Le Commandant HORVATH Gàbor

Armée de Terre, Défense Nationale de Hongrie

CID 5° Promotion, groupe A 1

Etude du cycle initiation à la stratégie

LA GUERRE INFORMATIQUE :

FUTURE ARME DE DESTRUCTION MASSIVE

DE PAYS PAUVRES DU XXIe SIECLE

1998

SOMMAIRE

INTRODUCTION

Un jeune israélien, âgé de 18 ans, vient d'être arrêté par les autorités américaines. L'explication : ce jeune, surnommé " l'Analyste " avait réussi avec des camarades, à pénétrer profondément dans les réseaux informatiques les plus secrets du Pentagone. Il était ainsi le premier emmené sous haute surveillance à Washington pour ce motif. En effet, " l'Analyste "

n’était qu’un, mais peut-être le plus dangereux des plusieurs centaines de milliers d’intrus qui essayent de briser chaque année les codes d’accès aux systèmes informatiques du sanctuaire de la défense américaine. Mais personne n’est aujourd’hui en mesure d’évaluer le nombre exact d’intrusions réussies.

Les Américains ont ressenti le danger. Dans une société hautement informatisée les dégâts d’éventuelles attaques sur les réseaux informatiques sont imprévisibles. Depuis les grands systèmes du transport et distribution d’énergie (réseaux électroniques, pipelines), les systèmes bureautiques des institutions financières jusqu’aux réseaux informatiques de circulation aérienne, toutes les activités sont désormais devenues sous-jacentes et complètement dépendantes de systèmes informatiques. Tout accès frauduleux peut donc leur causer des dégâts matériels importants, et probablement occasionner des pertes humaines.

Les systèmes militaires hautement spécialisés et relativement bien défendus sont à priori moins vulnérables face à ce nouveau type de menace. Par contre, les effets peuvent être beaucoup plus dangereux pour les grands systèmes civils qui seraient attaqués. L’arme informatique est donc sur le point de devenir une arme stratégique par excellence, et probablement une des plus dangereuses du siècle à venir.

Ce type d’arme menace les états profondément informatisés. Quels peuvent être ceux qui pourraient utiliser cette arme sans craindre de dégâts informatiques, découlant de l’interconnexion de plus en plus étendue entre systèmes? S’il s’agit d’un agresseur non-étatique, l’éventail est particulièrement large - les individus irresponsables, terroristes, acteurs de la vie économique, ... la liste pourrait être longue. S’agissant d’un agresseur étatique, il est probable que ce soit les nations les moins développées qui puissent choisir à l’avenir cette forme nouvelle d’armes.

C’est pourquoi nous pouvons constater que l’arme informatique pourrait devenir l’arme des " pauvres " du prochain siècle. Etant donné l’importance des éventuels dégâts, elle constituerait une véritable arme de destruction massive, ce qui pourrait bouleverser une société en quelques instants.

Pour analyser cette nouvelle menace nous essayerons d’abord de définir ce que peut être la guerre informatique, puis nous essaierons d’identifier quels pourraient être les objectifs visés par cette arme informatique. Ensuite nous tenterons de décrire un scénario d’agression informatique pour pouvoir en dégager quelques enseignements essentiels. Nous ne serons pas en mesure de proposer des solutions satisfaisantes pour s’y opposer, mais nous suggérerons des pistes de réflexion pour faire face à cette problématique du futur proche.

I - GUERRE INFORMATIQUE : QUELQUES DEFINITIONS

11 - " Guerre d’information " et " guerre informatique "

La définition de la guerre informatique n’est pas aisée. Dans la presse militaire, les auteurs confondent régulièrement " guerre d’information " et " guerre informatique ". Selon les définitions anglo-saxonne et française la guerre d’information comprend tous les domaines dans lesquels on conçoit, traite et exploite des informations, couvrant des domaines aussi divers que les médias ou les systèmes informatiques.

