La guerre dans la cinquième dimension : la guerre de l'information

Autor(en): **Richardot, Philippe**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **143 (1998)**

Heft 10

PDF erstellt am: **26.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-345932

La guerre dans la cinquième dimension: la guerre de l'information

«Nous vivons un âge conduit par l'information. Les percées technologiques (...) changent le visage de la guerre et la manière de la préparer.»

William Perry, secrétaire de la Défense des Etats-Unis.

Le XX[e] siècle a vu la guerre sortir de ses dimensions traditionnelles (la terre et la mer) pour s'étendre à de nouvelles dimensions: l'air, l'espace et l'électronique, la cinquième dimension. La guerre électronique conventionnelle consiste à localiser, brouiller ou intercepter des messages radios ou des émissions radar, sonar... Ce que les Etats-Unis appellent «Strategic Information Warfare» est d'une autre nature. L'acronyme C[4]ISR («Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance») résume bien ses moyens et ses objectifs.

Philippe Richardot

Internet et la désinformation: la nouvelle toile de Pénélope

Les théoriciens américains Alvin et Heidi Toffler prétendent qu'après les ères agraire et industrielle, nous entrons dans l'ère de l'information. A l'origine de cette ère nouvelle, le téléphone, les satellites et, surtout à partir des années 1980, les réseaux informatiques. Au cours des années 1990 se produit la révolution des autoroutes de l'information: Internet qui dérive du système Arpanet conçu pour le Pentagone pour protéger les communications et la sauvegarde des informations vitales du système de défense US. Il est désormais accessible à tous. Le nombre d'abonnés augmente chaque année et dépasse les 100 millions.

Internet véhicule toutes sortes d'informations, des plus saugrenues et des plus personnelles aux plus sérieuses et aux plus institutionnelles. La désinformation peut y trouver sa place. Les cibles de cette désinformation, bien évidemment les nations industrialisées d'Occident ou d'Asie! La première utilisation, commerciale, rejoint la seconde, politique: nuire à un Etat-concurrent ou rival. La masse et la précision des informations transmises par Internet, la capacité de créer un site ad hoc et de le perfectionner continuellement assurent une grande souplesse opérationnelle. Techniquement, grâce au système World Wide Web (W.W.W.), il est possible de créer des sites officiels (associations, universités, sociétés, institutions) et des sites personnels. Les sites antérieurs au Web, appelés sites *gophers*, étaient des bases de données fiables et institutionnelles; désormais, il est possible de créer des bases de données aux informations manipulées, de pirater un site *gopher* et de le modifier.

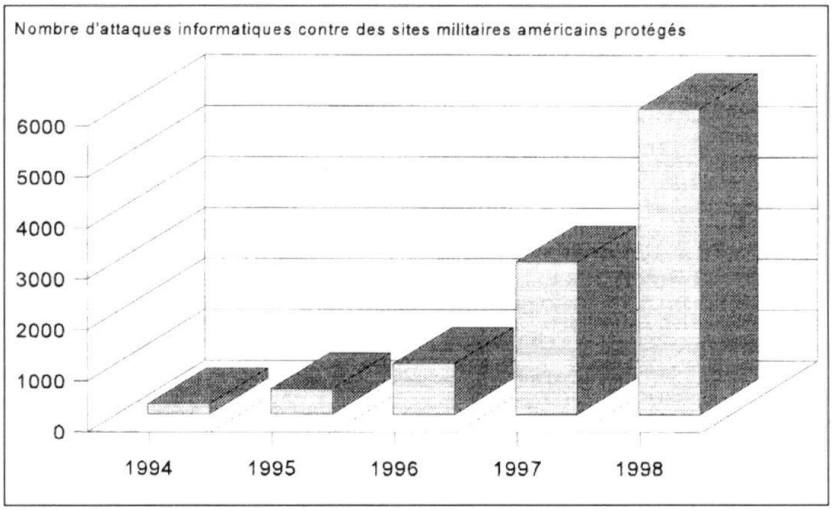
Exemple frappant: en septembre 1996, un *hacker* (pirate informatique) s'introduit dans le serveur Web de la Central Intelligence Agency (CIA) pour en modifier le titre de la page de garde en remplaçant «Intelligence» par «Stupid», avec la mention «Stop Lying» (Cessez de mentir). Ces sites sont des livres dont les pages se réécrivent continuellement, comme la toile de Pénélope... ils sont des outils de tromperie comme elle. La *Cyberwar* est la partie émergente de la guerre de l'information. Nouveaux outils, vieux principes: telle est l'évolution générale de l'art de la guerre.

