ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

PROJET

SCIENCE, TECHNIQUE et SOCIÉTÉ

Terrorisme informatique : Quels sont les risques ?

Patrick GALLEY

29 mai 1996

Table des matières

Introduction

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, finalement, s'occupe de vous.

De temps en temps, la presse dévoile aux yeux du public que des pirates informatiques 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 votre compte en banque ou se baladent dans les ordinateurs de l'armée. On nous apprend aussi que des virus informatiques circulent d'ordinateurs en ordinateurs en attendant l'instant où ils vont détruire le contenu de nos 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* [SCHWAR93] ont exploité cette hypothèse.

Un tel scénario est-il envisageable ou bien n'est-ce là que des spéculations d'auteurs de science-fiction.

C'est à cette question que je vais tenter de répondre dans ce mémoire. Je m'intéresserai uniquement aux pays fortement industrialisés, et particulièrement aux Etats-Unis dont les infrastructures informatiques sont les plus développées.

Méthode

Tout d'abord, je parlerai brièvement du terrorisme et des terroristes, afin de déterminer si leurs motivations et méthodes usuelles leur permettraient d'utiliser l'informatique comme nouvelle arme et d'obtenir ainsi des résultats similaires à l'utilisation de bombes, d'enlèvements ou d'assassinats.

Je passerai, ensuite, en revue l'univers de la criminalité informatique pour montrer ce que des individus décidés parviennent à faire avec des ordinateurs ne leur appartenant pas.

Je ferai mention de la vulnérabilité de certains systèmes informatiques sensibles, que ce soit face à des pannes ou à des sabotages.

Je parlerai de la "guerre de l'information", un des nouveaux sujets de prédilection de l'armée américaine (entre autres) afin de voir à quel point le risque d'un tel conflit les préoccupe.

Finalement, je ferai la synthèse de tous ces éléments et tâcherai de déterminer si il y a ou non un risque de terrorisme informatique.

Conventions

Je ne traduirai pas les termes anglais couramment utilisés en français, tels que *cracker*, *hacker* ou *phreaker*. Ces termes seront écrits en italique.

A la fin de ce document se trouve un lexique, donnant la signification de tous les termes techniques et sigles employés.

Les références à des ouvrages ou articles seront données entre crochets avec le nom de l'auteur et l'année, par exemple : [BRANDT95]. La bibliographie se trouve à la fin de ce document.

CHAPITRE 1

Terrorisme

Définitions

Le terme de "terrorisme" apparaît pour la première fois en 1798 lorsque le philosophe Emmanuel Kant l'utilise, étrangement, pour décrire une conception pessimiste du destin de l'humanité. La même année, on retrouve le terme dans un supplément du grand Dictionnaire de l'Académie française; il évoque alors les excès de la Terreur révolutionnaire et n'a donc pas le sens que nous lui prêtons aujourd'hui. Nous nous référons en effet, le plus souvent, à l'action de mouvements clandestins qui prennent pour cible le gouvernement d'un pays dans le but d'en renverser radicalement l'ordre politique et social: ce n'est pas seulement l'Etat qui est visé, mais l'ensemble du système social. [BONA94]

Voyons quelques autres définitions :

"Terrorisme : n.m Ensemble d'actes de violence commis par une organisation pour créer un climat d'insécurité ou renverser le gouvernement établi." [LAROUS83]

"(...) Le terrorisme est donc essentiellement une stratégie destinée à déséquilibrer un pays ou un régime, utilisant la subversion et la violence sur un milieu ou une institution en crise pour contribuer au désordre, à la veille d'une "remise en ordre" révolutionnaire ou d'une guerre de conquête menée par une puissance étrangère. (...)" [ENCYCL89]

Il convient de rajouter à ces définitions, l'utilisation du terrorisme comme moyen de pression. Dans le cas du terrorisme international, les attentats sont généralement utilisés pour faire pression sur un gouvernement, par le biais de l'opinion publique, afin d'obtenir quelque chose de précis, comme la libération d'un prisonnier ou l'arrêt des exportations d'armes vers un certain pays.

Formes de terrorisme

Le terrorisme peut prendre différentes formes. Luigi Bonanate [BONA94] propose la classification suivante :

Tout d'abord, il faut distinguer le terrorisme *interne* et le terrorisme *international*. Le terrorisme interne comprend à la fois le terrorisme d'Etat (terreur) et le terrorisme *révolutionnaire*, selon qu'il s'agit de renforcer ou de détruire l'Etat. L'Etat peut appliquer le *règne de la terreur* ou bien recourir au *terrorisme d'Etat*, comme lorsqu'on l'accuse de favoriser des actions terroristes déstabilisantes dans le but de renforcer l'autorité centrale. L'Etat peut être enfin à l'origine de formes de terrorisme *belliqueuses*, quand, par exemple, il recourt en temps de guerre à des bombardements massifs pour effrayer l'ennemi (bombardement de Dresde, 7-15 février 1945) ou pour le décourager définitivement (bombardement atomique d'Hiroshima et Nagasaki, 6 et 9 août 1945).

Il y a aussi divers types de terrorisme *international*. En premier lieu vient le terrorisme *indépendantiste* ou s*éparatist*e, s'agissant de mouvements qui veulent s'émanciper d'une domination coloniale ou constituer un Etat indépendant, ou même parfois s'unir à un autre Etat que celui auquel ils appartiennent. Par nature, le terrorisme *indépendantiste* est toujours international, car il porte ses coups au-delà des frontières du territoire concerné. C'est le cas du terrorisme palestinien. A l'opposé, on peut trouver un terrorisme *colonialiste* visant à conserver la souveraineté d'une puissance sur une colonie.

Pour compléter ce tableau, il convient d'évoquer une ultime forme de recours à la terreur à l'échelle planétaire, même si elle sort de la problématique spécifique du terrorisme : il s'agit de "l'équilibre de la terreur". Cette formule résume la politique conduite par les Etats-Unis et l'Union soviétique (jusqu'à la dissolution de cette dernière), afin de geler l'ordre international issu de la Seconde Guerre mondiale, et ce par la menace d'une destruction nucléaire totale.