Sous cette approche, la guerre informatique fait partie de la guerre d’information. Néanmoins, compte tenu de l’existence désormais commune et banale de systèmes informatiques dans tous les secteurs d’activités de la société et de leurs effets sur la vie quotidienne, la guerre informatique mériterait d’être traitée comme une catégorie à part. Si l’on veut bien suivre l’évolution de la réflexion militaire, il est très probable qu’elle devienne une nouvelle forme de menace dans le proche avenir.

12 - " Guerre électronique " et " guerre informatique "

Le seconde approche estime que la guerre informatique est l’extension logique de la guerre électronique. Partant du fait que les vecteurs de " l’arme informatique " sont partie intégrante des moyens de guerre électronique, et arguant que la guerre informatique n’a d’autres buts tactiques ou opératifs, les partisans de cette catégorisation aboutissent logiquement à ce que la " guerre informatique " participe pleinement à la suprématie du spectre électronique (spectrum supremacy).

Les procédures et les modes d’action (brouillage, déception, écoute etc.) utilisés dans le spectre électronique s’appliquent de manière similaire dans le spectre informatique. La grande différence entre les deux est que, dans le cas de la guerre électronique, la performance des vecteurs (émetteurs, brouilleurs, capteurs etc.) prédomine. Dans la guerre informatique ce ne sont que des outils de base : l’action elle-même se fait par des cerveaux brillants et des logiciels intelligents. Pour éclairer un peu la différence telle que nous la percevons, si la guerre électronique est une sorte de Formule 1 où la technologie prévaut, la guerre informatique serait un échiquier évolutif où l’enjeu s’avère beaucoup plus important.

13 - Une nouvelle composante de la guerre : la guerre informatique

Faute de définitions claires, nous essayons d'introduire, par convention, quelques définitions de travail qui doivent nous permettre de poser des hypothèses de travail.

Dans notre analyse, la notion " guerre informatique " désigne l'ensemble des actions menées par des moyens militaires ou civils de la technologie informatique d'un Etat ou d'une alliance, visant à produire des dégâts non-matériels, matériels et humains en vue d'obtenir un effet stratégique. L'effet stratégique dans ce contexte est l'objectif fixé par un Etat ou une alliance d'Etats. Les considérations de ce mémoire ne s'appliquent qu'à des acteurs étatiques.

S'il est clair que la majorité des actions frauduleuses pouvant exister aujourd'hui dans l'espace cybernétique serait le fait de protagonistes non-étatiques, il faut bien admettre que ni leur but, ni leurs modes d'emploi ne s'inscrivent dans un contexte stratégique, cadre de notre analyse. Par conséquent les acteurs non-étatiques, comme les individus, groupes d'individus, organisations intra-étatiques ou économiques cherchant à employer l'arme informatique pour des motifs criminels sont strictement écartés de ce qui suit.

La notion " arme informatique " couvre l'ensemble des logiciels hautement perfectionnés et spécialisés qui servent à manipuler, corrompre ou détruire le contenu des banques de données ou modifier, brouiller ou bloquer le fonctionnement du système informatique visé et éventuellement les moyens physiques spécialisés de leur introduction. Les logiciels en question ne peuvent pas se réduire à des virus informatiques. En effet, les " virus " peuvent être introduit illégalement dans des systèmes d'arme incluant des logiciels. Cependant l'éventail de l'arme informatique est beaucoup plus étendu que les seuls virus informatiques. Ils incluent également des logiciels de débordement, les logiciels de pénétration de défense informatique, les logiciels multilangues de déchiffrement, les logiciels de simulation ou d'émulation d'un environnement informatique ... et la liste est longue. Leurs caractéristiques communes sont la furtivité et l'évolutivité. L'introduction de ces logiciels s'effectue généralement par de simples moyens informatiques du commerce. Cela peut être aussi des moyens spécialisés de télécommunication des données, y compris les satellites de télécommunication.

