



bdc
Base de Connaissance

DES MISSILES, DES EMISSIONS, DES ELECTRONES

L'information, c'est la guerre

Mots clés

Cyber terrorisme, Réseau échelon, Infodominance

06/2001

Auteur :

François-Bernard Huyghe

Le(s) auteur(s) de ce document d'analyse, d'opinion, d'étude et/ou de recherche a autorisé l'AEGE à enregistrer l'article dans la base de données, dénommée : bdc.aege.fr. La diffusion, publication subséquente est aussi autorisée par l'(es) auteur(s) sur toutes formes de support écrit, électronique uniquement au sein des membres de cette association, utilisateur de cette base de données. Aucune autre forme de diffusion n'est autorisée. L'analyse, l'opinion et/ou la recherche reposent sur l'utilisation de sources éthiquement fiables mais l'exhaustivité et l'exactitude ne peuvent être garanties. Sauf mention contraire, les projections ou autres informations ne sont valables qu'à la date de la publication du document, et sont dès lors sujettes à évolution ou amendement dans le temps.

Le contenu de ces documents et/ou études n'a, en aucune manière, vocation à indiquer ou garantir des évolutions futures. Le contenu de cet article n'engage la responsabilité que de ses auteurs, il ne reflète pas nécessairement les opinions du(des) employeur(s), la politique ou l'opinion d'un organisme quelconque, y compris celui de gouvernements, d'administrations ou de ministères pouvant être concernés par ces informations. Et, les erreurs éventuelles relèvent de l'entière responsabilité des seuls auteurs.

Les droits patrimoniaux de ce document et/ou étude appartiennent à l'Association AEGE, voire un organisme auquel les sources auraient pu être empruntées. Le(s) auteurs ont expressément cédés les droits patrimoniaux subséquents à l'insertion de ce(s) document(s) dans la base de données bdc.aege.fr. Toute utilisation, diffusion, citation ou reproduction, en totalité ou en partie, de ce document et/ou étude ne peut se faire sans la permission expresse du(es) rédacteur(s) et du propriétaire des droits patrimoniaux.



Les optimistes prophétisent que le monde sera unifié par les nouvelles technologies, pacifié, voué au partage de l'intelligence et de la connaissance. L'esprit du temps exalte la communication et ses outils. Il les oppose à la violence forcément « archaïque ». À l'heure de la globalisation, de l'économie de l'immatériel, du nouvel ordre mondial, des réseaux, du village électronique et de la cybercitoyenneté, qui pourrait encore recourir à la guerre et aux armes, sinon des intégristes ou des extrémistes en proie à une « crispation identitaire » ? Tout au plus concède-t-on que les nouvelles technologies de l'information et de la communication se prêtent à de mauvais usages. En témoigne de temps en temps un fait divers spectaculaire : virus, cyberpirates, escroquerie, sans compter les inévitables pédophiles et révisionnistes sur la toile. Mais ce ne serait qu'une crise de croissance d'Internet, bref un « retard ». Quant aux pessimistes, ils répètent : aliénation, Big Brother, inégalités, catastrophe. Bref, le méchant Système. Tout est foutu. Alors, technophiles ou technophobes ? Paradis ou enfer ? Et si rien n'était joué ? Si l'alternative était plutôt : guerre ou paix dans le cybervillage ?

Depuis les révolutions militaires que concoctent stratèges et futurologues jusqu'au piratage qui menacerait tout ordinateur, en passant par les risques de chaos dans la nouvelle économie, deux facteurs communs : l'information et le conflit. L'information y participe dans tous les sens de ce terme (les connaissances que nous possédons, les messages que nous recevons, les données que nous conservons, voire les informations au sens des programmes informatiques). Le conflit, lui aussi, prend des formes nouvelles, hybrides, bizarres : pays à haute technologie contre États dits « voyous », entreprise contre entreprise, groupes militants contre institutions économiques ou étatiques, internautes contre internautes, cyberterrorisme ou concurrence dite « hypercompétitive », c'est-à-dire guerre économique sauvage, etc.

