Dans le domaine militaire: la soft-war

? Les nouveaux enjeux, les nouveaux risques, les **nouveaux systèmes d'arme**. Le renseignement, la manipulation, le sabotage, les **rapports entre le fort et le faible**

? Les technologies de l'internet sont aujourd'hui au cœur du dispositif tant défensif qu'offensif des armées modernes: pour ne citer qu'un exemple le département de la défense développe la "**smart dust**", poussière intelligente dont chaque grain (en 2003 de la taille d'une pièce de monnaie mais en 2007, en cas de succès, de la taille d'un grain de sable) est capable de recueillir les informations du champ de bataille, de communiquer en réseau avec les myriades d'autres grains et de transmettre ces informations à un avion ou un satellite. A noter qu'il fonctionne sur la base d'un système d'exploitation TinyOS qui est un logiciel libre…

Notons qu'aujourd'hui déjà ***Hitachi*** *commercialise pour quelques 10 ct des "poussières intelligentes" avec emetteur récepteur radio qui ne font que 0,15mm² et qui servent au marquage des produits (technologie* ***RFID*** http://www.rfid.org

? Par ailleurs il faut bien prendre conscience qu'internet ce n'est pas seulement des tuyaux et des protocoles qui véhiculent de l'information**: c'est le système nerveux de l'économie qui transmet des instructions et pilote des processus physiques** (régulation de la distribution électrique, télépilotage d'une chaudière, télémaintenance de machines, monitoring des malades d'un hopital, …) ou ayant une influence directe sur notre économie (contrôle des flux financiers du système bancaire, cession de titres sur une bourse des valeurs, …): un hacker peut donc depuis son ordinateur prendre directement les commandes, déclencher une grave crise financière ou créer des dégats physiques pouvant causer mort d'hommes *"une attaque informatique pourrait paralyser l'infrastructure du pays en quelques heures: distribution d'eau, électricité, transport" Robin Cook, ex-ministre des affaires étrangère britannique*

En 1997 un jeune "cracker" a mis en panne la ***tour de contrôle d'un aéroport de la région de Boston*** *avec une simple liaison modem (les Echos du 9/9/92)*

Devant la conférence des ambassadeurs ***le commissaire Daniel Martin*** *de la* ***DST*** *rapportait qu'en mai 1998 un groupe de jeunes Hackers de 15 à 18 ans, the* ***Milworm****, est entré dans le réseau d'un centre de recherche atomique indien et y a volé les travaux sur les derniers essais nucléaires..*

En 1998 un garçon de 12 ans a failli ***ouvrir les vannes d'un barrage de l'Arizona*** *après être rentré par erreur dans le système qui les gérait (les Echos du 9/9/92)*

En janvier 1999 l'hebdomadaire anglais Sunday Business faisait état du ***détournement du satellite Skynet4****: les pirates qui s'étaient introduits sur le site internet demandaient 3 millions de £ pour cesser leurs agissements* www.anu.edu.au/mail-archives/link/link9903/0079.html

du 25 avril au 11 mai 2001 *le système informatique qui* ***contrôle les flux d'électricité en Californie a été "tracké"****,) au plus fort moment de la crise électrique qui touchait cet Etat et de la crise diplomatique avec la Chine (les Hackers provenaient de China Telecom mais l'enquête n'a pas pu permettre de déterminer l'origine initiale). Le Los Angeles Times, assure que les "crackeurs" n'étaient pas loin de pouvoir contrôler la distribution d'énergie dans tout l'Etat. Officiellement, ce piratage n'aurait provoqué aucun dégât sérieux. L'article du Los Angeles Times.* http://www.latimes.com/news/la-000047994jul01.story

en Aout 2003 *la* ***paralysie du Nord des Etats-Unis*** *due à une gigantesque panne d'electricité privant pendant plusieurs jours 50 millions d'américains montre l'extrême fragilité de la régulation de ces grands réseaux et le risque présenté par ce type d'attaque :* ***"Le blackout américain du mois d'août n'aurait pas eu lieu sans la présence d'un virus"*** *Mikko Hyppönen Directeur du laboratoire anti-virus F-Secure* http://solutions.journaldunet.com/itws/030910_it_hypponen.shtml

"Microsoft n'a pas démenti que la panne "générale" d'électricité intervenue récemment à New-York puisse puiser ses origines sur les conséquences d'un virus (Ver plus exatement) qui aurait suscité un trafic exceptionnel congestionnant les réseaux secondaires raccordés à Internet". Jean Philippe Bichard Netcost&Security www.netcost-security.fr

