1995 – 1996 : souvenirs d'InfoWarCon - SSTIC 2003 - Rump Sessions

Guillaume Arcas <guillaume.arcas@free.fr>

« Peut-être l'infoguerre ne vous intéresse t-elle pas, mais l'infoguerre, elle, s'intéresse à vous. »
D'après Trotsky

Notes préliminaires :

- La présentation suivante a été faite lors des journées SSTIC 2003 de Rennes (cf. http://www.sstic.org).
- Les encadrés correspondent aux diapositives projetées durant la présentation.
- Certaines des idées rapportées ci-dessous reflètent la pensée des intervenants et organisateurs des conférences InfoWarCon 1995 et 1996 et non mes propres idées.
- La « couverture » de ces conférences s'inscrivait dans le cadre d'une mission de veille technologique ayant abouti à la rédaction d'une notice sur la guerre de l'information publiée dans un atlas de géopolitique en 1996.

Contexte

- L'affrontement Nord/Sud remplace la guerre froide et la guerre économique les conflits armés.
- Acteurs non étatiques mais conséquences nationales.
- Baisse des budgets militaires mais hausse des (nouveaux) besoins.

De la force brute à la force cérébrale...

Depuis la chute du mur de Berlin puis de l'empire soviétique, la bipolarisation du monde s'est accentuée.
D'un côté, les pays industrialisés glissent depuis 1990 vers une guerre économique et commerciale permanente dans laquelle les alliés d'hier (contre le bloc soviétique) se changent en adversaires plus ou moins déclarés. Cette guerre économique, menée par des acteurs obéissant à des intérêts privés non ou peu contrôlés par un Etat, a des conséquences dont les coûts - tant humains, environnementaux que financiers - sont entièrement (et volontairement ?) laissés à la charge des états : chômage, crises boursières, flux migratoires, pollution.

De l'autre, la violence se déchaîne dans un tiers-monde conventionnellement surarmé, ne possédant aucune culture ou tradition démocratique et formé d'Etats artificiels (héritage de la colonisation).

Tout serait pour le mieux dans le pire des mondes si les nations industrialisées n'étaient pas contraintes d'entretenir avec ce Sud sauvage[1] des relations :
- économiques : exploitation de ressources naturelles (pétrole, uranium...);
- politiques et historiques issues de la (dé)colonisation ;
- morales et humanitaires (mais bon, juste ce qu'il faut..).
- et surtout si les pays industrialisés n'étaient pas confrontés à une logique liée à la chute du mur

[1] Lire à ce sujet l'excellent ouvrage de Jean-Christophe Rufin⊡L'empire et les nouveaux barbares.

de Berlin de baisse des investissements et dépenses militaires !

C'est dans ce contexte qu'émerge aux Etats-Unis le concept d'Information Warfare[2] (IW) comme explication et remède universel à tous ces maux :
- l'IW doit apporter aux pays industrialisés et démocratiques les moyens de canaliser la violence endémique des pays du Sud ;
- ce au moindre coût tant financier qu'humain ;
- sans empêcher une lutte économique féroce entre "alliés" ;
- sans oublier bien sûr que seuls les Etats-Unis peuvent et doivent gagner ces guerres. ☺

InfoWarfare : pourquoi faire ?

- Toffler : à société de l'information, guerre de l'information.
- Émergence de l'Internet commercial.
- Robert Steele et les sources ouvertes.
- Winn Schwartau et le Pearl Harbor Electronique.

Indirectement, c'est Alfred Toffler[3] (sociologue et futurologue américain) qui donna le coup d'envoi à la campagne de médiatisation et de vulgarisation du concept d'IW.
Pour A. Toffler, la société de l'information a succédé à la société industrielle (laquelle a succédé à la société agricole). Et qui dit société de l'information dit guerre de l'information.

La libéralisation (au sens commercialisation) d'Internet va permettre à Winn Schwartau de lancer un nouveau troll : le Pearl Harbor Electronique, mythe suivant lequel il serait possible de détruire les infrastructures vitales d'un pays (i.e. Les Etats-Unis) par Internet au point de mener ce pays à la ruine.
Schwartau consacre quasiment tout son temps à porter cette bonne parole depuis bientôt 10 ans... Rappelons toutefois que les attaques du 11 septembre 2001 ont été diablement low-tech et non moins efficaces....