Notre société dite de l'information risque donc fort d'être celle du conflit. Un conflit qui aura l'information pour arme, pour enjeu ou pour mesure. Il s'agira d'en contrôler le contenu, la possession ou la diffusion, à l'insu d'une victime ou au détriment d'un adversaire. Dans le même temps, l'accès instantané à d'énormes mémoires interconnectées ou l'impossibilité de contrôler Internet feront du secret et de son viol de paradoxaux enjeux, de nouvelles stratégies se développeront. Nous vivons sans doute aussi dans la société du secret.

Quels sont les usages offensifs avérés des Nouvelles Technologies, en temps de paix et en temps de guerre ? Et les « vieilles » technologies, celles des mass media ? Quels jeux d'intérêts ou quelles croyances feront que ces moyens seront ou non employés ? Par qui et comment ? Quels sont les risques réels et quelle est la part des mythes ? Que faut-il craindre le plus : des mots mensongers,

des images trompeuses ou des moyens de destruction ou d'investigation invisibles, algorithmes, virus, satellites d'observation ?

Information, prédation, destruction

Longtemps la guerre s'est définie comme la lutte durable de groupes armés. Des siècles durant, les hommes prêts à donner et à recevoir la mort se rencontraient en un lieu, le front, pour une période, les hostilités. Vieilleseries ? Voici maintenant

- qu'en dépit de tous les discours sur la mondialisation la fin de l'histoire, les affrontements armés se multiplient
- qu'il devient de plus en plus difficile d'identifier de « vraies guerres » déclarées entre Etats-Nations, mais que prolifèrent d'autres conflits sanglants souvent sporadiques. Suivant son point de vue, chacun les nomme guérilla, troubles ethniques, opérations de maintien de la paix, émeutes, terrorisme, criminalité...
- que plus personne ne sait où est le front : là où explose un missile, là où a lieu un attentat, là où sont les troupes, les morts, les réfugiés ?
- que la séparation n'est pas plus claire entre la violence privée, fruit d'une avidité ou d'une inimitié et la guerre qui obéirait en principe à des finalités politiques et symboliques.
- bref que ni le temps, ni le lieu, ni les acteurs, ni les composantes de la guerre ne sont plus les mêmes.

Voici que fleurissent sous la plume de stratèges, économistes, spécialistes des nouvelles technologies des mots inquiétants, souvent précédés de « cyber » ou « hyper » ou « info » : cyberterrorisme, hypercompétitivité, cyberguerre, infodominance, etc (voir glossaire en fin de numéro). Le tout se résume dans l'idée de « guerre de l'information ». Elle consiste à dérober, détruire, pervertir l'information, depuis les connaissances intellectuelles jusqu'aux données informatiques. Son but est de produire un dommage, de gagner une hégémonie. Sa devise : « Information, prédation, destruction ». Cette guerre mobilise des panoplies militaires *high-tech*, des satellites ou des armes intelligentes, des moyens de fichage ou d'espionnage au service d'États ou d'entreprises, des outils logiciels destinés à violer des bases de données ou à saboter des systèmes informatiques. Le conflit est immatériel sans front dans le cyberspace, sans déclaration

de guerre ni traité de paix. Ses menaces inédites reflètent la complexité des systèmes numériques : des virus dans notre ordinateur aux satellites qui nous observent.

La société dite de l'information serait donc soumise à un double danger : celui de la violence archaïque toujours récurrente, celle qui martyrise les corps, et une violence nouvelle, qui brutalise ou altère des cerveaux, d'hommes ou d'ordinateurs. L'actualité fourmille d'exemples : chaque jour il est question de révélations sur le système de surveillance Echelon qui intercepte des millions de communications ou d'attaques numériques contre les géants de l'économie de l'immatériel. Dans cette guerre-là, l'élément tragique et symbolique, la mort d'homme a disparu. Subsistent en revanche la volonté d'agression, l'organisation, l'usage d'armes, même si les armes en question produisent plutôt des bits, des ondes, ou des images que des amas de chairs.