L'attaque: une guerre multiforme

La guerre de l'information peut être comparée à la guerre

bactériologique. Un réseau peut télécharger un virus sans que les utilisateurs en aient immédiatement conscience. Le programme vecteur de ce virus peut être sélectif et s'attaquer à un type de logiciels, d'ordinateurs spécifiques ou à une cible précise (entreprise, institution). Dans la guerre informatique de demain, les objectifs stratégiques sont à la fois nombreux et abordables: systèmes bancaires, boursiers, fiscaux, traitement des fonctionnaires, gestion des réseaux de transport ferroviaire et aérien, télécommunications, balisage NAVSTAR-GPS, des cibles d'autant plus rentables que les sociétés industrialisées sont dépendantes de l'informatique et n'ont pas de procédure de rechange immédiate.

Ce peut être «l'arme du pauvre», d'Etats terroristes incapables de s'offrir une flotte de bombardement stratégique ou des sous-marins nucléaires, mais assez riches pour se payer des mercenaires informatiques ou former leurs propres *hackers*. D'autre part, les sociétés occidentales ne manquent pas de déséquilibrés et de mécontents. La plupart des tentatives de pénétration sur des réseaux occidentaux, officiels ou militaires, sont des actions individuelles plus ludiques que subversives. Les *hackers* cherchent le plus souvent à révéler des failles; leur motivation, leur salaire, c'est l'orgueil. L'impunité et l'indétectabilité facilitent les comportements les plus négatifs. Paradoxalement la virtualité, la dimension non-humaine du *cyberespace* réactualise le mythe de David contre Goliath. Les résultats de l'attaque peuvent se manifester de trois manières:



■ **Assaut sportif**: le *hacker* a pénétré dans le réseau et le fait savoir par un message. Il a pu piéger le programme, modifier ou voler des informations. C'est la nouvelle version du guerrier qui prend des trophées, lance des cartes de la mort, fait une parade de victoire...

■ **Assaut captif**: Son but est le vol ou la capture. Le paiement par communication du numéro de carte de crédit offre de grandes possibilités déjà exploitées. A un niveau supérieur, il est théoriquement possible de détourner des fonds considérables ou de prendre en otage un système.

■ **Assaut massif**: les caractères sur l'écran se déforment ou disparaissent, les mémoires sont vidées. C'est l'apocalypse informatique, la guerre totale!

■ **Assaut furtif**: il n'y a aucune trace d'attaque, tout est normal... ou presque. Dans les millions de calculs nécessaires à l'élaboration d'un programme aérospatial, une erreur est insérée, le prototype s'écrase. Retard et surcoût considérable. Autre scénario, les informations à l'écran sont fausses mais paraissent véridiques: vous êtes désinformés, voire anesthésiés... Sabotage et désinformation. Rien ne va plus, mais la victime ne sait pas pourquoi

En définitive, l'attaque la plus efficace, la plus sournoise reste celle qui n'est pas détectée: le mal invisible. Et il n'y a plus de sanctuaire contre ce type d'agression. De nouvelles frontières doivent être dressées. Où? Comme il n'y a pas de coalitions internationales pour coordonner la défense, ces frontières ne pourront être que nationales.

La défense: un «limes» informatique?