En 1937, après l'attentat de Marseille contre le roi de Yougoslavie et le ministre français Louis Barthou en octobre 1934, la SDN élabora une convention internationale qui sera signée à Genève le 16 novembre par vingt-cinq pays (sauf l'Italie et les Etats-Unis). Cette convention définit globalement les actes terroristes comme "des faits criminels dirigés contre un Etat et dont le but ou la nature est de provoquer la terreur chez des personnalités déterminées, des groupes de personnes ou la population" (article 2). Les signataires du texte dressent ainsi la liste détaillée des différentes formes de terrorisme :

1. Les faits intentionnellement dirigés contre la vie, l'intégrité corporelle, la santé ou la liberté:
   a) des chefs d'Etats, des personnes qui exercent les prérogatives de chef d'Etat, de leurs successeurs héréditaires ou désignés;
   b) des conjoints des personnes préalablement citées;
   c) des personnes investies de fonctions ou de charges publiques lorsque le fait susmentionné a été commis en raison des fonctions ou des charges que ces personnes exercent.
2. Le fait de détruire ou d'endommager intentionnellement des biens publics ou destinés à une utilisation publique, qui appartiennent à un autre Etat signataire ou qui lui appartiennent en propre.
3. Le fait de mettre intentionnellement en danger des vies humaines afin de créer un danger commun.
4. La tentative de commettre des infractions prévues par les dispositions précédentes de cet article.
5. Le fait de fabriquer, de se procurer, de détenir ou de fournir des armes, des munitions, des produits explosifs ou des substances nocives en vue de l'exécution, dans n'importe quel pays, d'une infraction prévue par le présent article. [BONA94]

Evolution du terrorisme international

La dixième conférence annuelle internationale sur les problèmes de la justice pénale[1], a réunit, entre autre, fin juillet 1995, des membres actuels et anciens du FBI, du Département d'Etat et du Département de la Défense américains, des experts anti-terroristes argentins et israéliens.

Il ressort de cette conférence, que l'utilisation à l'avenir, d'armes provocant beaucoup plus de victimes civiles est très probable. D'après Peter Probst (DoD), les groupes terroristes ethniques ou religieux ne seront pas réticents à faire un grand nombre de victimes, alors que les anciens groupes terroristes politiques hésitaient à le faire, de peur de perdre la possibilité d'un soutien de la population. De plus, l'attentat au gaz toxique, au Japon, a brisé le tabou de l'utilisation de l'arme chimique. [FANNING95]

1 *Tenth Annual International Conference on Criminal Justice Issues*, Université d'Illinois à Chicago, du 31 juillet au 3 août 1995.

CHAPITRE 2

Criminalité informatique

Introduction

Le but de ce chapitre est de rendre attentif le lecteur à l'ampleur du phénomène de la criminalité informatique, ainsi qu'à notre vulnérabilité face à ces attaques.

Définition

La criminalité informatique est un vaste domaine, dont les frontières ne sont pas toujours faciles à définir. Chaque pays a une législation différente à ce sujet, et a réagi plus ou moins vite face à ce problème. En Europe, la Suède a été le précurseur, en instituant une loi en 1973, qui considérait comme crime, l'acquisition non autorisée de données stockées [LAB90_1], alors que les Pays-Bas n'ont considéré l'intrusion (sans dégâts) dans un ordinateur comme un crime qu'après 1990 [LAB90_4].

David L. Carter, professeur au département de justice pénale de l'université de l'Etat du Michigan, propose une classification de la criminalité informatique [CARTER92].

1. L'ordinateur est la cible

Cette catégorie comprend des actions telles que:

- Vol d'informations (plans de nouveaux produits, listes de clients, ...)
- Chantage, basé sur des informations obtenues par le vol de fichiers informatiques (informations médicales, ...).
- Sabotage des données ou du système.
- Accès non autorisé aux fichiers des autorités, pour y modifier des données (casiers judiciaires, permis de conduire, ...)
- Techno-vandalisme (destruction sans but précis, volontaire ou non, de données)
- Exploration (Intrusion dans un système, juste pour le plaisir d'y aller, sans intention d'y voler quoi que ce soit)

2. L'ordinateur est l'outil d'un crime conventionnel

Cette catégorie comprend les cas où l'ordinateur facilite le travail des criminels mais n'est pas essentiel.

- Détournements de fonds
- Meurtre par modification des dosages des médicaments d'un patient dans un hôpital.

- Serveurs fournissant des données illégales (pornographie enfantine, ...)

3. L'ordinateur génère de nouveaux types de crimes

Cette catégorie comprend des crimes "classiques", adaptés à l'ordinateur.

- Copies de logiciels
- Contrefaçons de matériel

Cette classification n'est pas exhaustive. Par la suite, je me préoccuperai essentiellement des deux premières catégories.

Hacking

Définition

Le *hacking* est l'activité du *hacker*. Les sens donné au terme *hacker* sont très variés[2]. A la base, un *hacker* est une personne qui a du 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 [STERLING92]. Dans ce document j'utiliserai le terme *hacker* dans ce dernier sens, en y incluant aussi le *phreaking* (piratage du téléphone), car ces deux activités sont indissociables

Introduction

Le but de ce chapitre sur le *hacking*, est de citer quelques cas pour montrer l'incroyable vulnérabilité des systèmes informatiques. Un 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 [ROUSH92]. Ces chiffres sont à prendre avec prudence, car très peu de cas sont effectivement raportés aux autorités. Le NCCS estime que moins de 10 % des cas d'intrusions sont signalés [ICOVE95], les entreprises victimes de *hackers*, n'ayant pas du tout envie de se faire une mauvaise publicité, en avouant leurs faiblesses.

Quelques cas

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 vit que 63 autres personnes avaient consultés la même information le même jour. Il remarqua un groupe de 700 personnes qui semblaient détenir la même carte de crédit et 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

[2] Une définition exhaustive est donnée dans le lexique à la fin de ce document.

gouvernemental de protection des témoins. En bon citoyen, il s'empressa de prévenir le FBI de cette faille potentielle dans la sécurité de leur programme de protection. [CLOUGH93]

Distributeur de billets

En France, un *hacker* avait trouvé le moyen de reprogrammer à distance les taux de change d'un distributeur de billets. Il s'octroyait, par exemple un taux de change de 5 dollars pour 1 franc, changeait 100 francs. Il effectuait l'opération inverse, le taux de change passait à 5 francs pour 1 dollar et il retournait changer ses dollars et recevait ainsi 2500 francs! [BLANCH95]