Dans le même temps, Robert Steele, ancien de la CIA (à ses dires, mais peut-on faire confiance à un espion ?), crée Open Source Solutions[4].

Steele et Schwartau s'allient alors pour organiser outre-Atlantique des conférences sur la guerre de l'information (InfoWarCon pour Information Warfare Conference, le mot Warfare pouvant tout aussi bien être traduit par « guerre » que par « moyens de faire la guerre »).

En 1996, la National Computer Security Association (NCSA[5]) se joint à eux.

En 1995 et 1996, Steele et Schwartau viennent porter la bonne parole sur le vieux continent à

[2] L'internaute curieux trouvera une compilation assez complète de textes «□fondamentaux□ sur la vision américaine de l'IW ici□http://www.dodccrp.org/publicat.htm
[3] Voir Guerre et contre-guerre, ouvrage rédigé avec son épouse Heidi.
[4] L'OSS (Office of Strategic Services est l'ancêtre de la CIA. C'est un peu comme si l'amiral Lacoste, ancien directeur de la DGSE, avait créé une société baptisée SDECE…
[5] Devenue ensuite ICSA puis TruSecure. http://www.trusecure.com

Bruxelles (Steele affirmant être persona non grata en France à cette époque, affirmation démentie par la suite par l'intéressé lui-même. Mais peut-on faire confiance à un espion ?).

R. Steele et l'OpenSource

- Steele : ancien de la CIA (opérations clandestines), fondateur du cabinet Open Source Solutions (OSS).
- Le renseignement coûte cher, les pays industrialisés doivent faire face à des menaces communes, baisse des budgets militaires.
- Sa solution : exploiter les sources ouvertes (Internet).

Le Credo de Steele est le suivant :
- le renseignement coûte cher ;
- l'acquisition des moyens de surveillance et d'acquisition du renseignement coûte cher ;
- le modèle soviétique (un KGB central pilotant des services de renseignements "nationaux" spécialisés) a fait ses preuves et peut être reproduit ;
- certains risques sont par nature transnationaux : terrorisme, crime organisé, prolifération NRBC[6]...
- la baisse des budgets consacrés au renseignement dans les pays industrialisés entrouvre la porte à une certaine forme de privatisation de la fonction "Renseignement" (grâce à des sociétés comme OSS[7]).

Histoire de peaufiner l'image éthique et lisse de cette entreprise (des esprits mal tournés pourraient effectivement penser que Steele compte mettre à profit - dans tous les sens du terme - ses anciennes relations au sein de la CIA pour obtenir des renseignements), Robert Steele fait sienne la doctrine d'exploitation des "sources ouvertes", à savoir toutes les informations librement disponibles mais qu'il faut savoir chercher, trouver et compiler. La fourmilière Internet plaide d'autant plus en faveur de ces officines privées de renseignement qu'elle semble, dans ces années 95-96, une insondable mine d'informations non structurée.

W. Schwartau et l'EPH

- Schwartau : journaliste - essayiste. Fait de la vulgarisation autour de la sécurité informatique.
- EPH : Electronic Pearl Harbor (thème développé depuis 1994).
- (Co)Organisateur des conférences InfoWarCon.

Winn Schwartau[8] est un journaliste et essayiste qui depuis le début des années 1990 vulgarise la sécurité informatique et ses enjeux dans le contexte de l'émergence d'un Internet ouvert au plus grand nombre.
A son actif plusieurs romans décrivant de façon apocalyptique le chaos engendré par des attaques

[6] Nucléaire Radiologique Bactériologique Chimique. On parle de prolifération nucléaire quand il s'agit de vente de matériaux ou de vecteurs destinés à la fabrication de bombes nucléaires. On parle de prolifération radiologique lorsque ces mêmes matériaux (dont notamment les déchets radioactifs) sont destinés à pollués radiologiquement et non à déclencher une réaction en chaîne.
[7] http://www.oss.net
[8] http://www.infowar.com

menées contre les infrastructures réseaux américaines. C'est ainsi qu'il met en scène dans l'un de ses ouvrages[9] un industriel japonais survivant d'Hiroshima et décidé à se venger des Etats-Unis, devenu un géant du logiciel qu'il distribue « backdooré » à souhaits dans le but de lancer une charge finale mortelle contre les ordinateurs américains (W. Schwartau devrait donc comprendre les suspicions européennes à l'égard d'un monopole comme celui de Microsoft… ☺).
En 1994, il invente le concept de « Pearl Harbor Electronique », thème qu'il ne lâchera désormais plus…

Le Credo officiel

- Internet constitue une menace réelle et sérieuse (Pearl Harbor).
- Internet est une mine d'informations/
- Il faut savoir « traiter » la menace (B-52 vs DDoS) mais aussi gérer les talents (corsaires contre pirates, nationalisme technologique).