La guerre informatique représente donc une nouvelle composante de la guerre d'information et de la guerre électronique. D'une part par son caractère purement stratégique, d'autre part par le rôle dominant de l'intelligence humaine et artificielle sur la technologie.

Après avoir essayé de définir quelques éléments de la terminologie générale de la guerre informatique, nous allons consacrer la partie suivante à " l'environnement stratégique " de cette guerre, en énumérant les problèmes liés à l'utilisation de l'arme informatique.

II - ENVIRONNEMENT STRATEGIQUE

21 - Les problèmes de ciblage : quels objectifs ?

Une attaque stratégique sur des systèmes informatiques - altération ou annulation des banques de données, modification des procédures dirigées par des ordinateurs - entraîne immanquablement le bouleversement de l'environnement informatique du système attaqué. Dans le cas d'un système extrêmement étendu et complexe, comme les grands systèmes financiers, l'effet de l'agression peut être ressenti dans un vaste rayon. Il est donc nécessaire de s'interroger sur la problématique du ciblage d'une agression informatisée.

Etant donné que tous les Etats utilisent un ou plusieurs systèmes de dimension mondiale, on ne peut plus exclure l'éventualité d'une agression sur l'un de ces systèmes mondiaux. Les dégâts causés dans ce cas ne seraient pas supportables même pour l'agresseur. Cependant on ne peut écarter, même si sa probabilité d'occurrence est très faible, l'éventualité d'attaque étatique qui aurait pour objectif de détruire un système informatique aux dimensions mondiales, par exemple pour un système informatique à vocation financière de la part d'un pays excessivement endetté.

Les cibles les plus probables de telles attaques sont les systèmes purement nationaux ou régionaux. On verra ici d'un effet positif de la mondialisation : plus les systèmes informatiques s'uniformisent, plus ils seront protégés grâce à leur intégration de plus en plus complète. Mais il ne faut pas perdre de vue : le danger est alors moindre pour les seuls acteurs étatiques ; mais non de la part des individus, des groupes frauduleux ou terroristes.

On peut donc conclure que les attaques par outils informatiques ne serviraient qu'aux individus, groupes ou Etats marginalisés. S'il s'agit d'Etats, ce seraient des Etats dont les valeurs -pour une raison ou l'autre - seraient tellement différentes de celles de la plupart de la communauté internationale, qu'ils n'oseraient risquer de déchirer totalement le tissu traditionnel des rapports entre Etats. De ce point de vue, en raison de la difficulté du ciblage et de l'incertitude sur des conséquences, la menace éventuelle de l'arme informatique présente beaucoup d'analogies avec la menace de l'arme nucléaire.

-

Systèmes		Vulnérabilité	Menace	Probabilité d'une attaque réussie
Systèmes mondiaux		Grande	Faible	Moyen
Systèmes		Assez grande	Moyen	Moyen

régionaux				
Systèmes nationaux		Moyen	Grande	Grande
Systèmes militaires	- 	Faible	Très grande	Faible

Tableau N° 1 : Classement des réseaux informatiques en fonction de leur vulnérabilité contre une attaque informatisée

22 - Dégâts matériels et virtuels

-

Quelles seraient les dégâts susceptibles de causer, par altération ou annulation des banques de données ou introduction d'un virus informatique, une modification des procédures susceptible de mutiler un grand système informatique ?

Tout d'abord et en premier lieu les dégâts seraient de l'ordre non-matériels ou virtuels. La perte ou la modification des données ralentirait certaines procédures. La fraude des données financières sauvegardées sous forme magnétique ou électro-optique causeraient des perturbations considérables mais seulement pour une durée relativement courte, estimable à quelques jours, une semaine tout au plus. Les dégâts dans ce contexte s'arrêteraient aux limites des institutions financières.