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 ordonnés par téléphone. La banque a appelé ses clients pour demander confirmation du transfert, mais les appels étaient détournés vers la résidence d'un des criminels. Les sociétés volées se sont vite rendu compte de l'affaire et une enquête a été ouverte. Grâce aux enregistrement des appels de confirmations, les enquêteurs ont pu appréhender les sept criminels avant qu'ils ne prennent la fuite. [ICOVE95]

Argent de poche

Fry Guy est un *hacker* de 17 ans, habitant dans l'Indiana (USA). En 1989, il est passé maître dans l'art de commander aux centraux téléphoniques de la compagnie locale de téléphone et il a trouvé un moyen de se faire un peu d'argent de poche facilement. Il contacte un commerçant en se faisant passer pour un employé d'une société de cartes de crédits et arrive à lui faire donner son numéro de client et son mot de passe. Munit 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 "à l'aise" au point de vue crédit, 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 la cabine vers un des ses téléphones. Il appel une banque pour faire un virement dans leur agence de Paducah en débitant la carte de sa victime. La banque rappelle 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. [CLOUGH93]

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 à1961 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*"[3], 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. [CLOUGH93]

Motivations et éthique

Beaucoup de *hackers* explorent les systèmes informatiques par simple curiosité et par défi intellectuel. Les "vrais" *hackers* ont un code éthique leur interdisant la destruction de toute information. Cependant, certains moins bien intentionnés, ont compris qu'ils pouvaient tirer de nombreux avantages de ces connaissances particulières. Le cas le plus classique est le vol de numéros de cartes de crédits, mais certains on trouvés des moyens plus originaux, tel ce *hacker* maîtrisant le piratage téléphonique, qui gagnait des jeux organisés par des stations radio, car il bloquait tous les appels téléphoniques des auditeurs et il était ainsi la première personne à appeler la radio et empocher le magot!

Des faits plus sérieux ont impliqués Karl Koch, un membre du fameux Chaos Computer Club, qui piratait des sites américains pour le compte du KGB, leur fournissant divers programmes, des listes de mots de passe, etc. [CLOUGH93] Il n'agissait pas par idéologie mais pour gagner de quoi s'offrir de la drogue, tout en pratiquant son sport favori, le *cracking*!

Le Dr Frederick B. Cohen propose une liste de motivations [COHEN95] pouvant inciter des personnes à entrer dans le monde de la criminalité informatique.

Le mobile le plus banal est **l'appât du gain** (voir les deux exemples précédents).

Par **défi** ou pour obtenir une certaine **reconnaissance sociale** (et pouvoir s'insérer dans un groupe) un jeune *hacker* se doit d'aller toujours plus loin. Le Dr Cohen cite le cas d'un club allemand qui demande à ses nouveaux membres, comme droit d'entrée, de créer un nouveau virus.

La vengeance d'un employé licencié est souvent la raison de destruction de données, voir même de matériel.

Dans un domaine proche, nous trouvons **l'autodéfense**. Par exemple, celle d'un programmeur qui introduit une bombe logique dans son programme, afin d'être sûr qu'il sera payé[4].

L'avantage économique requiert parfois d'entrer dans l'illégalité pour obtenir les derniers secrets de fabrication de son concurrent. Comme à la fin de la Guerre froide, il fallait trouver de nouvelles missions pour justifier les énormes infrastructures des services de renseignements, l'espionnage économique est devenu une des priorités de ces agences. Le degré d'implication varie d'un pays à l'autre. Il semblerait que les services français ainsi que les

[3] Le terme vient de la couleur du matériel saisi lors de la fraude de 1961. Il existe actuellement toute une gamme de dispositifs avec des fonctions différentes, chaque fonction étant associée à une couleur particulière; les désignations peuvent varier selon les utilisateurs.

[4] Cela peut sembler légitime au premier abord, mais la législation de certains pays, notamment les USA, considère cette pratique comme étant de l'extorsion.

américains soient très actifs dans ce domaine, les Français aidant directement leurs entreprises en leur fournissant des informations confidentielles, les Américains en discréditant les concurrents. [GUISNEL95]

Virus, vers et chevaux de Troie

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 l'autre, si l'on copie le programme infecté sur un ordinateur sain. S'ils ne faisaient que se reproduire, les virus n'inquiéteraient personne. Seulement voilà, 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.

Un ver diffère du virus au sens qu'il se transfert de lui-même d'un ordinateur à l'autre au travers d'un réseau. L'exemple le plus connu et le plus dévastateur est sans doute le ver d'ARPANET, qui paralysa le réseau en 1988.

Un cheval de Troie est un programme qui n'est pas ce qu'il à 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 honnête logiciel se cache un programme perfide! 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!

Exemples

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 à Ken et Dennis d'entrer dans le système grâce à un mot de passe par défaut.

Comme cette astuce pouvait se voir facilement lors de la lecture du code source du compilateur, Thompson rajouta une fonction dans le compilateur qui détectait si le programme à compiler était un compilateur C, et si c'était le cas, il y rajoutait le premier cheval de Troie. Il ne lui restait plus qu'à enlever du code source les traces de la manipulation et à partir de là, l'astuce est devenu indécelable. [COHEN93] [THOMP84]

Cette histoire a été révélée en 1984 par Ken Thompson. Nous ne saurons jamais si elle est véridique ou pas. Cependant, il l'a racontée dans le but de nous faire prendre conscience d'une chose :

Nous ne pouvons pas faire confiance à du code que nous n'avons pas complètement écrit nous même !

Informations sur le SIDA

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 de la licence, mettant en garde l'utilisateur contre l'utilisation frauduleuse du logiciel et l'invitant à payer le logiciel. 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-payement, des mesures seraient prises à l'encontre d'autres logiciels se trouvant dans l'ordinateur! De nombreuses personnes ont essayé sans autre ce logiciel et quelques temps après, le cheval de Troie détruisit leurs fichiers. On ne connut jamais l'ampleur exacte des dégâts. [DORAN96]

Le ver d'ARPANET

Le 2 novembre 1988, Robert Morris Jr, diplômé de l'Université de Harvard, lâche un ver sur ARPANET[5]. Le ver se transmet de machine en machine grâce à une faille dans le système de messagerie électronique. Le ver sature les machines contaminées en se reproduisant. 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. Le lendemain, le ver put être neutralisé et ce fut l'heure des constats. Le réseau ARPANET sensé être utilisé pour les communications militaires en cas d'attaque nucléaire, avait été "mis à genou" par un simple programme écrit par un étudiant! [CLOUGH93]

Facteur humain et *human engineering*

Si 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 pour des codes de bancomat, ou 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 "secret", "toto", etc. ? Il y a aussi des employés, 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 bout de 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. C'est la technique utilisée par *Fry Guy* dans un des exemples précédents. Il ne faut pas croire que ce soit un cas isolé, car en me documentant, j'ai eu l'occasion de prendre connaissance de nombreux cas, même dans des milieux qui devraient être sensibilisés aux problèmes de sécurités, tels que l'armée américaine. Matthew G. Devost cite l'exemple de Susan une *hacker* [DEVOST1] :

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. Une fois fait, elle découvre quel est le système d'exploitation utilisé et le nom du responsable de la machine.

