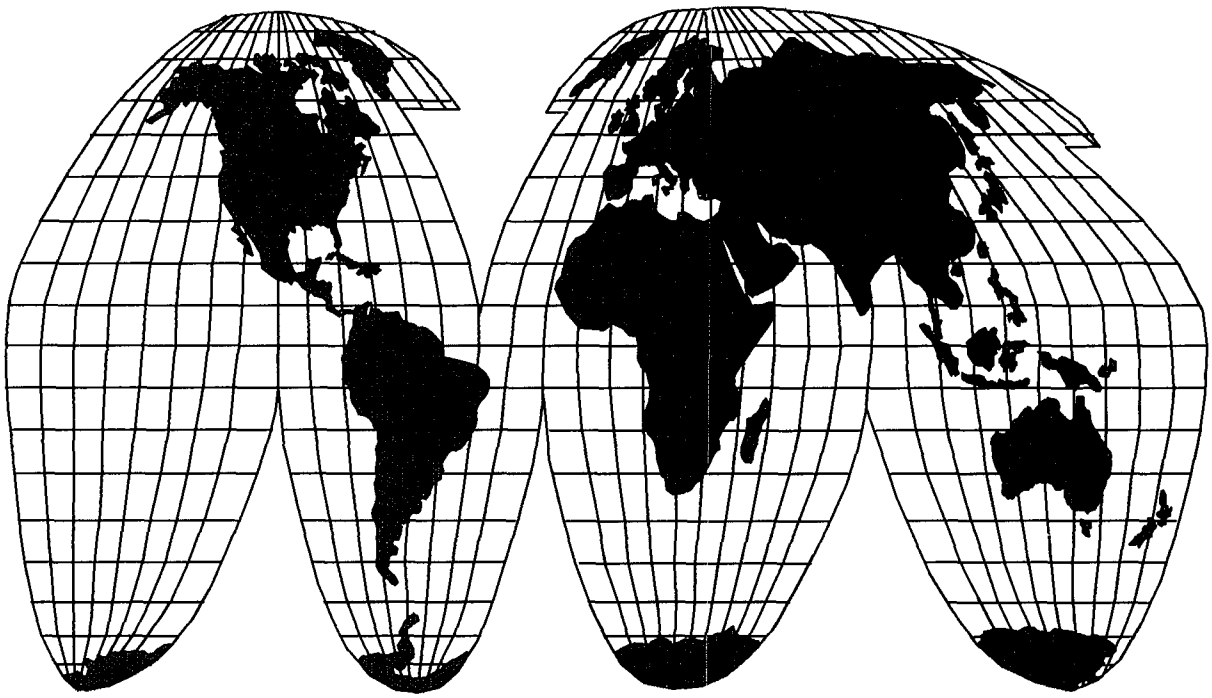
1998 - 164

MEMOIRE DE STRATEGIE



CYBERSTRATEGIE:
ELEMENTS DE REFLEXION

5ème Promotion 1997 / 1998
Division C / Groupe C 1
Mars 1998

Chef de Bataillon
Pierre-Yves HENRY

1. INTRODUCTION 2

2. TECHNIQUES ET TACTIQUES DE LA GUERRE INFORMATIQUE 4

2.1 HACKING 4
2.1.1 DEFINITION 4
2.1.2 QUELQUES CAS 4
2.2 PHREAKING 5
2.3 VIRUS, VERS ET CHEVAUX DE TROIE 6
2.3.1 DEFINITIONS 6
2.3.2 EXEMPLES 7
2.4 FACTEUR HUMAIN ET HUMAN ENGINEERING 7
2.5 CONCLUSION PARTIELLE 8

3. GUERRE INFORMATIQUE 9

3.1 LE TERRAIN 9
3.2 LES ACTIONS POSSIBLES 9
3.2.1 CLASSE 1: GUERRE INFORMATIQUE CONTRE LES PERSONNES 10
3.2.2 CLASSE 2: GUERRE INFORMATIQUE CONTRE LES ENTREPRISES 10
3.2.3 CLASSE 3 : GUERRE INFORMATIQUE GLOBALE 10
3.3 SCENARIO POSSIBLE 11

4. CONCLUSION 13

BIBLIOGRAPHIE 14

CYBERSTRATEGIE

1. INTRODUCTION

La guerre de l'information ou *information warfare* est le nouveau sujet de prédilection de nombreuses armées dans le monde entier, à commencer par les Etats-Unis. Or, si l'on en croit le cours de M. COUTAU-BEGARIE, il est constant dans l'Histoire que les civilisations dominantes ont toujours défini et développé les stratégies de leur temps et de l'avenir immédiat. C'est pourquoi il serait déraisonnable de ne pas nous intéresser de près au concept de la guerre de l'information et à la stratégie qui s'y rapporte.