Pour ne pas s'en tenir à la plainte sur l'éternelle méchanceté de l'homme, ni se borner au catalogue des menaces technologiques, mieux vaut aller voir la réalité des choses ; c'est d'ailleurs l'objet de ce numéro. Certes, le front ne coïncide plus avec un lieu concret et le conflit n'a plus pour but de gagner des arpents de terre. Pourtant, il y a bien bataille quelque part et le conflit fait bouger des frontières. Au moins celles de nos catégories mentales.

La frontière entre mass media et nouvelles technologies

Si les manières de croire et de faire dépendent pour une part des systèmes de transmission et de transport d'une époque, les modes d'affrontement n'échappent pas à cette règle. En clair : la guerre n'est pas affaire que de missiles et de mégatonnes mais aussi d'écrans et mégabits. Nous vivions à moitié dans le monde des mass media et à moitié dans celui des nouvelles technologies. Les premiers reproduisent et propagent les mêmes spectacles partout au même rythme, les seconds transforment toute information en unités numériques indéfiniment modifiables et accessibles. Les deux mondes se déterminent mutuellement : ainsi Internet change les lois de la télévision (ne serait-ce qu'en allant plus vite qu'elle), mais le monde virtuel se nourrit des idées, des mythes et des références des médias plus anciens.

Pendant des siècles, mots et images ont accompagné l'emploi de la force : ils exaltaient un camp, son identité et ses héros et dénigraient l'adversaire. La télévision a changé cette loi de la guerre stylisée : le front, l'adversaire et la victime sont transportés de l'autre bout de la planète jusqu'à notre salon. Une image résume un conflit, une scène juge une cause. La guerre est devenue à la

fois drame humain impliquant tous les hommes parce qu'il met en scène des individus qu'il rend proches, mais aussi un spectacle que remplaceront demain d'autres images dans la perpétuelle urgence du temps médiatique. Qui contrôle l'image, gère la pitié. Il y a des guerres avec et sans images (donc ignorées : pas vu pas tué), des guerres où l'on voit les victimes que l'on fait et celles que l'on a (tel fut le cas du Vietnam), des guerres où l'on voit tout sauf les morts adverses (Irak), des guerres où l'on ne voit que des réfugiés (Kosovo)... De servante de la guerre, l'image en est devenue théâtre et tribunal. Mais, dans la vidéosphère, véridique ou non, le média est censé refléter une réalité et n'agit qu'autant qu'il convainc.

Les Nouvelles Technologies de l'Information et de la Communication créent un rapport inédit entre l'information et la force destructrice. Des techniques sophistiquées d'observation, de calcul, de visée permettent de diriger ces forces : distance et territoire sont quasiment abolis pour ceux qui disposent des armes de haute technologie. Les belligérants observent du ciel et frappent à leur gré tout point du globe. Cliniquement, proprement, (en théorie). Qui voit gagne. Furtivité, virtualité, transmission, maillage, détection, précision, direction, tels sont les facteurs de la victoire. Ces panoplies intelligentes éloignent techniquement une guerre que la télévision rapproche émotionnellement.

Commence le stade où l'information devient la force. Mi-armes, mi-médias, les ordinateurs permettent et subissent des formes de prédation ou d'agression inconnues auparavant. Ici le procédé d'abstraction atteint son comble : non seulement il n'y a plus de distance, ni de frontière dans le cybermonde, mais il n'y a plus de véritable durée du conflit (instantané dans ses actions, permanent dans son déroulement même si la victime ne sait même pas toujours qu'elle est attaquée). Plus rien de tangible non plus dans les opérations : des bits reproduits, des mémoires pénétrées, des algorithmes perturbés. Certes, les conséquences de cette bizarre violence par électrons interposés sont, elles, très visibles : chaos, perte financière, domination. Une des dernières composantes de la guerre classique s'est dissoute : la notion de civil et de militaire. Qui servent les guerriers de l'information : un pays, une entreprise, leur intérêt, une idéologie, un jeu ? Les victimes sont-elles des organisations, des entreprises, des armées, des richesses, des gens ?

