Effets spéciaux: la Guerre au XXIè siècle*, consacré à la " révolution dans les affaires militaires " aux Etats-Unis, paraît en janvier 2000 chez Odile Jacob.*