Il s'agit d'un domaine très large, regroupant plusieurs concepts tels que la guerre électronique, la guerre psychologique, la bataille du renseignement et surtout, à notre époque, la guerre informatique qui de nos jours fédère et commande les autres concepts comme nous le verrons. De la guerre de l'information, le Dr John ALGER propose la définition suivante :

La guerre de l'information est l'ensemble des actions entreprises dans le but d'obtenir la supériorité dans la maîtrise de l'information en affectant les informations, le traitement de l'information et les systèmes d'information de l'ennemi, tout en protégeant ses propres informations, traitement de l'information et systèmes d'information.

Si l'on prend en compte le fait que le mot français *informatique* est obtenu par contraction de *information* et de *automatique*, on constate que l'aspect innovant du concept américain de *information warfare* repose en fait sur ce que nous pourrions traduire en Français par *guerre informatique.*

Notre société est de plus en plus dépendante de l'informatique. Où que vous soyez, quoi que vous fassiez, vous risquez d'avoir affaire, directement ou indirectement, à un ordinateur. Lorsque vous payez avec votre carte de crédit, réservez une place dans un avion, placez de l'argent sur votre compte en banque et même lorsque vous passez un simple coup de téléphone, c'est un ordinateur qui, in fine, s'occupe de vous.

Régulièrement, la presse se fait l'écho de pirates informatiques qui se sont introduits dans tel ou tel système, ont volé des centaines de numéros de cartes de crédit, peuvent consulter et modifier le contenu de comptes bancaires ou se promener dans les ordinateurs du Pentagone. On nous apprend aussi que des virus informatiques circulent d'ordinateurs en ordinateurs en gênant leur fonctionnement, voire en attendant l'instant où ils vont détruire le contenu des disques durs.

Que se passerait-il, si une organisation ou un gouvernement réunissait les compétences de ces pirates isolés pour mener une action de grande envergure contre un Etat ? Certains auteurs tels que Winn Schwartau dans son roman *Terminal Compromise* ont exploité cette hypothèse, et selon l'aveu de notre maître de stratégie, les auteurs de science-fiction se trompent moins souvent que les futurologues et autres stratégistes.

Après avoir passé en revue les techniques et les tactiques utilisées par les pirates informatiques isolés, nous nous efforcerons de montrer quelles pourraient être les formes prises par la guerre informatique, avant d'en proposer un scénario-type. Nous conclurons pour montrer qu'il existe bien une stratégie propre à la guerre

dans le cyberespace, ou à tout le moins qu'une stratégie informatique devra compléter toute autre forme de pensée stratégique globale.

2. TECHNIQUES ET TACTIQUES DE LA GUERRE INFORMATIQUE

2.1 Hacking

2.1.1 Définition

Le *hacking* est l'activité du *hacker.* Les sens donnés au terme *hacker* sont très variés. A la base, un *hacker* est une personne qui prend plaisir à explorer en détail un système programmable et qui cherche à étendre au maximum ses connaissances dans ce domaine. Actuellement le terme est généralement employé pour désigner des personnes s'introduisant illégalement dans des systèmes informatiques. Dans ce document, j'utiliserai le terme *hacker* dans ce dernier sens.

Le but de ce chapitre sur le *hacking* est de citer quelques cas pour montrer l'incroyable vulnérabilité des systèmes informatiques. Une étude effectuée en 1992 par USA Research inc. a montré que le nombre d'intrusions dans des systèmes informatiques aux Etats-Unis est passé de 339.000 en 1989 à 684.000 en 1991. Au cours de l'année 1995, on a dénombré 250.000 intrusions sur les seuls réseaux militaires américains. Ces chiffres sont à prendre avec prudence, car très peu de cas sont effectivement rapportés aux autorités. Le NCCS estime que moins de 10 % des cas d'intrusions sont signalés, les entreprises victimes de *hackers* n'ayant pas la moindre envie de se faire une mauvaise publicité, en avouant leurs faiblesses.

