COLLEGE INTERARMEES
DE DEFENSE

CYBERTERRORISME

Menace, réalité et riposte :

quel intérêt pour les forces armées ?

Mémoire de géopolitique

du Lieutenant-Colonel Alain KERBOULL

dans le cadre du séminaire
"Les menaces non militaires de niveau stratégique"

Directeur : Xavier RAUFER
de l'université Panthéon-Assas, Paris II

Avril 2001

LE CYBERTERRORISME

Sommaire

Introduction

Dans l'actualité mondiale, il ne se passe plus un mois sans que la presse ne fasse état d'actes d'intrusions dans des systèmes informatiques ou de diffusion de virus informatiques causant des pertes d'informations. Cette nouvelle criminalité évolue avec la montée de l'informatisation, non seulement dans les entreprises mais aussi dans les foyers. L'informatique participe aujourd'hui au fonctionnement de nombreuses infrastructures vitales : certaines sont devenues des ordinateurs en particulier les centraux téléphoniques. Dans ce contexte, de nombreuses failles existent et menacent la sécurité des Etats modernes.

Alors que des chercheurs français étudient l'utilisation possible de moyens non conventionnels par des terroristes, comme des armes nucléaires, bactériologiques ou chimiques, certains Etats ont déjà ajouté à ces menaces, le cyberterrorisme, en particulier les Etats-Unis. Des scénarios catastrophes sont établis et laissent à penser qu'une organisation terroriste pourrait 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 1996, Jean GUISNEL, journaliste au « Point », avait déjà traité dans son livre « Guerres dans le cyberespace » de l'intrusion des services secrets dans le réseau Internet et des usages possibles de cette toile planétaire. Aujourd'hui, ces organismes n'hésitent plus à recruter des pirates informatiques afin de s'introduire dans les réseaux adverses. Aussi nous pouvons penser que certains groupes terroristes se sont également équipés et ont recruté le même genre de personnel.

Jusqu'à présent, aucune action d'envergure n'a été révélée et revendiquée par une organisation terroriste connue, mais la multiplicité des attaques informatiques attribuées à des groupes de pirates ne sont-elles pas les prémices de ce cyberterrorisme ?

Face à ce nouveau risque, les pays les plus avancés technologiquement se préparent, cherchent à renforcer leur sécurité et envisagent déjà les ripostes à travers une lutte informatique offensive. Cette dernière pourrait fournir un nouveau type d'armes, intéressant les armées qui pourraient l'utiliser dans la gestion des conflits armés en phase préparatoire à une intervention.

Après avoir abordé l'intérêt des forces armées envers cette menace, nous allons définir le cyberterrorisme et tenter de cerner sa réalité à travers les faits révélés dans les médias. Nous développerons ensuite les solutions étudiées par les différents pays qui se sentent menacés.

1 Notion de cyberterrorisme

1.1 L'intérêt des forces armées : préparation à la Cyberguerre.

1.1.1 Une nécessaire maîtrise de l'information.

Dans l'exercice délicat de la maîtrise de l'information, les armées modernes, tout comme les entreprises, voient l'apparition de nouvelles vulnérabilités tant de leurs systèmes que des systèmes adverses.

Dans une réflexion sur « les engagements futurs des forces terrestres » élaborée par l'Etat-Major de L'Armée de Terre française, les pirates informatiques ou hackers sont cités parmi les nouveaux acteurs capables de transformer le paysage de la guerre : « Se plaçant au service d'organisations étatiques ou de groupes occultes pour des raisons idéologiques ou se donnant au plus offrant, les hackers pourront chercher à agresser nos systèmes d'information opérationnelle et réduire, voire annuler la supériorité opérationnelle que nous attendons demain, alors même que ces systèmes constitueront de plus en plus un centre de gravité de nos forces».

Aussi on peut penser que le cyberespace est devenu un véritable champ de bataille : Les fusils, les balles et le barbelé y sont remplacés par les ordinateurs, les paquets de données et les logiciels de filtrage. James ADAMS dans son livre « La prochaine guerre » a choisi comme sous-titre : « Les Armes sont les ordinateurs et le front est partout ». Les militaires américains sont sensibilisés à ce sujet. A ce titre, Bill CLINTON prononça le discours suivant à l'Académie Navale américaine : « Notre sécurité est de plus en plus mise au défi par des menaces non-traditionnelles de la part d'adversaires, anciens et nouveaux, non seulement des régimes hostiles, mais aussi des criminels et terroristes qui ne peuvent pas nous vaincre sur le terrain de bataille, mais qui néanmoins recherchent des nouvelles façon de nous attaquer en exploitant les nouvelles technologies et la mondialisation».