[5] ARPANET est l'ancêtre d'Internet

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, Specialiste Buchanan". Avec ces informations, elle peut maintenant appeler le responsable du centre informatique, et avec une voix autoritaire : "Ici le Spécialiste Buchanan appelant sur demande 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.

Moralité: ce n'est pas la peine de dépenser des millions pour des systèmes de protections si le personnel n'est pas formé correctement !

CHAPITRE 3

Vulnérabilité de systèmes

Introduction

Ce chapitre est destiné à citer quelques incidents ayant eu lieu dans des systèmes sensibles tels que compagnie de téléphone ou aéroport, sans que ce soient pour autant des actes de malveillance.

Exemples

Panne du système d'appel longue distance d'AT&T

Le 15 janvier 1990, suite à une mise à jour du logiciel des commutateurs téléphoniques, le réseau longue distance d'AT&T s'est planté et, pendant 9 heures, 60'000 personnes ont été complètement privées de téléphone, 70 millions d'appel ont été bloqués (des millions d'autres sont passés sans problèmes). Le problème est parti d'un commutateur à Manhattan et s'est répandu à travers le pays en moins de dix minutes [STERLING92].

Un câble coupé paralyse un aéroport

Le 15 octobre 1990, un planteur d'arbres dans la banlieue de Chicago endommage un important câble de téléphone privant 150'000 personnes de téléphone. Les distributeurs automatiques de billets de quelques banques on été paralysés. Les vols prévus à l'aéroport international O'Hare ont été retardés car la tour de contrôle a perdu le contact avec le centre principal de contrôle aérien de la FAA pour la région de Chicago [RISKS-10.62].

Panne de téléphone : Trois aéroports paralysés

Le 17 septembre 1991, un groupe de commutateurs téléphoniques de la région de New-York est privé de courant et les batteries de secours ne s'enclenchent pas. De plus les deux personnes chargées de la surveillance étaient justement ce jour-là en train de suivre un cours sur les procédures en cas de panne! Résultat, trois aéroport fermés : Kennedy, La Guardia et Newark. 500 vols ont été annulés, 500 autres retardés [STERLING92].

CHAPITRE 4

Guerre de l'information

Généralités

La guerre[6] de l'information (*information warfare*) est le nouveau sujet de prédilection de nombreuses armées dans le monde entier et surtout aux Etats-Unis. C'est un domaine très large, groupant plusieurs concepts[7] tels que la guerre électronique, la guerre psychologique, le renseignement et la guerre des *hackers (hacker warfare* ou *hackerwar)*. Le Dr John Alger propose la définition suivante [HAENI95]:

La guerre de l'information est l'ensemble des actions entreprises dans le but d'obtenir la supériorité 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, traitements de l'information et systèmes d'information.

Winn Schwartau propose la classification suivante:

Classe 1 : Guerre de l'information 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 dossier médical, les fiches de paye, le casier judiciaire, etc. En résumé, il faut retenir les points suivants :

- Des centaines de bases de données contiennent ensemble une image digitale de notre vie.
- Les informations disponibles ne sont pas forcément correctes.
- Il est presque impossible de corriger des informations erronées.

Classe 2 : Guerre de l'information contre les entreprises

Concrètement, aujourd'hui, cette classe correspond à la concurrence entre entreprises qui s'affrontent dans une guerre sans pitié. L'espionnage industriel est une des activités possibles, mais la désinformation est un moyen très efficace de se débarrasser d'un concurrent. A l'heure actuelle, il est très facile de lancer des rumeurs avec une portée mondiale grâce notamment à Internet. De plus il est bien connu que plus un fait est démenti, plus l'opinion publique se dit qu'il doit y avoir quelque chose, qu'il n'y a pas de fumée sans feu.

---

[6] Le terme "guerre" n'est pas une traduction exacte de "warfare". Warfare désigne plutôt des hostilités pouvant avoir lieu même en dehors d'un état de guerre.

[7] Pour une définition complète et précise, voir [LIBICKI95]

Classe 3 : Guerre globale de l'information

Ce type de conflit vise les industries, l'ensemble des forces économiques, l'ensemble d'un pays. Dans cette classe, il faut multiplier la puissance des classes 1 et 2 par un grand facteur. Avec des investissements ridicules vis à vis 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 économique. 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 sensibles 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 se mettre à dos l'opinion publique. [DEVOST95]

Opinions divergentes

Certains auteurs sont d'avis que la première guerre de l'information fut la Guerre du Golfe. La coalition menée par les Etats-Unis avait la maîtrise totale de l'information sur le champ de bataille (satellites, AWACS, JSTARS, etc.), alors que l'Iraq avait été, dès les premiers instants de la guerre, privé de ses principales infrastructures de communication.

D'autres, par contre, trouvent que les techniques employées lors du conflit sont reprise de la "vague industrielle"[8] (emploi de bombardements massifs) mais aussi de la "vague de l'information" (largage de bombes "intelligentes" sur des centres de communications). Pour eux, cette guerre n'était pas une "pure" guerre de l'information.