L'Empire romain a conceptualisé le type de frontière militaire le plus efficace de l'histoire. Il reposait sur le filtrage, le barrage et l'intervention. Ce

modèle n'est pas périmé. Les sociétés informatiques pratiquent le filtrage avec les programmes «Cheval de Troie» qui répertorient le nombre et la nature des utilisateurs de sites Internet. Des veilles signalent le jour et l'heure où certains réseaux sont fréquentés. Le barrage informatique est la solution retenue par la Chine qui établit des *firewalls* ou écluses pour empêcher les Chinois d'accéder au réseau mondial. Le ministère des Postes et Télécommunications, maître de ChinaNet a, en sens inverse, bloqué l'accès du réseau par des éléments jugés dangereux (dissidents, Taïwan, médias Américains...). Le barrage chinois fonctionne dans les deux sens, mais c'est une société totalitaire. Les nations occidentales, démocratiques et plus vulnérables, devront être plus imaginatives.

Le circuit fermé, même en alimentation électrique, semble être le moyen le plus éprouvé pour des réseaux institutionnels ou de recherche très secrets: c'est la redécouverte des douves des anciens châteaux-forts! Dans le domaine du barrage filtrant, on peut imaginer des alertes qui, à la manière des mines antipersonnel, coupent la progression de l'intrus dans un réseau dès qu'il atteint certaines limites. Des délais peuvent lui faire perdre du temps en l'obligeant à se dévoiler partiellement pour continuer son intrusion. Des sites-leurres peuvent piéger le *hacker*.

Alors vient l'intervention: lui faire avaler un virus à son insu, obliger son programme à s'auto-identifier sans qu'il le contrôle. Le système peut être aussi complexe qu'un réseau de mines: certaines évidentes, d'autres décisives, parce qu'elles le sont moins. Dans cette guerre, il faut savoir que le *hacker* se méfie de la simplicité, la complexité le rassure et lui paraît véridique. L'avortement de l'intrusion ou la mise hors-service du matériel de l'intrus ne sont que des objectifs secondaires. Le véritable but de la *cyberwar*, par opposition au monde virtuel du *cyberespace*, ne peut être que l'identification et la neutralisation «In Real Life» (IRL) de l'intrus. Outre l'identification «la main dans le sac», la constitution de fichiers sur les *hackers* devient une nécessité, de même pour leurs techniques, leurs signatures et leurs faits d'armes. Des manuels de tactiques devraient suivre...

La Gazette de la presse et des médias francophones, *février-mars 1986.*

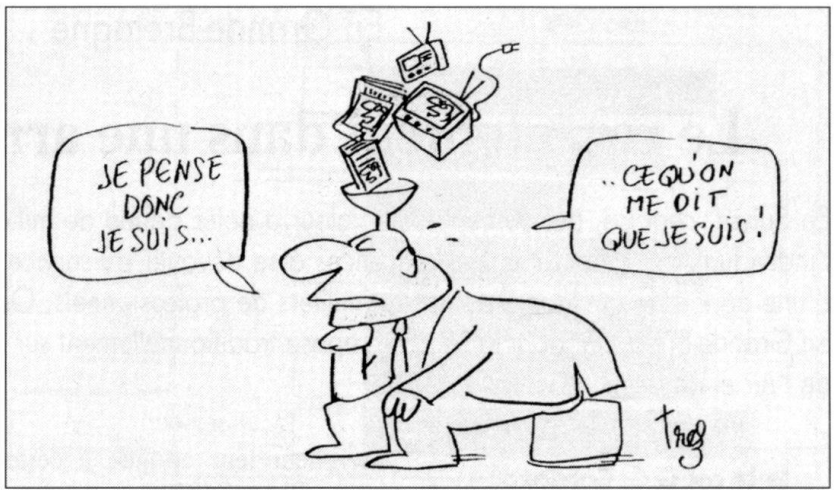
Par ailleurs, le recrutement de *cyber-guerriers* doit être une priorité de tout Etat moderne. Il ne peut être encore institutionnalisé, car nous sommes en des temps de pionniers. Le mérite et l'imagination restent les seuls critères de sélection. Le recrutement peut passer par une annonce Internet avec une invitation sur place à prouver son talent d'*Intruder* contre une rémunération susceptible de tirer hors de leur virtualité les plus doués des *hackers*. Le temps permettra de former des *cyber-combattants* opérationnels, mais l'expérience doit être effectuée rapidement, car les choses vont très vite...