Les dégâts matériels commenceraient par la destruction ou modification des données ou des logiciels de pilotage de certains systèmes de télécommunication ou d'énergie. En ce qui concerne les dégâts sur des systèmes de télécommunication, le ravage s'élargirait très vite au niveau mondial, et donc causerait des conflits internationaux. Les systèmes informatiques touchés dans le secteur énergétique, semi-nationalisé partout dans le monde, transmettraient les malfaçons aux autres secteurs productifs de l'économie. Il suffit pour cela d'imaginer quelle peut être la situation où tous les réfrigérateurs d'une ville s'arrêtent pour une journée faute d'électricité !

Les pertes en vies humaines, certes, seraient moins probables, mais cependant possibles. Imaginons pour cela une situation où le système d'atterrissage d'un grand aéroport fasse défaut pendant une durée de quelques secondes et provoque la mort de quelques centaines d'innocents voyageurs.

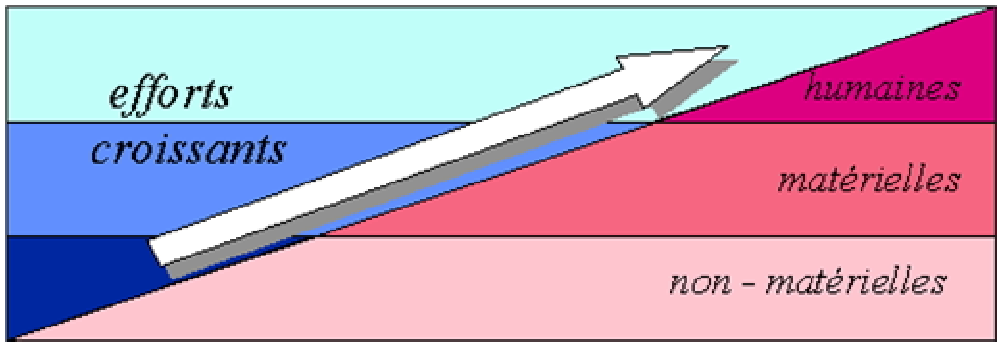

Figure No. 1 : Le rapport probable entre la nature des pertes et

les efforts nécessaires (complexité de " l'arme informatique ") pour les produire.

Par conséquent, il est difficile de prévoir, mais également d'estimer les dégâts d'une défaillance délibérée de tel ou tel système informatique. En conclusion partielle, l'incertitude des dégâts potentiels est un facteur qui doit nous amener à une conscience plus aiguë de la sécurité de nos systèmes.

23 - Une nouvelle forme de destruction mutuelle assurée

La problématique du ciblage et des dégâts nous permettent d'imaginer une situation un peu similaire à celle de la Guerre Froide. Les dégâts potentiels, imprévisibles, pousseraient les pays les plus développés (et les plus informatisés) à maintenir un équilibre dans le domaine de la guerre informatique. Il s'agirait d'une nouvelle forme de la destruction mutuelle assurée (Mutually Assured Destruction), dans laquelle les protagonistes s'abstiennent mutuellement de l'utilisation de l'arme informatique.

La plupart des pays en voie de développement probablement suivront cet armistice établi par les grands, d'une part parce qu'ils seront dépendants des grands systèmes informatiques qui leur restent leurs fournisseurs de services et de ressources, d'autre part parce que leurs systèmes, assurément moins sophistiqués, seront beaucoup plus vulnérables contre ce type d'attaque.

Ce fait nous montre bien que l'usage de cette arme pourrait se faire par les Etats qui ne trouveraient pas leur place dans le concert mondial des Etats. Au chantage nucléaire, s'ajoute donc le chantage informatique. Et il n'est pas sûr que les deux puissent se combiner. Certains auteurs américains même parlent d'un nouveau défi stratégique, en prétendant qu'une attaque informatique significative toucherait les intérêts vitaux de l'Etat et déclencherait ainsi automatiquement la riposte nucléaire.