Comment cohabiteront trois guerres : celle des écrans qui conquièrent les têtes, celle des armes intelligentes et celle de l'intelligence militarisée ? Comment s'emboîteront le « vrai monde » où l'on tue et où l'on meurt, le monde représenté et le monde virtuel ? De cette première question dépendra l'avenir du conflit.

La frontière entre les sphères politique, économique et privée

Là encore, nos certitudes s'effondrent. Autrefois, il y avait le politique. Il déclenchait la guerre, une violence rare, sporadique, dirigée vers l'ennemi extérieur. Il exerçait la violence légitime intérieure (donc la répression et le contrôle de la violence privée). Enfin il réglait la violence ritualisée, celle du jeu politique pacifique, théoriquement au moins dans une démocratie. L'économie était le domaine de la concurrence, compétition aux règles conventionnelles pour s'approprier des ressources rares avant l'autre, mais non pour combattre l'autre. Et puis, dans la sphère privée, l'individu poursuivait ses intérêts et ses passions. Il y avait son intimité et ses inimitiés.

Ces séparations claires sont menacées. Lorsque les moyens gigantesques d'Echelon, le système d'écoute et d'espionnage né de la guerre froide, sont mis au service de l'économie américaine ou quand des entreprises luttent par des moyens d'espionnage ou de sabotage dignes de cette même guerre froide, il devient évident que conflit et concurrence se rapprochent. Quand « faire de la politique » ne consiste plus à participer à des élections ou à dresser des barricades, mais à militer dans le monde virtuel d'Internet en attaquant un site d'organisme ou de société situé à l'autre bout du monde, les mots changent de sens. Quand des milliers de gens réclament de leur gouvernement le droit d'utiliser la cryptologie et combattent en Bill Gates comme un avatar de Big Brother, la distinction entre vie privée et vie publique s'obscurcit. Quand la conquête des marchés se militarise, qu'il y a des armées privées ou des États mafieux et qu'un conflit dans un monde globalisé et interconnecté implique toute la planète, alors plus personne ne sait plus où finit la paix. Quand l'État ne contrôle ni les flux d'argent, ni les flux d'information, ni les flux humains, quand les entreprises n'ont plus de frontières et quand les individus se regroupent en tribus virtuelles éparpillées dans le cybermonde, territoires, pouvoirs et normes sont bouleversés. Quand dominer équivaut à contrôler des connaissances et des réseaux, des opinions et des électrons, tout change.

La frontière entre violence, communication et technique

Il faut renoncer à l'idée simple que la violence agit sur les corps, la communication sur les cerveaux et la technique sur les choses. Et plus encore à la croyance que toute communication est bonne et toute technique neutre. Or nous vivons dans un monde où prédomine une idée, pour ne pas dire une idéologie : à savoir que les technologies de l'information et de la communication seraient par nature pacifiques, éclairantes, démocratiques. La conviction qu'Internet nous

délivrera de la rareté, de la matérialité, de la censure, de l'archaïsme identitaire, de l'ignorance, etc..., bref l'utopie qui décrit comment nos moyens de communiquer feront de l'humanité une unité intelligente et heureuse, tout cela est d'une naïveté évidente. Ce qui ne justifie pas la naïveté inverse : découvrir en toute technologie une domination cachée et dénoncer le Système diabolique.

À ces simplifications, il faudrait opposer quelques vérités anciennes. Les technologies, et en particulier les technologies de transmission ne changent les sociétés qu'autant qu'un milieu humain les reçoit (l'imprimerie n'a pas le même impact dans la Chine confucéenne, dans le monde islamique et dans l'Europe de la Renaissance). Un nouveau média ne donne pas à l'humanité en général de nouvelles possibilités d'expression et de communication, mais il réorganise nos biens symboliques (les idées, croyances et représentations) et nos façons de lutter pour imposer ou répandre ces biens symboliques. Tout langage est pour partie un combat et toute guerre aussi un langage. Nos stratégies (nos luttes partagées), nos technologies (nos instruments partagés) et nos croyances au sens large (nos représentations partagées) s'interpénètrent.