Sécurité des ordinateurs militaires

Paradoxalement, ce n'est qu'à la suite de la Guerre du Golfe que les Etats-Unis ont pris conscience de leur vulnérabilité. A la demande du Pentagone, la DISA a réuni une équipe de *hackers* "maison", leur a donné un accès à Internet, et leur a demandé de s'introduire dans le plus d'ordinateurs possible du DoD. Ils ont pris le contrôle de 88 % des 8900 ordinateurs qu'ils ont attaqués et seulement 4 % des attaques ont été signalées aux différents responsables des ordinateurs! En combinant ces résultats avec 350 intrusions détectées provenant de *hackers* non identifiés, ils sont arrivés à la conclusion que 300'000 intrusions dans des ordinateurs du DoD ont eu lieu en 1994 ! [MUNRO95]

Attention, les ordinateurs militaires, qui sont connectés sur Internet, ne contiennent généralement pas d'informations confidentielles et n'effectuent pas des tâches vitales. Cependant ces ordinateurs sont quand même chargés de la logistique, de la gestion du personnel, de la comptabilité, des domaines qui peuvent se révéler sensibles. Lors de la Guerre du Golfe les Etats-Unis ont beaucoup utilisé Internet pour transmettre des informations de logistique, parfois même sans les coder. Les informations sur le personnel peuvent être utilisées dans le but de déterminer des cibles potentielles pour faire du chantage ou de la corruption afin d'obtenir des informations confidentielles.[BRANDT95] Un groupe de hackers hollandais aurait proposé à Saddam Hussein de perturber les communications de l'armée sur Internet pour un million de dollars. Il aurait décliné l'offre. [WALLER95]

[8] Selon la classification du futurologue Alvin Toffler dans son livre *War And Anti War*, l'évolution de la guerre dans l'histoire de l'humanité se décompose en trois vagues : la vague agraire (homme contre homme) , la vague industrielle (destruction massive), la vague de l'information (attaque dirigée contre l'information)

Dépendance de l'armée vis-à-vis des infrastructures civiles

Comme nous l'avons vu précédemment, l'armée possède pour ses activités sensibles des ordinateurs biens protégés. Cependant, les bases militaires américaines (ce doit très certainement être le cas dans les autres pays) dépendent des infrastructures civiles notamment dans les domaines de l'alimentation électrique et des communications. Près de 95 % des communications de l'armée américaine passent par le réseau téléphonique normal. Les transports de troupes, que se soit par rail ou par avion, se font sous le contrôle de systèmes civils! [RAND95]

Simulations

Afin de mieux cerner le problème de la guerre de l'information, le Département de la Défense américain a demandé à la société RAND de conduire des exercices de simulations stratégiques sur ce sujet. [RAND95] [THOMPM95] Six exercices ont eu lieu entre janvier et juin 1995. Les participants étaient des hauts responsables de la sécurité nationale et des industriels du secteur des communications. Une des situations était la suivante :

Février 2000, l'Iran tente de couper la production de pétrole de l'Arabie Saoudite afin de faire monter les prix. Washington envisage d'envoyer des troupes en Arabie pour mette 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.

Des centraux téléphoniques de bases militaires deviennent inutilisables, saturés d'appels provoqués par l'ennemi, d'autres centraux dans le pays sont 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 est enfin consciente du problème. Un train convoyant du matériel militaire, destiné à partir pour l'Arabie, vers un aérodrome militaire, déraille suite à un problème dans le système de contrôle du trafic ferroviaire (bombe logique). La Banque d'Angleterre, signale qu'elle vient de découvrir une tentative de sabotage du système de transferts 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 soldats 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 déploiement.

Une grande banque 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 s'étend à tout le pays.

Plus tard, tout Washington est privé de téléphone (même les mobiles), il est alors très difficile pour le Président de réunir ses conseillers. On signale aussi des programmes pirates de propagande sur les chaînes de télévision aux Etats-Unis et en Arabie.[9]

A partir de là, les participants à l'exercice, avaient 50 minutes pour trouver quoi faire...

[9] J'ai raccourci le scénario, une version assez complète se trouve dans [THOMPM95].

Les principales conclusions tirées de ces exercices sont :

- ***N'importe qui peut vous attaquer.***
- ***Vous ne pouvez pas savoir ce qui est réel.***
- ***Il est difficile de savoir que vous êtes attaqué.***

Pas tous les militaires croient à ce genre de scénario catastrophe. Pour Martin Libicki, enseignant à la *National Defense University*, 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 d'une "virée à bord d'une voiture volée" !

Techniques diverses

Le but de ce paragraphe est de mettre en évidence certaines techniques utilisable lors d'une guerre de l'information et dont le grand public n'a quasiment pas connaissance.

Chipping

Le *chipping* est l'implantation matérielle d'un cheval de Troie (voir p.13). Cela consiste à rajouter une fonction, à l'insu de l'acheteur, dans un composant électronique d'une arme (ou autre matériel), de façon que si un jour cette arme devait être utilisée contre le pays vendeur, elle puisse être neutralisée à distance. [WALLER95]

Bombes EMP-T

Depuis, le début de l'ère atomique, les militaires ont entrepris de protéger leurs systèmes électroniques des radiations électromagnétiques qui seraient produites lors d'une explosion nucléaire. Sans mesures adéquates, il est possible de détruire les systèmes électroniques d'un pays en faisant exploser une bombe atomique à haute attitude.

Depuis des années, se préparent des armes non-mortelles, chargées de neutraliser les systèmes électroniques ennemis. D'après Winn Schwartau (voir note 14), des bombes EMP-T *(Electro-Magnetic Pulse Transformer*) peuvent être construites pour quelques centaines de dollars, et sont capables effacer les information stockées sur un support magnétique à 200 mètre à la ronde.

Radiations Van Eck

Jusque là, j'ai essentiellement traité des cas de piratages ayant pu avoir lieu parce que l'ordinateur pris pour cible était ouvert au monde extérieur, que se soit au travers d'un réseau informatique ou par téléphone. Si je vous dis que votre ordinateur personnel, coupé du monde extérieur et sur lequel vous êtes en train d'éditer un rapport confidentiel, peut révéler vos secrets à une personne se trouvant à une centaine de mètres de votre bureau, sans que vous ne vous rendiez compte de rien, vous direz que c'est de la science-fiction.

Et bien non! C'est tout à fait possible. Votre écran d'ordinateur émet des radiations, même avec les normes les plus strictes (civiles), et il est possible avec l'équipement adéquat de reconstituer le contenu de votre écran à distance. Cette technique a été employée par le FBI pour la surveillance de Aldrich Ames, un agent du KGB au sein de la CIA.