III - SCENARIO D'UNE ATTAQUE INFORMATIQUE

31 - Caractéristiques d'une attaque informatique

Les auteurs américains ont identifié un certain nombre de caractéristiques de la guerre informatique. Leur analyse souligne qu'une attaque informatisée présente un très grand nombre d'incertitudes. Tout d'abord, l'attaque ne dure que quelques secondes. Durant une période assez longue - et même pendant longtemps - l'attaqué ne réalise pas qu'il a été agressé, étant donné que les effets de l'attaque se présentent soit sous une forme de défaillance du système, soit par des arrêts graduels. Le système informatique altéré propage ses dégâts sur les systèmes conjoints, qui peuvent être géographiquement très éloignés. La reprise de la gestion du système ne serait possible qu'après avoir délimité la zone infectée, identifié la nature de l'attaque et mis en oeuvre les procédures de réinitialisation des systèmes à partir de sauvegardes préalablement enregistrées.

Dans le cas d'une attaque de la part d'un acteur étatique, un certain nombre de caractéristiques pourrait être mieux définies. Si l'on admet qu'un Etat hostile puisse se procurer une arme informatique en vue d'obtenir un effet stratégique qui serve ses intérêts, une attaque de sa part revêtirait une forme plus " sophistiquée " que celle, par exemple, d'un individu déséquilibré ou d'un groupe terroriste. La destruction comme finalité ne s'inscrit pas comme l'objectif principal d'un Etat (au moins depuis Ghengis Khan). Par conséquent une attaque informatique sur les réseaux stratégiques a plutôt vocation à s'exercer comme un chantage transnational, ou bien pourrait constituer une action préliminaire ou parallèle à des actions de combat. Mais l'incertitude serait toujours présente concernant l'objectif final de l'attaquant.

32 - La défense

Une attaque informatique déclenche automatiquement des mesures de défense et de contre-attaque. Pendant qu'une partie des " forces informatiques " de l'attaqué essayerait de stopper l'infection, l'autre partie déclencherait la contre-attaque, qui par nature, aurait les mêmes problèmes de ciblage et d'estimation des dégâts causés que l'attaque initiale. Tout cela se déroule en quelques minutes, voire en quelques secondes. La durée d'une telle bataille informatique serait tellement courte que le grand public l'ignorait probablement complètement et pendant relativement longtemps. Sauf en cas de pertes humaines indirectes, les médias ne seraient pas avertis. De ce point de vue il n'est pas exclu que les premières batailles informatiques aient déjà existé et se soient déroulées sans que personne ne s'en soit aperçu.

Une question se pose alors inévitablement : comment prévoir une telle attaque et comment se défendre contre elle? Il est difficile à répondre à ces questions. Une forme de la défense et apparemment la seule que les Américains ont conçu outre la création de l'Information Warfare Center consiste à répertorier l'infrastructure informatique nécessaire minimale (minimum essential information infrastructure - MEII). La MEII représente la configuration minimale des systèmes informatiques, les procédures, les instruments juridiques et de taxation des Etats-Unis qui sont nécessaires pour assurer une bonne continuité du fonctionnement de l'Etat, même en cas d'attaque informatique sophistiquée.

Mais cette solution de préservation de moyens informatiques minimums ne représente qu'une forme de " quarantaine " pour les systèmes essentiels de l'Etat. Les questions de la prédiction de la défense active, voire la possibilité d'une contre-attaque organisée et la problématique de la décontamination et du rétablissement du fonctionnement des systèmes endommagés ne sont pas encore résolus.

33 - Description du champ de bataille après une guerre informatique

Que verrait-on après une guerre informatique ? Selon la nature de l'attaque et la position de l'observateur on pourrait assister à des défaillances répétitives de certains systèmes informatisés. On peut envisager par exemple les télécommunications ou le positionnement global (GPS) fonctionnellement détruits, des problèmes graves sur Internet, suite à la disparition de certains noeuds et de certains grands fournisseurs de données.