1.1.2 Création d'unités spéciales et recrutement de hackers[1]

Pour participer à l'effort de sécurité et préparer les opérations informatiques offensives, les armées recrutent. L'Etat-Major de l'armée américaine souhaite enrôler les meilleurs pirates informatiques. A ce titre, Art MONEY, vice-secrétaire d'Etat à la Défense, est intervenu au plus grand rassemblement de hackers au monde baptisé DEF CON 8.0, en septembre 2000 à Las Vegas. Au premier jour de la manifestation, il a invité les pirates informatiques à « rejoindre le gouvernement, ou le secteur privé et à se ranger du côté de la défense ».

[1] Les hackers sont des personnes explorant les limites des systèmes matériels et réseaux d'informatique.

Peu de pays ont annoncé officiellement avoir créé des unités chargées de la guerre informatique. Ces informations restent classifiées. Et contrairement aux armes conventionnelles qui sont montrées à titre dissuasif, ces nouvelles unités avec ses armes sont développées dans le secret, car leur force résidera dans l'effet de surprise causée par une attaque informatique.

Cependant quelques informations sont données à ce sujet. Ainsi on a appris, en décembre 1999, que le gouvernement suédois envisageait sérieusement de créer une unité spéciale « NTIC »[2] au sein de ses forces armées. L'armée suédoise devrait à cet effet former une nouvelle catégorie de militaires, les "IT soldiers" (IT pour Information Technology). Leur mission serait non seulement défensive, protéger les systèmes informatiques gouvernementaux d'attaques extérieures, mais aussi offensive, « détruire » à distance des serveurs ennemis.

Ces nouveaux militaires pourraient changer la face de la guerre. Il faut tempérer tout de même les possibilités de ces équipes qui ne pourront intervenir que dans une phase préliminaire avant une intervention physique qui restera nécessaire avec ses moyens conventionnels.

1.1.3 Des armes informatiques pour une lutte offensive.

La guerre de l'informatique concerne les attaques visant le système informatique adverse et les mesures de protection de ses propres systèmes. Une multitude d'actions peut être menée, allant de l'espionnage au sabotage en passant par la prise sous contrôle de systèmes adverses gérés par l'informatique. En France, le concept de maîtrise de l'information préparé par l'Etat-Major des Armées reste confus sur son contenu. Pour l'instant, la France se défend de préparer une extension de la guerre électronique.

Le Pentagone américain a classé comme prioritaire le recours en temps de guerre aux opérations dites « informationnelles » (Information Operations IO). Ces actions englobent la guerre psychologique, les perturbations électroniques, l'attaque des systèmes de communications ou même l'anéantissement des réseaux informatiques ennemis. La revue « le Monde du Renseignement », du 7 octobre 1999, confirme l'information en annonçant que « le département de la défense américaine a engagé, dans le cadre de la crise au Kosovo, une unité spéciale chargée de la guerre électronique et de la guerre de l'information. Les bureaux du IO avaient pour tâche d'accéder, via leurs ordinateurs, aux réseaux d'informations des infrastructures serbes et de les perturber ». Cependant cette information n'est pas confirmée du côté américain où l'on préfère dire avoir envisagé de pirater le réseau serbe d'ordinateurs mais avoir abandonné le projet en raison des conséquences négatives d'une guerre informatique. Ainsi les chefs militaires américains auraient renoncé à une telle option par crainte qu'une guerre informatique menée sans

[2] NTIC : Nouvelles Technologies d'Informations et de Communications

discrimination n'entraîne des poursuites contre le Pentagone pour crimes de guerre, étant donné la nature non militaire des cibles visées. Les militaires précisent aussi que les systèmes informatiques yougoslaves, rudimentaires ou décentralisés, se prêtaient mal à une telle attaque.

Ce projet américain donne cependant une indication sur la croissance du secteur de l'armement informatique, qui pourrait révolutionner en partie la nature de la guerre.

Certains pays annoncent leur potentiel de riposte dans un but dissuasif. Ainsi le responsable des communications du ministère de la défense de Taïwan a annoncé, à l'agence Reuter en janvier 2000, que « son armée s'est munie d'un arsenal de puissants virus informatiques pour répliquer à toute attaque électronique de la Chine populaire». L'armée taïwanaise a pour cela rassemblé plusieurs virus informatiques afin de les étudier et de contre-attaquer un éventuel assaut informatique.