Le terme utilisé par l'armée américaine pour décrire cette technologie est TEMPEST[10] *monitoring*. Un équipement protégé contre ce type d'écoute est dit TEMPEST *certified*. La norme[11] indiquant les détails, tels que la quantité de radiations émises autorisée afin d'éviter toute détection est classifiée. Aux Etats-Unis, comble de l'aberration, l'utilisation du TEMPEST *monitoring*[12] est possible par le gouvernement sans demande d'autorisation[13], alors qu'il est illégal, pour un particulier ou une société privée, de s'en protéger! [SELINE89]

Frank Jones qui travaille dans une société produisant des équipements dans le domaine, entre autre, de la sécurité informatique, explique grossièrement [JONES96] comment ils ont conçut un tel équipement de détection afin de pouvoir réaliser des protections pour les ordinateurs de leurs clients. Une fois mis au point, ils ont testé avec succès leur matériel, sur des cibles tels que banques, postes de police, distributeurs de billets de banques, téléviseurs, bureaux.

Si la réalisation d'un tel équipement est à la portée de n'importe quel bureau d'ingénieurs, il est fort probable que des personnes mal intentionnées puissent sans problème se procurer un tel équipement pour se livrer à des activités criminelles.

[10] Transient Electro-Magnetic Pulse Emanation STandart.

[11] NACSIM 5100A

[12] Ecoute des systèmes qui ne sont pas TEMPEST *certified*

[13] Contrairement aux écoutes téléphoniques.

CHAPITRE 5

Terrorisme informatique

Introduction

Jusqu'à présent, j'ai essayé de donner un aperçu assez large de notre vulnérabilité du point de vue informatique, et j'espère vous avoir convaincu que nous sommes assis sur une bombe. Il est temps, maintenant, de déterminer si une organisation terroriste pourrait avoir envie d'utiliser l'informatique soit comme arme, soit comme cible, dans le but de poursuivre son combat, habituellement mené par des attentats à la bombe ou des enlèvements.

En janvier 1995, s'est tenu à Montréal une conférence[14] sur *l'information warfare*, réunissant des militaires canadiens, américains et européens, ainsi que des représentants du FBI et du Service canadien de renseignement et de sécurité. Un des thèmes de discussion fut l'attentat du World Trade Center de New-York, en février 1993. Cet attentat, qui à priori n'a rien a voir avec le sujet de la conférence, peut être considéré comme étant l'un des premiers actes de terrorisme informatique, car en fait le préjudice s'est moins situé au niveau des dégâts matériels, qu'au niveaux des dégâts "virtuels". Des milliers de firmes ont été incapables de relier leurs ordinateurs au reste du monde pendants de nombreux jours. Selon les études, cette situation a engendré des pertes évaluées à plus de 700 millions de dollars, au cours de la première semaine seulement! [VOIR1] [SZAFR1]

Définition

Il convient tout d'abord de définir la notion de "terrorisme informatique". Ce sujet n'étant pas traité en tant que tel dans la littérature, je propose ici deux définitions :

Le terrorisme informatique est le fait de détruire ou de corrompre des systèmes informatiques, dans le but de déstabiliser un pays ou de faire pression sur un gouvernement.

Le terrorisme informatique est le fait de mener une action destinée à déstabiliser un pays ou à faire pression sur un gouvernement, en utilisant des méthodes classées dans la catégorie des crimes informatiques.

[14] *Second International Conference on Information Warfare : "Chaos on the Electronic Superhighway"* 18 juillet 1995, Hôtel Hilton, Aéroport Dorval, Montréal, Canada

Il est possible de mener trois types d'actions contre un système d'information, une attaque physique, syntaxique ou sémantique. [GARIG1]

- L'**attaque physique** consiste à endommager les équipements de manière "classique", bombe, incendie, etc.
- L'**attaque syntaxique** consiste à modifier la logique du système, afin d'y introduire des délais, ou d'en rendre le comportement imprévisible. Une attaque au moyen de virus ou de chevaux de Troie entre dans cette catégorie.
- L'**attaque sémantique** est plus perfide. Elle exploite la confiance qu'ont les utilisateurs dans leur système. Il s'agit de modifier les informations entrant dans le système ou en sortant, à l'insu des utilisateurs afin de les induire en erreur.

Réflexions

Après avoir énuméré un grand nombre de faiblesses dans les systèmes informatiques, et avoir montré avec quelle facilité il était possible d'y mettre le chaos à distance, il est intéressant de se demander **pourquoi n'y a-t-il jamais eu d'attentat informatique[15] jusqu'à présent ?**

Si l'on prend la dernière vague d'attentats ayant eu lieu en France en 1995, menée par les Islamistes algériens du GIA (Groupe Islamique Armé), une réponse peut-être que, ces groupes rejetant l'occidentalisation de leur pays, rejettent par conséquent la technologie allant avec, et ne sont donc pas à même de faire du terrorisme informatique. De plus, et je crois que c'est là la principale raison, la disproportion des moyens à mettre en œuvre pour passer au terrorisme informatique fait que les groupes terroristes restent confinés aux méthode classiques.

Moyens à mettre en œuvre

Dans la théorie de la guerre de l'information de classe 3, il est admis que ce type de conflit demande beaucoup moins de ressources humaines et financières qu'un conflit avec des armes "classiques". C'est le cas parce que les conflits modernes coûtent des sommes astronomiques, mais si l'on regarde en valeur absolue, l'investissement à consentir pour faire du terrorisme, le rapport résultat/coût est fortement en défaveur du terrorisme informatique, face au terrorisme "classique".

Si l'on prend le cas d'un groupe terroriste, il est capable, avec des moyens réduits, de réaliser quelques bombes artisanales et de semer la panique dans un pays entier[16]. Dans le cas de l'attentat de l'immeuble administratif d'Oklahoma City en avril 1995, la bombe artisanale composée notamment d'engrais, a fait près de 100 morts et il semblerait que le terroriste ait agit seul ! Dans ces deux cas, avec le même investissement, il leur aurait été impossible de produire le même effet psychologique avec des attentats informatiques.

Le terrorisme informatique doit être vu comme un acte proche d'un acte de guerre, il s'agit, pour être efficace d'établir une **stratégie à long terme** et d'avoir la maîtrise d'un très grand nombres de facteurs. Le piratage des systèmes informatiques (forcément pour la plupart différents les uns des autres) de manière parfaitement synchronisée, ainsi que l'infiltration

[15] Si l'on exclue l'attentat du World Trade Center qui a été réalisé dans l'optique du terrorisme "classique", malgré son action entrant dans la définition du terrorisme informatique.

[16] Exemple, la dernière vague d'attentats en France en 1995.

d'agents dans différentes compagnies dans le but d'insérer des chevaux de Troie ou des *back doors*, est un travail de longue haleine.