Les effets secondaires pourraient constituer une sorte de tremblement de terre informatique. Les rapports habituels d'échange mondial produiraient des phénomènes difficilement prévisibles. Les prix des ressources énergétiques par exemple alterneraient de façon erratique pendant un certain temps. Le monde financier subirait un crack boursier suite à " l'effet de cascade " de défaillance des systèmes informatisés de la finance et à la perte de confiance des acteurs financiers. Ces effets pourraient faire plusieurs fois le tour de la Terre, un peu comme les raz de marée déclenchés par un tremblement de terre sous-marin.

Malheureusement ce serait certainement les Etats de taille et de développement moyens, équipés des systèmes informatisés, qui subiraient probablement le plus de dégâts. Ne disposant pas de moyens de contrôle ou d'analyse de défaillance des systèmes ils retomberaient tout à coup à l'ère de Guttenberg en perdant très rapidement leurs outils informatisés.

CONCLUSION

Heureusement tous les éléments de la vision effrayante que nous venons de décrire ne sont pas encore réunis à l'échelle mondiale. La vie humaine n'est pas encore devenue totalement dépendante des systèmes informatisés. Mais elle la deviendra de plus en plus, car on ne peut pas arrêter l'évolution du monde.

Veiller à la sécurité des citoyens et des biens de la nation est la responsabilité des armées, responsabilité qu'elles partagent avec les autres institutions de l'Etat. La guerre informatique vise à nuire aux intérêts vitaux d'un Etat moderne. Par conséquent les armées devront être capables de faire face à une telle menace aussi. Outre l'autodéfense de leurs propres systèmes informatiques, elles auront pour mission d'assurer la sécurité du fonctionnement des grands systèmes informatisés de l'Etat.

Exagérer la menace de la guerre informatique serait une erreur ; mais l'ignorer constituerait une plus grande. L'âge postindustriel, nommé l'Age de l'Information nous oblige, nous les militaires à y réfléchir.

OUVRAGES CONSULTES

Gérard Delmaire : Systèmes d'information mondiaux et renseignement par satellites

Défense Nationale

Renaud Bellais : Technologie militaire et système d'information de défense

Défense Nationale

Roger C. Molander, Andrew S. Riddile, Peter A. Wilson : Strategic Information Warfare : A New Face of War

Richard J. Harknett : Information Warfare and Deterrence

Robert J. Bunker : Advanced Battlespace and Cybermaneuver Concepts : Implications for Force XXI

Parameters, vol. XXVI, No. 3, Autumn 1996

Timothy L. Thomas : Deterring Information Warfare : A New Strategic Challenge

Parameters, vol. XXVI, No. 4, Winter 1996-97

VA Arthur K. Cebrowski - John J. Garska : Network-Centric Warfare, Its Origin and Future

Proceedings, January 1998

Lt.Gen. L.D. Holder - COL Edward J. Fitzgerald : Winning in the Information Age

Military Review, July-August 1997

Ens. Thomas G. Mahnken : War in the Information Age

Joint Forces Quarterly, Winter 1995-96

Lt.Comm. Randall G. Bowdish, USN : The Revolution in Military Affairs : The Sixth Generation

Military Review, November-December 1995

LCL Dennis M. Murphy : Information Operations on the Nontraditional Battlefield

Military Review, November-December 1996

COL Michael D. Starry - LCL Charles W. Arneson : FM 100-6 : Information Operations

Military Review, November-December 1996

Sqn Ldr Peter Emmett : Information Mania - A New Manifestation of Gulf War Syndrome ?

George J. Stein : Information Warfare

Air Power (Magazine de la RAF)

Mensuels, hebdomadaires régulièrement consultés : Revue de presse securité des systèmes d'information (Centre d'électronique de l'armement, CASSIC); TTU ; The Worldwide Weekly Defence News, ainsi que des nombreuses magazines d'informatique.