Ce que l'on a pu entendre lors des conférences InfoWarCon...
Lors de la première édition, Schwartau et Steele dispensent à l'assistance nombreuse leur numéro bien rodé :
- Internet constitue une menace pouvant mener à un Pearl Harbor Electronique ;
- mais en même temps, c'est une formidable mine d'informations gratuites (Steele).
- il faut donc :
    - sécuriser Internet ;
    - identifier les menaces ("hackers") ;
    - … et les "traiter" (y compris par élimination physique : B-52 vs DDoS) ;
    - sans pour autant se priver des talents des hackers "bien de chez nous".
    (Corsaires contre Pirates : parmi les bons hackers de Steele : Lopht).

Schwartau ira jusqu'à remettre en cause la confiance accordée aux technologies importées. En gros : de la xénophobie technique.
A ce duo viendra se joindre en 1996 la NCSA, organisme de formation en sécurité informatique et de "labellisation" (moyennant finances) de solutions de sécurité.

La voix de l'Europe

- Juge belge : les tribunaux seront vite engorgés par les affaires de cybercriminalité.
- Professeur néerlandais : l'infoguerre ne changera rien à la face du monde, cela ne recouvre que des outils nouveaux.

Ceci dit, InfoWarCon n'était pas qu'une tribune libre donnée aux thèses américaines. Les points de vue d'acteurs européens y ont également été exprimés :
- un juge belge exprimant sa crainte de voir la cybercriminalité engorger les tribunaux européens du fait de la disparité des lois ;
- un professeur néerlandais prendre à contre-courant le discours "officiel" en disant que toutes les activités rangées sous le vocable d'IW n'étaient que des outils, certes nouveaux, et que l'infoguerre ne changerait pas la face du monde. Qu'il ne fallait pas succomber au sensationnalisme de Steele et Schwartau

[9] Pearl Harbor dot com.
http://www.getinsightnow.com/promotions/books/pearlharbor.html

Quelques suites concrètes…

- Etats-Unis : Création du Critical Infrastructure Protection Center.
- France : création de l'Ecole de Guerre Economique, émergence d'une « infoguerre » à la Française.

Dans les mois qui suivirent la seconde (et dernière) édition du chapitre européen de l'InfoWarCon, certaines des idées avancées tant dans les conférences que dans les couloirs se concrétisèrent :
- aux Etats-Unis, création d'une agence gouvernementale pour la protection des infrastructure critiques (Critical Infrastructure Protection Center) dont Internet ;
- puisqu'Internet est considéré comme infrastructure stratégique, des attaques perpétrées contre les réseaux américains peuvent justifier des réponses militaires.
- en France : dans la lignée du rapport Martre[10], projet pilote mené conjointement par la chambre de commerce et d'industrie de l'Essonne et le SGDN (Intelligence Economique en Essonne) pour sensibiliser les entreprises aux enjeux de l'intelligence économique (terme préféré à celui d'infoguerre et au vocable « guerre économique »).
- puis, en 1996, création de l'Ecole de Guerre Economique (le général Pichot-Duclos, speaker à InfoWarCon '96, ancien directeur de l'Ecole Interarmes du Renseignement et des Etudes Linguistiques, en est un des fondateurs).

En guise de conclusion….

- Convergence : la sécurité informatique peut être un outil au service de la sécurité de l'information.
- Confusion : la sécurité informatique n'est pas la sécurité de l'information.
- Infoguerre : guerre de pays riches ?