Le chef des services secrets allemands, August HANNING, a confirmé, en novembre 2000 dans un congrès sur la guerre informatique, que les services de renseignements s'intéressent aux nouvelles technologies et que les armées forment des soldats au piratage informatique. Il a souligné que chaque Etat est en train de mettre au point ses virus pour paralyser les systèmes d'autres pays ou pour les espionner.

Ainsi les virus informatiques devraient de plus en plus faire partie des conflits entre nations. Le seul frein à l'utilisation de cet arsenal reste l'aspect juridique. En effet pour l'instant aucune loi ne permet aux armées de les utiliser, car les militaires pourraient, en fonction de la législation du pays visé, être poursuivis pour crime.

1.2 Définition du cyberterrorisme

La notion de cyberterrorisme est souvent amalgamée à la cybercriminalité. Pour cette dernière le mobile de l'acte peut être le gain pécunier, la vengeance ou autre. Aussi il paraît important dans un premier temps de définir le cyberterrorisme afin de mieux comprendre les actions qui peuvent lui être attribuées.

Le terme « Cyberterrorisme » est apparu dans les années 1980. Barry COLLIN[3], un chercheur de l'Institut pour la Sécurité et le Renseignement en Californie, l'utilisait pour parler d'une convergence entre le cyberespace et le terrorisme. Dorothy DENNING[4], professeur de l'Université de Georgetown, en utilisant cette définition, la complète en expliquant que le

[3] Barry COLLIN de The Institute for Security and Intelligence in California est aussi consultant auprès d'agences fédérales américaines.
[4] Article de Dorothy E. DENING « Activism, Hacktivism and Cyberterrorism : The Internet as a tool for Influency Foreign Policy » Décembre 1999.

cyberterrorisme couvre des opérations de Hacking[5] motivées politiquement et ayant pour but de causer des atteintes graves à la société comme la perte de vies humaines ou de sévères dommages économiques. Elle donne en exemple une intrusion dans le système de contrôle de la navigation aérienne qui causerait une collision entre deux avions.

Nous voyons que le cyberterrorisme vise à causer des atteintes sévères aux sociétés modernes en particulier des dommages économiques à partir du cyberespace. Ce dernier est un monde virtuel constitué de l'ensemble des ordinateurs connectés en réseau.

Mark POLLITT, agent spécial du FBI, précise les cibles visées : « Le cyberterrorisme est une attaque préméditée, politiquement motivée contre l'information, les systèmes d'information, les programmes informatiques et les données, contre des cibles combattantes ou non combattantes, par des groupes subnationaux ou des agents clandestins ».

Le dictionnaire technique et critique des nouvelles menaces de Xavier RAUFER le définit comme une attaque préméditée, par une entité ennemie étatique ou non, des ordinateurs cruciaux d'un pays en vue de les saboter, de les piller, de les détruire ou d'en prendre le contrôle.

En Grande-Bretagne, une nouvelle loi, entrée en vigueur le 19 février 2001, assimile tous les pirates informatiques à des terroristes. La loi « Terrorism Act 2000 »[6] inclut dans sa définition tout acte conçu sérieusement pour gêner ou pour perturber sérieusement un système électronique, avec l'intention d'influencer le gouvernement ou d'intimider la population, selon une cause politique, religieuse ou idéologique, et ce incluant les actions hors Royaume-Uni. Au passage elle ne fait aucune distinction entre les jeunes pirates informatiques « bidouilleurs » et les véritables pirates malveillants, rois de l'intrusion illégale. Cette loi vient en remplacement de la loi de prévention du terrorisme de 1973 (Prevention of Terrorism Act) dont elle étend aux nouvelles technologies les pouvoirs dont dispose la police. Les autorités peuvent ainsi détenir durant 48 heures des personnes suspectées de terrorisme sans justification.