2.1.2 Quelques cas

2.1.2.1 Programme de protection des témoins

Dans les années 80, un *hacker* nommé Michael Sinergy pénétra dans le système informatique de l'agence de crédit nationale (TRW), qui détient des informations financières sur près de 80 millions d'Américains, dans le but d'aller consulter le fichier du président Ronald Reagan. Il découvrit le fichier qu'il cherchait et constata que 63 autres personnes avaient consulté la même information le même jour. Il remarqua un groupe de 700 personnes qui semblaient détenir la même carte de crédit et dont l'historique de leur compte était étrange. Ils semblaient ne pas avoir de passé. Il réalisa qu'il devait très certainement être en train de consulter l'historique des crédits, ainsi que les noms et adresses de gens qui travaillaient dans le cadre du programme gouvernemental de protection des témoins. En bon citoyen, il s'empressa de signaler au FBI cette faille logique qui permettait d'identifier des personnes à qui on était précisément sensé garantir un anonymat total.

2.1.2.2 Détournement de fonds

En 1988, sept criminels ont effectué un détournement de fonds à la First National Bank de Chicago. Ils ont transféré 70 millions de dollars appartenant à 3 grosses compagnies sur un compte dans une banque de New-York, puis, de là, dans deux banques à Vienne. Les transferts ont été effectués par intervention via messagerie électronique sur les fichiers centraux. La banque débitée a appelé ses

clients pour demander confirmation du transfert, mais les appels étaient détournés vers la résidence d'un des criminels, après que celui-ci soit intervenu sur le central téléphonique informatisé. Les sociétés volées se sont vite rendu compte de l'affaire et une enquête a été ouverte. Grâce aux enregistrements des appels de confirmations, les enquêteurs ont pu appréhender *in extremis* les sept criminels avant qu'ils ne prennent la fuite.

2.1.2.3 Argent de poche

Fry Guy est un *hacker* de 17 ans au moment des faits, habitant dans l'Indiana (USA). En 1989, il est passé maître dans l'art de commander aux centraux téléphoniques informatisés de la compagnie locale de téléphone et il a trouvé un moyen de gagner un peu d'argent de poche facilement. Il contacte des commerçants en se faisant passer pour un employé d'une société de cartes de crédit. Après suffisamment d'essais il en trouve un assez naïf et parvient à lui faire donner son numéro de client et son mot de passe. Muni de ces informations, *Fry* Guy se connecte sur l'ordinateur de la compagnie de crédit pour trouver la liste des clients du commerçant. Il choisi un client relativement aisé, relève son numéro de téléphone et son numéro de carte de crédit.

Il détourne la ligne téléphonique de sa victime vers une cabine téléphonique dans la petite ville de Paducah, et la ligne de cette cabine vers son propre téléphone. Il appelle la banque de sa victime pour faire un virement dans leur agence de Paducah, en débitant la carte dont il détient le numéro complet. La banque rappelle chez la victime pour demander la confirmation du transfert et c'est lui qui répond. Il ne lui reste plus qu'à rétablir les lignes téléphoniques et à aller récupérer l'argent. Cet exemple se situe à la limite du *hacking* et du *phreaking.*

2.2 Phreaking

Le *phreaking,* est l'action de pirater les réseaux téléphoniques. Cette activité est liée au piratage informatique parce que les *hackers* devaient passer de longues heures à essayer de se connecter par modem sur les ordinateurs qu'ils avaient pris pour cible, et que cela aurait fini par leur coûter cher. C'est pour cela que la plupart des *hackers* sont aussi des *phreakers.* De plus, comme les centraux téléphoniques modernes sont des ordinateurs, le piratage du téléphone se rapproche beaucoup du piratage d'un ordinateur " classique ".
Le premier cas de *phreaking* recensé remonte à 1961 et le premier article sur ce sujet fut écrit en 1971 dans le magazine *Esquire. A* cette époque le *phreaking* était une activité essentiellement pratiquée par des aveugles qui utilisaient le téléphone comme moyen de rompre leur isolement. Ils utilisaient pour se parler des lignes de test utilisées pour la maintenance du système. Ces lignes de test sont caractérisées par le fait que chaque extrémité possède un numéro de téléphone qui lui est assigné et qu'il suffit à deux personnes se mettant d'accord à l'avance sur quelle ligne utiliser, d'appeler chacun une des extrémités pour se trouver en contact, gratuitement.