En conclusion, quelques remarques personnelles :
- Il y a une convergence entre la sécurité informatique et la sécurité de l'information dans ce sens que la première est un outil au service de la seconde ;
mais aussi confusion en ce sens que la première n'est qu'un outil au profit de la seconde.
- Il y eut aussi des conflits d'intérêts entre Schwartau, Steele et la NCSA, conflits qui, associés à une certaine désaffection du public visé par ces conférences (beaucoup de représentants d'administrations, peu d'entrepreneurs) sonnèrent le glas des éditions européennes d'InfoWarCon. Ceci dit, l'accueil des pays continentaux - ou tout du moins des participants présents - fut très mitigé voire suspicieux.
- Pour reprendre Toffler : si la guerre de l'information est la guerre de l'âge et des sociétés de l'information, seules les sociétés ayant pénétré dans ce nouvel âge sont concernées… Pour les autres, les moyens « classiques » low-tech restent extraordinairement efficaces semble t-il….
- Enfin, quand bien même serait-il possible de mettre à genoux les Etats-Unis à coup de vers informatiques, 3 Boeing détournés à l'aide d'armes blanches lancés contre des symboles forts frapperont toujours plus les esprits que Yahoo et Google inaccessibles pendant 4 heures…
- L'infoguerre semble plus une forme de guerre à usage et à destination des nations industrialisées (forte dépendance technologique oblige) qui ne peuvent (encore) se faire

[10] Intelligence économique et stratégie des entreprises. Commissariat au Plan, 1994.

ouvertement et classiquement la guerre car elles doivent rester alliées pour faire face ensemble à certaines formes bien classiques de conflits (première guerre du Golfe, mais aussi conflit en ex-Yougoslavie, dans l'Afrique des Grands Lacs, lutte contre le terrorisme, le crime organisé transnational et la prolifération NRBC …). C'est ainsi que dans la liste noire américaine des nations suspectées de développer des programmes actifs d'infoguerre (et on a vu récemment ce qu'il advient des nations suspectes…) on trouvait en 1996 la France et Israël aux côtés de la Chine. Plus récemment, la Corée du Nord a rejoint ce club…

- L'infoguerre a peut-être plus d'avenir que d'actualité (encore).
- W. Schwartau[11] a rangé en trois classes les cibles d'actions d'infoguerre : entreprises, particuliers, états (pour simplifier). L'observation tend à montrer que les entreprises ont été les premières cibles d'attaques informatiques (pas forcément liées d'ailleurs à l'infoguerre mais relevant plus de la criminalité et de la délinquance) car elles furent aussi les premières connectées à Internet, ce parfois dans des conditions de sécurité faibles (plusieurs facteurs : faible prise de conscience des risques, peu d'outils disponibles, etc.…). Les particuliers, du fait de la démocratisation des moyens de connexion permanents (dont l'ADSL) et communicants (technologies sans-fil), de la convivialité de ces outils (synonyme de mécanisme d'autoconfiguration transparent – opaques ? – pour l'utilisateur) et du renforcement constaté des obligations de traçabilité pesant sur les fournisseurs d'accès, vont par contre se retrouver en première ligne (si ce n'est déjà le cas) des attaques informatiques : que ce soit pour du vol de données (cartes bancaires) ou du vol/détournement de ressources (il y a fort à parier qu'une des prochaines tendances des vers et autres saloperies numériques sera l'installation en sous-marin de proxies permettant à des utilisateurs malicieux de surfer sur le web et d'anonymiser leurs traces), stockage de données illicites (logiciels piratés, etc…). Le risque est de voir cette phase (particuliers cibles) s'éterniser tant il sera toujours plus facile de s'attaquer aux plus faibles et ce au moindre risque qu'aux plus forts : les états, sans que cette opinion ne remette en cause le fait qu'un jour (mais quand ?) l'infoguerre aura une réalité également au niveau des nations.
- Quant aux terroristes, je pense qu'ils sont plus intérêt à utiliser Internet, que ce soit pour communiquer plus ou moins secrètement (cryptographie libre ou stéganographie) ou bien pour financer leurs activités « classiques » (trafic de données ou de logiciels/jeux piratés) qu'à le détruire, le « choc » psychologique ainsi créé étant moins frappant que, une fois encore, trois avions lancés dans des bâtiments publics…
- Enfin, l'infoguerre peut être vue comme une nouvelle forme de dissuasion du fort au fort ou entre alliés dans des cas où toute menace conventionnelle et a fortiori toute action de ce type serait désapprouvée tant par la communauté internationale (dont cependant nous avons pu récemment apprécier le poids aux yeux de certains…) que par l'opinion publique de l'attaquant. Les opérations d'infoguerre peuvent alors être envisagées comme une forme high tech de guerre secrète ou clandestine, des groupes de hackers constitués ad hoc pouvant alors servir de couverture à un gouvernement.

[11] Preuve qu'un «□hauvais□ vecteur peut véhiculer de bonnes idées…□☺