Les ***chercheurs finlandais*** *de Oulu University ont mis en évidence la fragilité actuelle des* ***réseaux électriques*** www.tekes.fi/eng/news/uutis_tiedot.asp?id=2006&paluu=default.asp *qui pouvaient* ***complètement s'effondrer*** *en cas d'attaque*

*Hogsbreath, Hacker interviewé par Le Monde(26 octobre 2000) déclarait: "****bientôt, même votre toaster sera connecté à Internet, imaginez ce qui pourra vous arriver"****!!*

SQL Slammer en 2003 nous en a donné un avant gout de ce qui peut se produire: il a réussi en quelques heures à paralyser le réseau coréen, 13.000 distributeurs de Bank of America et surtout des infrastructures critiques comme le centre américain d'appel d'urgence (911) et encore une chance que ce ver n'ait pas été programmé pour détruire les fichiers des 300.000 serveurs dont il avait pris le contrôle !

A l'occasion de la fusion des systèmes ***d'Elf et de Total****, Philippe Chalon déclarait aux Echos :"Lorsque le réseau tombe c'est notre trésorerie qui ne fonctionne plus, tout comme nos ERP, sans parler des raffineries qui ne peuvent plus charger les camions de livraison,…*

fin juillet 2001*, les* ***Experts du Kurchatov*** *Institute de Moscou détectent un* ***bug*** *dans le logiciel de base de donnée* ***SQL*** *de Microsoft. Celui-ci met en péril le système de gestion de* ***l'arsenal nucléaire Américain et Russe****: des milliers de têtes nucléaires auraient ainsi pu s'évanouir virtuellement en cas d'utilisation prolongée des logiciels de Microsoft. (voir Center for Defense Information www.cdi.org/nuclear/nukesoftware.html et* www.newsfactor.com/perl/story/12219.html*)*

? Jusqu'alors les conflits opposaient des Etats basés sur des territoires.aujourd'hui, et l'attaque du 11 septembre l'a rendu plus évident encore, on assiste à un affrontement entre les Etats d'un côté et les réseaux de l'autre (intégristes, mafias). Dans ce cadre le leader démocrate au Sénat américain, Tom Daschle qualifiait le projet de bouclier antimissile *de "la réponse la plus couteuse à la menace la plus improbable"*. Cet attentat dramatique a clairement montré que ce n'était ni le nombre, ni la technologie qui en fut l'élément clé mais la maitrise de l'information

? les NTIC fournissent de nouvelles capacités aux armées et aux systèmes de renseignement. D'autre part, conformément à la volonté d'origine elles sont peu sensibles à un attentat terroriste ou à une attaque nucléaire.(lors des dramatiques évènements de septembre, alors que les réseaux téléphoniques se sont écroulés, seules les messageries ont permis le maintien des communications)

Mais à l'inverse elles présentent de **nouvelles vulnérabilités** : des équipes peu nombreuses et ne disposant que de moyens limités, sont néanmoins susceptibles de créer de graves perturbation **tant dans le domaine militaire que civil.** 2002 a connu une chaude alerte avec l'attaque simultanée des 13 ordinateurs qui servent de "plaques tournantes" au trafic de l'Internet (serveurs d'adresse) et qui ont conduit à les paralyser pendant une heure

"aujourd'hui la France n'avance dans ce domaine que sur la pointe des pieds par rapport aux avions et aux chars" déclare aux Echos ***Paul Ivan de Saint Germain*** *ancien directeur des recherche au ministère de la défense*

A la suite des attentats du 11 septembre les USA ont encore considérablement accru leurs moyens de recherche dans ce domaine pour éviter ce qu'ils nomme un "**digital Pearl Harbour**": La **NIPC** (National Infrastructure Protection Center) a vu son budget porté à 125M$, le programme **Cybercorps Scholarship** vise à attirer les jeunes étudiants brillants frais émoulus de l'Université vers la lutte contre le cyberterrorisme, le le programme "**Cyberspace Security**" conduit par Rober Clark, conseiller auprès du Président et les 38 Milliards de $ consacrés aux problèmes de sécurité dont une large part pour la sécurité sur Internet

Une des questions de base à se poser est l'utilisation de logiciels propriétaires, dont l'expérience a montré les innombrables failles de sécurité et dont les codes couverts par le secret peuvent révéler bien des surprises

Dans cette optique l'option pour des logiciels libres mérite d'être sérieusement examinée

"Un système qui a été harcelé et testé par des milliers d'adolescentsfutés a vu ses faiblesses décelées, bien avant qu'un gouvernement étranger n'ait eu le temps de les exploiter" (David Brin, consultant auprès du gouvernement américain)