David L. CARTER, spécialiste des délits informatiques de la Michigan State University, donne la définition suivante : « Le cyber-terrorisme consiste essentiellement à placer une bombe d'information pour détruire des données dans un système ou pour fournir des renseignements erronés à ses utilisateurs. Les criminels s'introduiront dans les ordinateurs d'entreprises pour se procurer de l'information sur les produits, des listes de mise en marché et toute autre donnée

[5] Hacking : « hachage » de code, bidouillage des ordinateurs dans le but de s'introduire dans les systèmes informatiques

[6] Texte de la loi britannique Terrorism Act 2000 disponible sur le site Internet www.hmso.gov.uk/acts/acts2000/20000011.htm

ayant une valeur pour la compagnie. Ils menaceront alors de détruire ces fichiers pour obtenir de l'argent. »

Quelle que soit la définition retenue, l'objectif du cyberterrorisme est d'altérer, de neutraliser ou de détruire l'information en tant que valeur stratégique. Au regard de cette définition, quelle est la mesure exacte des menaces et risques émergents auxquels doivent faire face nos sociétés ouvertes ?

1.3 La menace

1.3.1 Vulnérabilité des nouvelles technologies

Le Conseil national de la recherche américaine publiait un article en 1991 sous le titre « les ordinateurs en dangers », il annonçait déjà la vulnérabilité des nouvelles technologies :

« Nous sommes exposés à des risques. Les États-Unis dépendent des ordinateurs. Ces derniers contrôlent l'alimentation en énergie, les communications, l'aviation et les services financiers. Ils servent à archiver des informations vitales, telles que les dossiers médicaux, les plans commerciaux et les casiers judiciaires. Malgré la confiance que nous leur faisons, ils sont vulnérables : vulnérables aux défauts de conception et à l'insuffisance du contrôle de la qualité, vulnérables aux accidents et, peut-être est-ce là le point le plus alarmant, vulnérables aux attaques intentionnelles. Le brigand moderne peut voler davantage muni d'un ordinateur que d'une arme. Le terroriste de demain sera peut-être capable d'infliger plus de dommages à partir d'un clavier qu'au moyen d'une bombe. »

Les services de sécurité et de renseignement, à travers le monde, constatent aujourd'hui que tout pays qui utilise les nouvelles technologies est vulnérable au cyberterrorisme. Ils affirment que les terroristes d'aujourd'hui ont accès à la télédétection spatiale ainsi qu'à l'imagerie par satellite, leur permettant de pénétrer des sites autrement inaccessibles ou d'évaluer les failles en matière de sécurité des installations militaires, nucléaires et autres. Aussi toutes les infrastructures vitales dont le fonctionnement ou la gestion repose sur un système informatique, voire électronique, peuvent être prises pour cible.

Cette vulnérabilité peut ainsi être exploitée par le cyberterrorisme. Son action est facilitée par des instruments technologiques lui permettant d'agir aussi sous couvert d'anonymat et de manière imprévisible.

1.3.2 Caractéristiques des cyberattaques

Le cyberterrorisme dérive du terrorisme. A ce titre nous pouvons définir brièvement la menace terroriste comme regroupant toutes les actions concourant à déstabiliser l'ordre établi. Les

actions entrant dans cette catégorie peuvent avoir un caractère violent ou plus insidieux comme l'intoxication et la désinformation par détournement ou manipulation d'information, les perturbations engendrées dans un système et susceptibles de déclencher des troubles sociaux latents, etc.. Les auteurs recherchent un résultat spectaculaire et les effets médiatiques qui l'accompagnent.

Barry COLLIN, l'inventeur du terme cyberterrorisme, explique : « D'ici 5 à 10 ans, nous penserons que les terroristes des années 80 et 90 étaient vraiment primitifs, parce qu'ils employaient des bombes et des armes à feu pour tuer des gens. La mort de quelques personnes dans une explosion n'a pas encore obligé un gouvernement a changé radicalement de politique. Mais qu'en serait-il si les terroristes parvenaient à affecter des dizaines de milliers de personnes ? Vous avez alors une panique qui se diffusera réellement ».

Les groupes qui commettent ce genre d'action disposent en général de moyens financiers importants et de complicités leur permettant d'envisager pratiquement tout type d'attaque sur des systèmes en particulier sur ceux relevant de l'appareil de sécurité de l'Etat.

Dans le n°51 de la revue Perspectives Stratégiques[7], Marc BOUVIER[8] explique que les actions cyberterroristes présentent deux degrés de gravité. Le premier consiste en une opération de déstabilisation. Il s'agit de paralyser partiellement un système d'information. Cette neutralisation peut s'avérer temporaire afin d'affaiblir le système visé, ou permet de s'y introduire dans le but de l'utiliser, ou pour y déposer des composants spécifiques : des cookies[9] (fichier traces), un cheval de Troie, des traceurs électroniques, etc.. Le second degré porte sur la destruction totale d'un système de protection et sort du domaine de l'intimidation et de l'espionnage, pour rentrer dans une manifestation physique caractérisée. Le résultat recherché et l'intensité de l'agression sont alors l'expression de la revendication cyberterroriste.