Petit à petit, les techniques se sont perfectionnées et il devint possible aux pirates d'utiliser toutes les fonctionnalités du réseau, grâce à la *"blue box",* un boîtier

capable de générer des tonalités de commandes, permettant aux *phreakers* de commander le réseau au même titre qu'un employé de la compagnie de téléphone.

Il est évident que les techniques du *phreaking,* employées de manière organisée et sur une grande échelle, sont de nature à permettre la destruction ou au moins la neutralisation ou le détournement de l'ensemble d'un réseau national ou régional de télécommunications.

2.3 Virus, vers et chevaux de Troie

2.3.1 Définitions

Un virus est un programme capable de se reproduire dans un ordinateur, pouvant infecter d'autres programmes et ainsi se transmettre d'un ordinateur à un autre, si l'on copie le programme infecté sur un ordinateur sain. S'ils ne faisaient que se reproduire, les virus n'inquiéteraient personne. Le problème réside en ce qu'ils peuvent être programmés pour être nuisibles, par exemple en effaçant les données de la machine sur laquelle ils s'exécuteront à une date précise ou lors de la détection d'un événement donné. Il existe un grand nombre d'autres actions possibles pour des virus, et nous laisserons le soin au lecteur de les imaginer.

Un ver diffère du virus au sens qu'il se transmet de lui-même d'un ordinateur à l'autre au travers d'un réseau, sans qu 'il soit nécessaire de copier ou d'exécuter un fichier. L'exemple le plus connu et le plus dévastateur est sans doute le ver d'ARPANET, qui paralysa ce réseau en 1988. Cet exemple sera détaillé plus loin.

Un cheval de Troie est un programme qui n'est pas seulement ce qu'il a l'air d'être. Par exemple, vous recevez par la poste une publicité, sous la forme d'une disquette contenant la version de démonstration d'un traitement de texte. Si en plus de faire office de traitement de texte, son programmeur a décidé de lui faire rechercher la liste de toutes les applications contenue dans votre ordinateur et d'effacer les fichiers des logiciels de traitement de texte concurrents, il s'agit d'un cheval de Troie. Sous l'aspect d'un logiciel dédié à une application donnée se cache un programme qui exécutera tout autre chose à l'insu de son utilisateur. Il est aussi possible d'utiliser un cheval de Troie, pour introduire un virus sur un ordinateur. Dans ce dernier cas, le cheval de Troie idéal est un antivirus que l'utilisateur installe en toute confiance sur sa machine! Bien entendu, il est très facile d'installer un cheval de Troie sur un ordinateur-cible en utilisant une messagerie électronique : on l'envoie en pièce jointe d'un courrier anodin, et il suffira que l'utilisateur double-clique dessus pour que le cheval de Troie s'installe et commence à faire son travail. Par exemple, envoyer à telle adresse une copie de tout document qui serait enregistré sur le disque dur de l'ordinateur-cible par son utilisateur.

2.3.2 Exemples

2.3.2.1 Un compilateur C comme cheval de Troie

Le compilateur C conçu par Ken Thompson et Dennis Ritchie dans le but de réécrire le noyau du système UNIX était un cheval de Troie, car il ne se contentait pas de compiler le programme désiré. Si le programme à compiler était le code source d'UNIX, le compilateur modifiait le code de la fonction de *login,* afin d'y introduire une *back door,* permettant a Ken et Dennis d'entrer dans le système grâce à un mot de passe par défaut.

A l'heure actuelle, c'est au sein même du tableur EXCEL 97 que se cache un magnifique jeu de Doom, lequel peut être activé en positionnant le curseur dans une certaine case et en effectuant une séquence donnée d'instructions au clavier et à la souris. Si une société comme Microsoft a pu cacher un tel cheval de Troie, aussi ludique et inoffensif qu'il soit, dans un logiciel qui fait mondialement autorité, que peut-on s'attendre à trouver dans d'autres domaines et d'autres applications ?