"c'est aujourd'hui une faute professionnelle grave contre la sécurité et la confidentialité que d'utiliser des produits microsoft" *déclarait* Pierre Faure DSI de Dassault et président de l'Afnet à net2003. Selon une enquête de Forrester Research, début 2003 les trois quart des responsables de la sécurité informatique des grands groupes doutent de la sécurité des logiciels de Microsoft

Un ***groupe d'experts du Pentagone****, le* ***Csis****, estime qu'****une trentaine de hackers*** *répartis sur la planète et doté d'un budget de* ***10 millions de dollars*** *pourraient causer de très sérieux dégâts à la première puissance du monde (Netsurf juin 1999)*

Les responsables de la sécurité aérienne craignent le détournement des systèmes de contrôle aérien pour prendre lepilotage du trafic avec les dangers que l'on imagine.

Bill Joy*, directeur scientifique de Sun déclarait "Modifier frauduleusement la* ***composition d'un médicament*** *fabriqué de façon automatique ou rendre nocive la* ***composition de l'air conditionné*** *géré par une seule société dans l'ensemble du quartier financier de San Francisco serait un jeu d'enfant pour un pirate motivé"*

Comme en écho en Août 1999 ***l'armée chinoise*** *annonce qu'elle est favorable au recrutement et à la formation de hackers et au même moment, le 8 août, trois sites officiels de Taiwan sont victimes d'attaques*

En septembre 1999 ***José Ramos*** *Horta leader* ***timorais*** *menace de lancer les "****Hacktivists****" à l'assaut des systèmes vitaux indonésiens*

En octobre 2000, dans le ***conflit israélo-palestinien****, l'Intifada s'est étendue aux sites Web. Celui du Hezbollah libanais a été victime d'attaques par saturation.* /www.internetactu.com/flash/flash134-24octobre.html#t2 *En mars 2001, c'est un* ***virus*** www.internetactu.com/archives/enjeux/enjeux79.html#soc4 *qui générait une fenêtre où s'inscrivait un appel en faveur du peuple palestinien.*

Au ***Cachemire*** *une quarantaine de sites indiens ont ainsi été piratés : un message pro-pakistanais s'affichait sur leurs pages d'accueil.* www.internetactu.com/archives/enjeux/enjeux67.html#ten7

En Mai 2001, après la collision entre un avion espion ***américain*** *et un chasseur* ***chinois****, les "hackers" des deux bords s'en sont donnés à coeur joie.* www.internetactu.com/flash/flash260-27avril.html#t1 *d'après* www.Chinabyte.com *, les hackers chinois "Hongker Union" (les pirates rouges), ont attaqué plus d'un millier de sites américains entre le 1er et le 9 mai, date à laquelle ils ont annoncé un "cessez-le-feu"."A la date du 9 mai, plus de 1.100 sites chinois avaient été attaqués" (voir le communiqué du FBI* www.nipc.gov/warnings/advisories/2001/01-009.htm*) Selon le groupe "Hongker Union" il convient à l'avenir de moins dépendre des logiciels américains afin de réduire leur vulnérabilité*

Toujours en mai 2001, deux ***virus*** *"anarcho-pacifiques"* www.internetactu.com/archives/enjeux/enjeux88.html#soc5 *sont apparus sur le réseau. L'un, "Mawanella", veut, comme son "cousin" palestinien", sensibiliser les internautes au sort des musulmans au* ***Sri Lanka****. L'autre, baptisé "LoveLet-CL", contient dans son code un texte critique à l'encontre de la politique américaine et du système d'écoute Echelon (lire en Société).*

En juin 2001 un exercice d'attaque cybernétique s'est déroulé en ***Suisse***

L'organisation ***Al-Qu'ida*** *dispose du réseauJOL (Jihad On Line) utilisant la* ***Stéganographie*** *(méthode de cryptage utilisant les pixels des images pour dissimuler les images) les Echos sept 2001* voir page **Erreur! Signet non défini.**

? mais sur un plan plus prosaïque internet permettrait une **fabrication beaucoup plus rapide et plus souple des armements** (industrialisation et production) dans la logique mise en œuvre dans l'industrie automobile: cela permettrait sans doute de **focaliser davantage les budget sur la recherche**, la fabrication de **prototypes** et **l'organisation** d'une production plus flexible et plus réactive. Là encore internet devrait permettre de **limiter les stocks** de matériel inemployés et rapidement obsolètes notamment au niveau de leur électronique

? autre domaine à explorer: celui de la gestion du parc de matériel et de sa **maintenance**: un récent rapport du Simmad qui stigmatise un taux d'indisponibilité de 40% pour le matériel aéronautique. On peut penser qu'un usage efficace de l'internet pourrait permettre de sérieux progrès dans ce domaine