Domaine d'utilisation

Ce genre de terrorisme ne se prête pas à des représailles suite à un événement précis tel que l'arrestations ou l'assassinat d'un des leaders du mouvement, sauf si l'éventualité avait été prévue longtemps à l'avance.

Le cadre idéal, pour l'utilisation de telles armes est le prélude d'un conflit armé, une sorte de Pearl Harbor[17] informatique. C'est actuellement une des principales craintes des responsables de la défense américaine. Comme les Etats-Unis ont une politique fortement interventionniste (ne les a-t-on pas surnommés "gendarmes du monde" ?), un pays décidant d'attaquer un voisin (allié des USA) aurait tout intérêt à mener d'abord une attaque informatique contre les USA, avant de s'occuper de sa véritable cible[18]. Comme un plan d'invasion ne s'établit pas à la sauvette, il est concevable d'y inclure un chapitre afin de prévoir de neutraliser par avance toute riposte venant de pays interventionnistes tels que les USA ou la France.

[17] Rade des îles Hawaï, où la flotte américaine du Pacifique fut détruite par surprise, par les Japonais, le 7 décembre 1941, ce qui provoqua l'entrée de Etats-Unis dans la Seconde Guerre mondiale.

[18] Il est aussi possible, d'attaquer d'abord puis d'attendre l'annonce de l'intervention avant d'agir dans le domaine informatique. (voir l'exemple de simulation page 19)

Conclusion

Nous voilà au terme de ce document, il est temps de répondre à la question que je m'étais posé au début : " Terrorisme informatique : Quels sont les risques ? ".

Après avoir fait ce large tour d'horizon, mon avis est qu'au point de vue de la menace terroriste telle que les pays occidentaux l'ont vécue jusqu'à présent, il n'y aura pas de passage au terrorisme informatique dans un avenir proche. Par contre des mouvements tels que les milices américaines, ou les cartels de la drogue qui utilisent largement les nouveaux médias et qui sont donc totalement immergés dans la société de l'information, sont susceptibles de mener une offensive dans le *cyberspace*.

Du points de vue militaire, je suis d'avis qu'un scénario du type de ceux utilisés en simulation par l'armée américaine est très plausible. Il serait suicidaire pour un quelconque dictateur de la trempe de Saddam Hussein, de tenter à l'heure actuelle une offensive majeure sans tirer parti au maximum des avantages du principal talon d'Achille de la société occidentale: les systèmes d'information.

A l'heure actuelle la guerre de l'information préoccupe les gouvernements occidentaux et ils sont en train de prendre des mesures afin d'éviter d'en être la cible. Cependant, la tâche à accomplir est colossale, rien que pour mieux sécuriser les systèmes militaires il faudra déjà des années et des millions de dollars, sans parler des infrastructures civile.

Il est impossible de savoir à l'instant où vous lisez ces lignes, si une attaque informatique est en train de se préparer où si elle a déjà commencé. Qui sait si des logiciels mondialement répandus comme Microsoft Windows™ ou Netscape Navigator™ ne sont pas des chevaux de Troie ?

Lexique

ARPANET	Premier réseau, créé en 1969 par l'ARPA (Advanced Research Project Agency) pour relier quelques laboratoires scientifiques américains. C'est l'ancêtre d'Internet.
AWACS	Aiborne Warning and Control System. Avion radar.
BACK DOOR	Littéralement "porte de derrière", crée par le programmeur d'un système informatique, afin de lui permettre de pénétrer sans autre dans le système, même lorsque celui-ci aura été installé chez le client, à l'insu de ce dernier.
BOMBE LOGIQUE	Programme ou morceau de programme, placé dans un ordinateur avec comme but la destruction ou la modification de données lorsqu'une certaine condition se réalise, par exemple le nom d'un employé est effacé de la liste des employés. (technique utilisée comme vengeance en cas de licenciement)
CIA	Central Intelligence Agency. Service de renseignement américain.
COMPILATEUR	Programme chargé de traduire le code source d'un programme (lisible facilement par le programmeur), en un fichier directement compréhensible par l'ordinateur.
CRACKER	Personne qui casse les sécurités dans un système. Terme inventé, vers 1985 par des *hackers* pour se défendre de la mauvaise utilisation du terme *hacker* par les journalistes, faisant l'amalgame entre les "bons" *hackers* et les criminels!
DISA	Defense Information Systems Agency
DoD	Département de la Défense (USA)
FAA	Federal Aviation Admistration.
FBI	Federal Bureau of Investigation. Police fédérale des Etats-Unis, chargée, entre autre, du contre-espionnage.

HACKER	1) Une personne prenant du plaisir à explorer les détails des systèmes programmables et comment les utiliser au maximum. 2) Quelqu'un programmant avec enthousiasme (voir même de manière obsessionnelle) ou qui a du plaisir à programmer plutôt que de faire des théories sur la programmation. 3) Une personne appréciant les valeurs du *hacking*. 4) Une personne qui est bonne pour programmer rapidement. 5) Un expert au sujet d'un certain programme ou quelqu'un qui l'utilise fréquemment. (UNIX *hacker*) 6) Un expert ou un enthousiaste de quelque sorte, par exemple en astronomie. 7) Une personne qui aime les défis intellectuels, et passer outre les limitations. 8) [Désapprouvé] Un fouineur qui cherche a découvrir des informations sensibles en fouillant partout. (Le terme correct est *cracker*) Ces définitions proviennent du Jargon, le dictionnaire des *hackers*. Note : Le sens donné par les expert en sécurité, les journalistes et le grand public, se rapproche de la définition n° 8. C'est dans ce sens là que je l'emploie dans ce document.
JSTARS	Joint Surveillance and Target Attack Radar System. Avion de surveillance électronique et de contrôle du champ de bataille.
KGB	Komitet Gossoudarstevennoï Bezopasnosti. Service secret soviétique.
LOGIN	Action de se connecter sur un ordinateur, généralement caractérisée par l'introduction de son nom et de son mot de passe.
MODEM	MODulateur DEModulateur. Dispositif permettant de connecter son ordinateur à un autre ordinateur, au travers d'une ligne téléphonique normale.
NCCS	National Computer Crime Squad
OMS	Organisation Mondiale de la Santé
PENTAGONE	Autre nom pour le Département de la Défense américain, donnée en raison de la forme du bâtiment abritant ses bureaux.
PHREAKER	Personne pratiquant le *phreaking*
PHREAKING	L'art et la science de pirater le réseau téléphonique (par exemple pour faire des appels longue-distance gratuitement). Par extension, passer outre les sécurités d'un système quelconque (par exemple dans des réseaux de communication)
SDN	Société des Nations, ancêtre de l'ONU (Organisation des Nations Unies)

TEMPEST	Transient Electro-Magnetic Pulse Emanation STandart. Désigne la norme définissant le taux de radiation qu'un système peut émettre sans compromettre l'information qu'il contient. La désignation officielle pour les équipements d'écoute des systèmes qui ne sont pas à la norme TEMPEST est toujours classifiée. Des auteurs utilisent alors aussi le terme de TEMPEST, avec la signification suivante : Transient Electro-Magnetic PulsE Surveillance Technology.
UNIX	Système d'exploitation, inventé dans les laboratoires Bell vers1970.