Gagner la guerre de l'information

Gagner la guerre dans le *cyberespace* n'est qu'une partie de l'*Information War* (IW). Les Etats-Unis ont pris conscience les premiers de cette nouvelle forme de conflit à laquelle on était déjà parvenu empiriquement lors de la Guerre du Golfe en 1990-1991. En janvier 1995, le département de la Défense a créé un bureau chargé de l'IW. En octobre 1995, le secrétaire adjoint à la Défense pour le Commandement, le Contrôle, les Communications et le Renseignement (ASDC^{3}I)

a développé le concept de C⁴ISR évoqué en introduction. Les objectifs sont multiples.

Au plan stratégique, le renseignement est une action permanente à l'échelle planétaire et orbitale. Au plan opérationnel, gagner la guerre de l'information est un des cinq objectifs majeurs de l'US Army dans son actuelle refonte (*Joint Vision 2010*). Le but est de donner aux forces US une écrasante supériorité dans le domaine du renseignement lors des combats. La collecte de l'information par des moyens satellitaires, aériens, électroniques, humains (Special Forces) n'est pas en soi révolutionnaire. En 1990-1991, Norman Schwarzkopf, commandant en chef des troupes coalisées contre l'Irak, pouvait déjà affirmer: «Aux plans stratégique et tactique, pas un chef dans l'histoire n'a eu une meilleure connaissance de l'ennemi qui était en face de lui». Ce qui change réellement c'est la diffusion de l'information à tous les échelons pour permettre aux chefs et aux soldats de savoir où sont les amis et les ennemis dans le cadre du champ de bataille automatisé (*Digitized Battlefield*). En fin de compte, grâce au système NAVSTAR-GPS, au téléphone-satellite, aux réseaux de transmission automatiques, tout le monde, depuis le simple trooper, fera de l'IW et sera en contact avec tout le monde…



La Gazette de la presse et des médias francophones, *juin 1998.*

«Connais-toi toi-même», comme le disait Socrate, semble être la deuxième révolution du C⁴ISR. Le commandement pourra savoir «en temps réel» combien il a de monde sur le terrain et l'emplacement de chacun, le nombre de blessés, de malades, l'état des stocks de munitions, de carburant, de vivres, de produits médicaux… Le but est de transformer l'art du commandement opérationnel en un *Kriegspiel* sans inconnues. L'*IW* a également des missions offensives combinées (détruire le système de défense aérienne ennemi, paralyser son C3 (commandement, contrôle et communications) ainsi que des missions défensives (protéger le réseau de communications et d'informatique, rendre plus efficace la défense aérienne et anti-missiles).

Le concept de guerre de l'information n'en est qu'à ses débuts. Les premiers à maîtriser ces techniques auront un avantage indéniable au début du XXIe siècle. Un type de guerre qui ne fait pas couler le sang et touche autant le domaine de la sécurité que celui de la défense. Il faut y aller !

P. R.

Bibliographie:

National Communications System: *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications*. Arlington, Office of the Manager, NCS, 5 décembre 1994.

Martin Libicki: *What Is Information Warfare?* Strategic Forum. Institute for National Strategic Studies, National Defense University, 28, mai 1995.

Jean Guisnel: *La guerre dans le cyberespace*. Paris, La Découverte, 1995.

Roger C. Molander et alii: *Strategic Information Warfare. A New face of War.* Rand, National Defense Research Institute, 1996.