2.3.2.2 SIDA informatique

En décembre 1989, 20.000 disquettes contenant un programme d'information sur le SIDA sont envoyées aux quatre coins du monde, dans un emballage faisant croire qu'elles provenaient de l'OMS. Lors de l'utilisation du programme, s'affiche le traditionnel texte sur la propriété intellectuelle, mettant en garde l'utilisateur contre l'utilisation frauduleuse du logiciel et l'invitant à payer la licence. Généralement personne ne lit ce texte, mais cette fois-ci, cela aurait été préférable. Il était spécifié dans les termes du contrat d'utilisation, qu'en cas de non-paiement, des mesures seraient prises à l'encontre d'autres logiciels se trouvant dans l'ordinateur! De nombreuses personnes ont essayé sans autre précaution ce logiciel et quelques temps après, le virus détruisit leurs fichiers. On ne connut jamais l'ampleur exacte des dégâts.

2.3.2.3 Le ver d'ARPANET

Le 2 novembre 1988, Robert Morris Jr, tout jeune diplômé de l'Université de Harvard, lâche un ver écrit par lui sur ARPANET. Le ver se transmet de machine en machine en activant automatiquement le système de messagerie électronique. Le ver sature les machines contaminées en s'y reproduisant indéfiniment. Très vite, l'ensemble des communications sur le réseau est très fortement ralenti. Les administrateurs systèmes n'ont pas eu d'autres choix que de déconnecter leurs machines du réseau. Une semaine plus tard, le ver put être neutralisé et ce fut l'heure des constats. Le réseau ARPANET, sensé être utilisé pour les communications militaires en particulier en cas d'attaque nucléaire, avait été "mis à genoux" par un simple programme écrit par un étudiant!

2.4 Facteur humain et human engineering

S'il existe un maillon faible dans la chaîne de la sécurité informatique, c 'est bien l'homme. La plupart des intrusions dans les systèmes informatiques protégés par des mots de passe sont faites en utilisant des dictionnaires de termes courants. Combien d'entre nous utilisent comme mot de passe d'ordinateur une date de

naissance (la nôtre ou celle d'un proche), le nom de sa femme, de ses enfants, des termes banals tels que "secret", "toto", etc. ? Il y a aussi des opérateurs, qui de peur de ne pas se rappeler un mot de passe compliqué (et donc beaucoup plus sûr pour le système) l'écrivent sur un papier collé sur le bord de l'écran de leur ordinateur!

Le terme de *human engineering (ou social engineering)* est utilisé pour désigner le fait de manipuler à son insu une personne en se faisant passer pour quelqu'un d'autre et en usant de psychologie et du jargon adéquat pour lui faire révéler le plus naturellement du monde, une information qu'elle détient. Il s'agit d'une forme non conventionnelle d'action psychologique. C'est la technique utilisée par *Fry* Guy dans un des exemples précédents. Il ne faut pas croire que ce soit un cas isolé. On trouve en effet de nombreux cas, y compris dans des milieux qui devraient être sensibilisés aux problèmes de sécurité tels que l'armée américaine. Matthew G. Devost cite l'exemple de Susan H, une *hacker* :

Elle est reçue par un groupe de responsables militaires. Sur la table de conférence se trouvent un ordinateur, un modem et un téléphone. Ils lui tendent un enveloppe scellée contenant le nom d'un site informatique dans lequel elle doit pénétrer par n'importe quel moyen. Sans perdre un instant, elle se connecte sur un répertoire militaire facile d'accès afin de déterminer où se trouve le système qu'elle doit pirater. Ceci fait, elle découvre quel est le système d'exploitation utilisé et le nom du responsable de la machine. Elle appelle la base et utilise ses connaissances dans la terminologie militaire, pour savoir qui est le commandant de la base. La réceptionniste lui indique qu'il s'agit du Major Hasting, puis elle continue : " Je n'arrive plus à me rappeler le nom de la secrétaire du Major Hasting, c'était... comment déjà ? " La réceptionniste enchaîne : Buchanan, Sergent Buchanan ". Avec ces informations, elle peut maintenant appeler le responsable du centre informatique, et avec une voix autoritaire : " Ici le sergent Buchanan appelant sur ordre du Major Hasting. Il essaye d'accéder à son compte, mais ça ne marche plus, il ne sait pas pourquoi ". (...) En moins de vingt minutes, elle avait sur son écran les informations confidentielles de ce centre informatique de l'armée.