Des arguments moins philosophiques et plus pratiques devraient surtout nous faire comprendre l'importance des conflits informationnels. L'agression devient plus facile : il est plus aisé d'envoyer du courrier électronique ou d'attaquer des bases de données par modem interposé que de créer un parti ou de dépêcher une canonnière. Ses motivations changent : un *hacker* ludique ou intéressé, ou un cyberterroriste ne sont pas un guérillero ni un soldat. Les formes d'agression par les technologies intelligentes n'ont plus guère de lien avec l'emploi de la force physique. Elles consistent à créer le chaos dans un système, prélever ou altérer des bases de données intangibles, accéder à des niveaux de contrôle ou d'autorisation, emprunter des identités ou des signatures électroniques, sidérer ou saturer l'adversaire, le rendre numériquement parlant amnésique, muet et aveugle... À côté de cela, les vieilles pratiques de l'espionnage, de l'intoxication ou de la désinformation paraissent antédiluviennes. Enfin et surtout, de nouvelles fragilités se révèlent : les méga-organisations sont à la merci d'un algorithme, les individus sont menacés de méga-systèmes de surveillance. Les premières peuvent être paralysées par quelques électrons via une ligne de téléphone, les seconds peuvent être « tracés », suivis par des réseaux de surveillance qui couvrent la planète, archivés dans des mémoires interconnectées.

Pour comprendre ces formes mixtes et instables du conflit, il est inutile de compulsier les dizaines d'essais ou de rapports qui prophétisent la future société de l'information, ou célèbrent le

cybermonde et l'économie de l'immatériel, car ils évacuent superbement la question du conflit. Quant aux propos alarmistes sur les dangers de la technologie, descriptions de futurs Pearl Harbour informatiques, anthologies de crimes et délits numériques, histoires de pirates sur Internet ou de sorcellerie logicielle, ils réduisent souvent les faits au fait divers. Il faudra reconnaître ces frontières, cartographier ces nouveaux territoires, observer les occurrences, les régularités, les caractères de ces conflits informationnels. Rapporter ces nouvelles violences aux conditions économique-techniques qui les favorisent, certes, mais aussi aux mentalités et aux mythologies qui les sous-tendent, aux stratégies, aux intérêts qui les animent. C'est à cette condition que nous apprendrons à maîtriser le conflit, pas en nous réfugiant dans l'angélisme.

F.B. Huyghe

Sommaire de Panoramiques N° 52

<http://www.editions.corlet.fr/panoramiques/sun/html/nouveautes.html>

L'information c'est la guerre

Des missiles, des émissions, des électrons...

Introduction

Information, prédation, destruction François-Bernard Huyghe

I Guerre des symboles : idées et images

Au commencement était la propagande Catherine Bertho-Lavenir

Le pouvoir médiatique comme pouvoir spirituel entretien avec Régis Debray

Le « pouvoir doux » de la communication : entre utopie et hégémonie Armand Mattelart

Vivre et informer en un monde dangereux XavierRaufer

Homo commutans contre homo sapiens ? Paul Soriano

II Guerre des forces : fronts et batailles

Le cybermonde n'est pas la paix Pierre Lévy

La guerre du sens Général. Loup Francart

Réseaux d'information et mutations stratégiques Philippe Forget

Cyberconflits et cyberarmées Michel Wautelet

Gestion des crises internationales par la maîtrise de l'information Claude Michel

III Guerre de l'économie : territoires et réseaux

La désinformation, arme de guerre économique Rémi Kauffer

Les batailles.com Général. Éric de la Maisonneuve

Information et dominance, l'infoguerre vue des USA Winn Schwartau

La guerre économique du faible au fort Christian Harbulot

Les ONG instruments du libéralisme informationnel? François Mabile

La distribution des prix, marchands de traces Monique Sicard

IV Guerre du secret : citoyens sous surveillance et cybermilitants

Le citoyen victime et coupable Gilles Klein

Le secret politique à l'âge démocratique Tanguy Wuileme

La science du secret entretien avec Jacques Stern

La société du secret F.B. Huyghe

Glossaire

Bibliographie

Biographie des auteurs