Bibliographie

BLANCH95 BLANCHARD Philippe
Pirates de l'informatique
Enquête sur les hackers français
Addison Wesley, 1995

BONA94 BONANATE Luigi
Le terrorisme international
coll. XX^{e} siècle
Casterman, Giunti, 1994

BRANDT95 BRANDT Daniel
Infowar and Disinformation : From the Pentogone to the Net
Octobre 1995
http://www.cs.albany.edu/~ault/security/infowar.html

CARTER92 CARTER David L.
Computer Crime Categories:
How Techno-criminals Operate
FBI Law Enforcement Bulletin, 1992
http://nsi.org/Library/Compsec/crimecom.html

COHEN93 COHEN Frederick B.
Information Warfare Considerations
http://all.net/books/iw/iwardoc.html

COHEN95 COHEN Frederick B.
Protection and Security on the Information Superhighway
John Wiley & Sons, Inc. , 1995

CLOUGH93 CLOUGH Bryan, MUNGO Paul
La Délinquance Assistée par Ordinateur
DunodTech, 1993

DEVOST1 DEVOST Matthew G.
The Digital Threat : United Statee National Security and Computers
http://chelsea.ios.com/~mdevost/hackers4.html

DEVOST95 DEVOST Matthew G.
Political Aspects of Class III Information Warfare
Global Conflict and Terrorism
Janvier 1995
http://chelsea.ios.com/~mdevost/montreal.html

DORAN96 DORAN Serge le, ROSÉ Phillipe
Cyber Thrillers, 35 histoires vraies de la délinquance informatique
Albin Michel, 1996

ENCYCL89 *Encyclopaedia Universalis*
1989

FANNING95 FANNING Paul
Terrorism: Past Present, and Future
http://www.acsp.uic.edu/oicj/pubs/cja/080501.htm

CARIG1 GARIGUE R.
Information Warfare, Developing a Conceptual Framework
http://www.cse.dnd.ca/~formis/overview/iw

GUISNEL95 GUISNEL Jean
Guerres dans le cyberespace. Services secrets et Internet
La Découverte, 1995

HAENI95 HAENI Reto
An Introduction to Information Warfare
Décembre 1995
http://www.seas.gwu.edu/student/reto/infowar/info_war.html

ICOVE95 ICOVE David, SEGER Karl, Von STORCH William
Computer Crime : A Crimefighter Handbook
O'Reilly, 1995
http://www.ora.com/gnn/bus/ora/features/crime/crime1.html

JONES96 JONES Frank
Nowhere to run... Nowhere to hide... The vulnerability of CRT's, CPU's and peripherals to TEMPEST monitoring in the real world
1996
http://www.thecodex.com/c_tempest.html

LAB90_1 Legal Advisory Board,
Commision of the European Communities
Access to public-sector information,
data protection and computer crime.
janvier-février 1990

LAB90_4 Legal Advisory Board,
Commision of the European Communities
Computer crime in the Netherlands
avril 1990

LAROUS83 *Petit Larousse illustré*
1983

LIBICKI95 LIBICKI Martin
What is Information Warfare ?
Août 1995
http://www.ndu.edu/ndu/inss/actpubs/act003/a003cont.html

MUNRO95 MUNRO Neil
The Pentagone's New Nightmare : An Electronic Pearl Harbor
Washington Post, Juillet 95
http://vislab-www.nps.navy.mil/~sdjames/pentagon_nightmare.html

RAND95 *Information Warfare: A Two-Edged Sword*
RAND Corp. , 1995
http://www.rand.org/publications/RRR/RRR.fall95.cyber/infowar.html

RISKS-10.62 *Severed Phone Line Disrupts Chicago Zone*
The New York Times, 16 octobre 1990
Risks Forum Digest, 10.62
http://catless.ncl.ac.uk/Risks

ROUSH92 ROUSH Wade
Hackers: Taking a Byte Out of Computer Crime
1995
http://web.mit.edu/afs/athena/org/t/techreview/www/articles/apr95/Roush.html

SCHWAR93 SCHWARTAU Winn
Terminal Compromise
1993
ftp://ftp.ircom.fr/pub/misc/novel/termcomp.1 .2 .3 .4

SELINE89 SELINE Christopher
Eavesdropping On The Electromagnetic Emanations of Digital Equipements:
The Laws of Canada, England and United States
1989
http://csrc.ncsl.nist.gov/secpub/tempest.html

STERLING92 STERLING Bruce
The Hacker Crackdown,
Law and Disorder on the Electronic Frontier
1992
http://gopher.well.sf.ca.us:70/1/Publications/authors/Sterling/hc

SZAFR1 SZAFRANSKI Richard, Colonel USAF
A Theory of Information Warfare
http://www.cdsar.af.mil/apj/szfran.html

THOMP84 THOMPSON Ken
Reflections on Trusting Trust
Communication of the ACM, Vol 27, No 8, Août 1984
http://www.acm.org/classics/sep95/

THOMPM95 THOMPSON Mark
If War Comes Home
A strategic exercise simulates an info attack on the U.S. and its allies
TIME Magazine, 21 août 1995, Vol. 146, No 8

VOIR1 *Guérilla électronique, la guerre du future*
VOIR, 26 janvier 1995
http://www.lanternette.com/hugo/infowar.html

WALLER95 WALLER Douglas
Onward Cyber Soldiers
TIME Magazine, vol 146, No 8, Août 95
http://ei.cs.vt.edu/~cs3604/fall.95/Hacking/Cyberwar.html

Comme principal outil de recherches sur Internet, j'ai utilisé :

http://www.altavista.digital.com

Index