2.5 Conclusion partielle

Dans le cyberespace, le *bit* pourrait bien être devenu l'ultime évolution de l'arme à guidage terminal. Quelles que soient les barrières logiques mises en place pour interdire les connexions à des sites sensibles, elles ne sont ni plus étanches ni plus inviolables que ne le sont les barrières matérielles qui sont sensées protéger les installations en dur contre les accès physiques de cambrioleurs ou de commandos organisés. Tout au plus ces barrières logiques permettent-elles de déceler une tentative d'intrusion, de donner l'alerte et de gagner des délais autorisant une réaction.

Il devient impératif de se prémunir contre la menace que feraient peser sur notre sécurité nationale des gouvernements hostiles, des groupes terroristes ou des *hackers* isolés qui pourraient chercher à s'introduire sur nos réseaux afin d'y piller des informations sensibles, ou d'y désorganiser des bases de données ou des réseaux stratégiques. Il est dès à présent plus que probable que plusieurs Etats sont

en train de développer des doctrines, des outils et des réseaux de spécialistes pour mener cette guerre totale sans combat que représenterait une attaque combinée sur nos systèmes d'informations.

L'image qu'emploient les Américains pour évoquer une telle éventualité est celle d'un « Pearl Harbor électronique » qui prendrait pour cible l'infrastructure nationale de l'information. Au cours d'un colloque national sur le sujet, le 26 juin 1995, le sénateur Sam Nunn affirmait « Je crois que nous sommes dès à présent parfaitement alertés face à ce risque. Je ne sais pas comment nous pourrions faire face à un Pearl Harbor électronique, mais nous serons, j'en suis sûr, dans de grandes difficultés. Je suis certainement fondé à prédire de vastes problèmes très inconfortables. »

Il est bien évident que la France, actuellement en retard dans son implantation sur l'Internet, est en passe de se retrouver dans la même situation que les Etats-Unis à court terme.

3. GUERRE INFORMATIQUE

3.1 Le terrain

L'expansion rapide de la communication entre ordinateurs a fait naître ce qu'il est devenu d'usage d'appeler le cyberespace. Le réseau Internet en est la meilleure et la plus universelle illustration, dont la croissance exponentielle est de nature à le rendre incontournable pour tous les échanges de données ou d'instructions dans les domaines économiques, financiers ou politiques entre autres. Cette évolution sans précédent dans l'Histoire nous amène à accepter l'existence d'un nouvel univers, parallèle en quelque sorte a celui dans lequel nous existons et agissons, dans lequel existent et circulent l'ensemble des données qui régissent notre monde matériel. C'est ainsi que les comptes bancaires, les cotations en bourse, la gestion des transports aériens ou de surface, les télécommunications de toutes natures, et jusqu'aux installations de production ou de gestion d'énergie sont désormais contrôlés exclusivement par des ordinateurs. Ceux-ci sont de plus en plus interconnectés entre eux, soit directement soit par l'intermédiaire.d'un réseau interne (Intranet) ou externe (Internet) L'existence même de cet univers parallèle ou cyberespace permet de conclure qu'il existe forcément une stratégie parallèle, ou cyberstratégie, qui doit permettre à un groupe d'agir dans le cyberespace avec pour but d'imposer sa volonté à un pays ou une organisation, par l'application pure et simple des principes de la guerre.

3.2 Les actions possibles

La guerre informatique peut bien entendu revêtir diverses formes et avoir plusieurs degrés d'intensité.

Winn Schwartau propose la classification suivante :

3.2.1 Classe 1: guerre informatique contre les personnes

Cette classe comprend les atteintes à la sphère privée de l'individu. Cela inclut la divulgation d'informations stockées dans une quelconque base de données. Nous n'avons aucun contrôle actuellement sur les données nous concernant qui se trouvent un peu partout telles que: l'historique des utilisations d'une carte de crédit, le montant d'un compte en banque, le suivi d'un dossier médical, les fiches de paye, le casier judiciaire, etc. On peut retenir les points suivants:

- des centaines de bases de données contiennent ensemble une image digitale de la vie d'un individu ;
- les informations disponibles ne sont pas forcément correctes ;
- il est presque impossible de corriger des informations erronées ;
- tout abus de cette image digitale pourrait amener la mort politique d'un grand de ce monde à un moment critique.