Les cyberterroristes peuvent ainsi mener différents types d'actions contre les systèmes d'information. Il est intéressant à ce stade d'étudier les méthodes employées afin de comprendre combien certaines infrastructures deviennent aujourd'hui vulnérables.

1.3.3 Les différentes formes d'attaques

Les spécialistes du cyberterrorisme classent les actions contre un système d'information en trois types, l'attaque physique, syntaxique ou sémantique.

[7] Perspectives Stratégiques est une revue électronique de la Fondation pour la Recherche Stratégique.
[8] Marc BOUVIER est un consultant spécialiste du cyberterrorisme.
[9] Les "cookies" sont des petits fichiers de traces qui s'enregistrent sur les ordinateurs et permettant de repérer les internautes. Cette pratique utilisée dans le secteur du commerce électronique pour conserver le détail des articles commandés commence à être décriée, car elle porterait atteinte à la vie privée des internautes.

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.

Dans une attaque sémantique, l'agresseur insère des données dans un système d'information pour le faire dysfonctionner ou le piéger en l'obligeant à exécuter des opérations non autorisées. Le simple fait de diffuser des informations de propagande ou des informations erronées est considéré comme une forme d'attaque informatique. Des formes plus sophistiquées d'attaques peuvent être la manipulation des fichiers de la cible visée, le brouillage de ses transmissions radio ou de ses détecteurs voire le débordement d'un site Internet par l'envoi massif de messages entraînant un « déni de service »[10]. Ce dernier type d'action est souvent le fait des hackers. Ce sont les spécialistes de l'intrusion dans les systèmes informatiques.

1.3.4 Le Hacking ou l'intrusion dans les systèmes

Pour perturber un système, il faut en premier lieu y pénétrer. Les hackers cherchent, à travers les réseaux ouverts sur l'extérieur comme Internet, des serveurs et ordinateurs vulnérables parmi les entreprises et les universités. Ils peuvent ensuite pénétrer ces ordinateurs en y installant un logiciel « esclave » qui attend leurs instructions. Ils peuvent ainsi prendre le contrôle d'un système d'information, le perturber, refuser son utilisation, voler des ressources ou des informations importantes ou observer clandestinement le système informatique.

Aujourd'hui, l'équipement des foyers en ordinateur et en modem permet à presque n'importe qui de se lancer dans cette aventure. Les connaissances et outils techniques requis ne sont pas trop difficiles à obtenir sur le Web. Un regroupement de hackers appelé « Electrohippies »[11] a même annoncé son intention de rendre accessible tous les logiciels nécessaires à une attaque de type « déni de service ».

Dans ce type d'action, le hacker, après avoir pris le contrôle de serveurs relais, émet à leur intention un signal nécessitant une réponse. Leur réponse n'est pas redirigée vers le hacker mais au contraire, il crée « une adresse de retour » qui oriente les réponses vers les sites victimes. Le site attaqué est submergé de fausses réponses de centaines d'ordinateurs qui encombrent le système et le rendent inaccessible.

[10] Déni de service: Impossibilité d'accès à des ressources pour des utilisateurs autorisés ou introduction d'un retard préjudiciable dans les opérations.

1.3.5 Les attaques par le biais de logiciels

Les attaques par le biais de logiciels sont en général très sophistiquées. Les programmes utilisés pénètrent non seulement les systèmes ciblés mais y effectuent surtout des opérations agissant sur leur fonctionnement. Les formes les plus pointues d'attaques par le biais de logiciels agissent de telle sorte que ceux-ci ne peuvent être détectés. Ils peuvent même effectuer des contre-mesures s'ils rencontrent des tentatives de protection du système ciblé. Les formes les plus connues d'attaques de software sont les virus d'ordinateurs. Il existe aussi des programmes informatiques qui installent des « portes », appelées aussi cheval de Troie, permettant l'accès aux intrus de manière continue et permanente.

1.3.6 Chantage et objectifs économiques

Les chantages existent aujourd'hui dans le domaine informatique. Des hackers menacent de paralyser les activités d'une entreprise ou organisation, à moins qu'une somme ne leur soit versée. Les organisations terroristes peuvent y voir un moyen de relever les fonds financiers nécessaires à leur fonctionnement. Nous sombrons alors dans le domaine du terrorisme économique.