Il n'est que de se rappeler que l'assassinat, par un étudiant serbe, de l'Archiduc François-Ferdinand fut directement à l'origine de la Première Guerre Mondiale pour mesurer la portée que pourrait avoir une attaque informatique contre une ou plusieurs personnalités dans le cadre d'une stratégie concertée.

3.2.2 Classe 2: guerre informatique contre les entreprises

Concrètement, aujourd'hui, cette classe correspond à la concurrence entre entreprises qui s'affrontent dans une guerre commerciale sans pitié. L'espionnage industriel est une des activités possibles, mais la désinformation est également un moyen très efficace de se débarrasser d'un concurrent. A l'heure actuelle, il est très facile de lancer des rumeurs de portée mondiale, notamment grâce à l'Internet. On peut également, par le procédé dit de la " mascarade ", créer un site WEB qui, après saturation automatique du site WEB d'une entreprise, sera consulté en lieu et place du site d'origine par quiconque voudra s'y connecter, et ce à l'insu de ce dernier ainsi que du gestionnaire du site. Il sera ainsi possible de faire passer des informations proprement suicidaires sur le site d'une société ou d'une organisation sans que personne ne puisse s'apercevoir que celles-ci sont fausses.

Comme de plus il est bien connu que plus un fait est démenti, plus l'opinion publique considère qu'il ne peut y avoir autant de fumée sans feu, le mal sera fait quelle que soit la parade adoptée.

3.2.3 Classe 3: guerre informatique globale

Ce type de conflit vise les industries, le potentiel économique, la puissance militaire, et donc l'ensemble d'un pays. Dans cette classe, il faut multiplier la puissance des classes I et 2 par un grand facteur. Avec des investissements dérisoires en regard de ceux consentis dans le cas d'armes "traditionnelles", il est possible pour un groupe terroriste ou un pays quelconque de mettre à genoux une grande puissance. L'avantage pour l'attaquant, s'il entre dans la catégorie des pays

en voie de développement, est qu'il ne sera que très peu sensible à des représailles de même nature. De plus, il serait très difficile pour un pays industrialisé et démocratique de répondre à une attaque de ce genre par des représailles armées, sans s'aliéner l'opinion publique mondiale.

Il est communément admis que seuls les Etats-Unis et quelques très rares pays, dont la France, auraient les moyens de développer une stratégie informatique offensive. Or à mon sens il n'en est rien, car depuis des années la saisie du code source des logiciels les plus performants est sous-traitée à des pays à main d'œuvre bon marché. L'Inde et le Pakistan, pour ne citer que ces pays, on ainsi acquis une grande maîtrise dans l'informatique des codes sources : à force de faire, on finit fatalement par savoir faire. Il y a probablement tout lieu de craindre qu'une attaque informatique contre un pays développé puisse venir de n'importe où, relayée par des serveurs et des ordinateurs d'un ou plusieurs pays tiers *a priori* non impliqués.

3.3 Scénario possible

Afin de mieux cerner le problème de la guerre de l'information, le Département de la Défense américain a demandé à la société RAND Corporation, qui fête son cinquantenaire en 1998, de conduire des exercices de simulations stratégiques sur ce sujet. Six exercices ont eu lieu entre janvier et juin 1995. Les participants étaient de hauts responsables de la sécurité nationale et des industriels du secteur des communications. Une des situations était la suivante:

Février 2000, l'Iran rente de couper la production de pétrole de l'Arabie Saoudite afin de faire monter les cours. Washington envisage d'envoyer des troupes en Arabie pour mettre fin au conflit. Les Iraniens se souvenant de l'échec de Saddam Hussein, décident de porter le combat sur le sol américain, en visant la grande force et aussi la plus grande faiblesse des USA, les systèmes d'information automatiques.

Des centraux téléphoniques de bases militaires deviennent inutilisables, saturés d'appels provoqués par l'ennemi mais arrivant de tous les continents, d'autres centraux dans le pays sont purement et simplement hors service. Sans avoir une vision globale des choses, il est alors impossible de se rendre compte qu'une attaque est en cours.

La Maison Blanche prend enfin conscience du problème après 48 heures de chaos dans les télécommunications militaires. Des trains convoyant vers un aérodrome du matériel militaire, destiné à partir pour l'Arabie, déraillent suite à un problème dans le système de contrôle du trafic ferroviaire. La City Bank d'Angleterre signale qu'elle vient de découvrir un sabotage de son système de transfert de fonds. CNN annonce que l'Iran a payé des experts en informatique russes et des programmeurs indiens pour détruire l'économie occidentale. Suite à cette information, les cours des bourses de New York et Londres s'effondrent.

L'ordre de départ des unités vers l'Arabie est donné, mais ce dernier s'effectue dans le plus grand chaos causé par les problèmes de communications dans les bases de regroupement et par la neutralisation des transports ferroviaires et aériens.

Une grande banque américaine découvre que son ordinateur devient fou, il crédite et débite au hasard des milliers de dollars sur les comptes de ses clients. L'information s'ébruite et c'est la panique chez les épargnants qui veulent à tout prix récupérer leur argent. La panique et des émeutes graves s'étendent à tout le pays.

Plus tard, tout Washington est privée de téléphone (y compis les mobiles), il devient entre autres très difficile pour le Président de réunir ses conseillers. On signale aussi des programmes pirates de désinformation sur les chaînes de télévision aux Etats-Unis et en Arabie.

Il s'agit ici d'un résumé du scénario, qui en lui-même aurait été plus long que ce mémoire. A partir de là, les participants à l'exercice avaient 50 minutes pour proposer des solutions...

Les principales conclusions tirées de ces exercices sont :

- n'importe qui pourrait mener une telle attaque;
- il est impossible de distinguer ce qui est réel de l'intoxication;
- il est très difficile de déceler l'attaque;
- tous les schémas décisionnels usuels s'effondrent.

Un certain nombre de responsables de la sécurité des Etats-Unis refusent de croire à de tels scénarios catastrophes. Martin Libicki, enseignant à la *National Defense University,* considère qu'il est excessif d'extrapoler une menace pour la sécurité nationale à partir de faits qui jusqu'à présent n'ont été que des versions électroniques de la " virée à bord d'une voiture volée ".
Ce point de vue fait cependant peu de cas des extraordinaires capacités de concentration des effets qu'offre l'informatique de réseau. Libicki refuse d'admettre qu'un gouvernement ou une organisation terroriste pourraient fort bien mener des actions coordonnées en regroupant des *hackers* de haut niveau, en les dotants des moyens nécessaires et en leur fixant des objectifs stratégiques en lieu et place de leurs objectifs individuels d'enrichissement personnel.

4. CONCLUSION

Nier l'existence du concept de guerre informatique en 1998 pourrait bien procéder de la même clairvoyance que le refus d'admettre, en 1914, qu'un aéroplane de bois et de toile pourrait un jour couler un cuirassé ou raser une ville.
Rappelons-nous qu'en 1996, l'ordinateur Deeper Blue d'IBM a terrassé sans discussion possible le champion du monde d'échecs Gary Kasparov. Si l'on admet que les échecs représentent bien l'archétype du jeu de stratégie, on est en droit de se demander ce que feraient plusieurs de ces ordinateurs, travaillant en réseau et programmés par des génies du *hacking* pour détruire ou neutraliser l'informatique d'un pays, ce qui se traduirait par une crise immédiate et probablement extrêmement grave. La destruction ou la paralysie des systèmes de paiement, de transport, de télécommunications, tous très informatisés et fonctionnant en réseau, aurait en effet toutes les chances de se traduire en quelques heures par des troubles extrêmes.
Alors que la France, sous l'impulsion explicite de son gouvernement, se tourne résolument vers l'Internet et l'informatique de réseau, il est temps de prendre en compte la stratégie qu'elle aura à définir et à suivre pour s'assurer, dans le cyberespace, la souveraineté qu'elle y mérite autant que dans l'univers physique.

BIBLIOGRAPHIE

Les documents utilisés pour la rédaction de ce mémoire ont tous été téléchargés sur le Web, en utilisant les moteurs de recherche *Yahoo* et *Excite.*

Les mots-clés rentrés en recherche ont été :

- Cyberwar
- Information warfare
- Hacking
- Phreaking

La liste des sites et des articles ainsi obtenue n'a pas été relevée par écrit, mais peut aisément être retrouvée et enrichie par la même recherche.