1.3.7 Recrutement de hackers par des organisations terroristes.

Les hackers sont aujourd'hui recherchés sur le marché de l'emploi. L'agence Reuter, dans une dépêche du 4 février 2000, explique que les experts en informatique ont assisté à la naissance d'un marché des pirates sur Internet : « Les sociétés souhaitant pénétrer dans les ordinateurs d'un concurrent ne prennent pas le risque de le faire elles-mêmes et recrutent, elles aussi, des pirates professionnels pour faire le sale boulot à leur place. »

Certains essaient déjà de monnayer leur savoir auprès d' Etats-Voyous. Pendant la Guerre du Golfe, selon des fonctionnaires du Pentagone, un groupe de hackers hollandais aurait proposé à l'Irak de perturber le déploiement militaire des Etats-Unis au Moyen-Orient pour un million de dollars. Saddam HUSSEIN aurait rejeté l'offre. Selon Steve KENT, un expert privé en sécurité informatique et membre d'un comité consultatif du Pentagone sur la guerre de l'information, le potentiel de nuisance était bien réel. En effet pendant la Guerre de Golfe, les militaires américains ont eu une utilisation intensive d'Internet pour leurs communications, ils en auraient certainement souffert si les Irakiens avaient accepté cette proposition.[12]

Par le passé, il n'y avait pas d'intérêt pour les terroristes de se former à l'informatique. Cela a très vite évolué. Aujourd'hui plus de 60% des diplômes universitaires dans le domaine

[11] Groupe « Electrohippies » site Internet www.gn.apc.org/pmhp/ehippies/
[12] Article du TIME Magazine du 21 août 1995, "Onward Cyber Soldiers"

informatique sont attribués aux étudiants de pays en voie de développement dont une grande majorité de pays musulmans. Alors que les organisations étatiques recrutent des pirates informatiques, il est légitime de penser que des groupes terroristes, qui ont des difficultés à former leurs propres pirates informatiques, recherchent, elles aussi, leurs spécialistes de l'intrusion à distance. Des organisations, telles que l'ETA, l'IRA ou le GIA, sont d'ailleurs déjà présentes sur Internet pour y effectuer de la cyberpropagande[13]. John DEUTCH, ancien directeur de la CIA, a affirmé que le Hezbollah avait déjà la possibilité de porter des cyberattaques.

1.3.8 Cyberconflits entre Etats

La menace dépasse aujourd'hui la seule action terroriste d'un groupe isolé. Les actes de cyberterrorisme peuvent aussi être le fait d'un Etat, cela s'appelle alors un cyberconflit. Ce type d'attaque est pris particulièrement au sérieux depuis 1995 par les Etats-Unis qui évoque cette menace sous le vocable de Pearl Harbour Electronic.

Ainsi les risques de sabotage de sites sensibles d'un pays par une organisation, voire un Etat ennemi, ne sont pas non plus exclus. En 1998, le Pentagone américain avait essuyé une cyberattaque inédite, lorsque des pirates étaient parvenus à pénétrer ses ordinateurs. Certains pays y voient un moyen de rivaliser avec les puissances atomiques.

En 1999, Taïwan a officiellement accusé la République populaire de Chine d'avoir tenté à 60 reprises de pénétrer ses systèmes informatiques.

Ainsi le phénomène de cyberconflit serait en voie d'expansion.

1.4 Cibles privilégiées : Des scénarios catastrophes.

1.4.1 Les infrastructures vitales

Afin d'illustrer la menace cyberterroriste, il est intéressant de parcourir un scénario élaboré par le docteur Andrew RATHMELL dans un article publié dans le journal du Royal United Service Institute en octobre 1997 :

« L'Armée républicaine irlandaise (IRA) préfère frapper là où ses coups risquent de faire le plus mal, histoire de forcer les troupes britanniques à quitter l'Irlande du Nord. Ses cibles ont donc été, pour la plupart, économiques et industrielles.

Plutôt que de continuer à risquer la vie de ses membres pour frapper une seule cible, et plutôt que de continuer à risquer de s'attirer l'opprobre populaire en tuant des victimes innocentes, l'IRA décide de changer de tactique et lance une vaste offensive cybernétique qui

[13] Le Hezbollah a également son site Internet : www.hizbollah.org

frappe simultanément, disons, British Telecom, Railtrack et la Banque centrale de Londres. Les dégâts sont incalculables et la publicité générée, massive. Et tout ça sans aucune perte de vie et avec des risques minimes. »

A travers ce scénario, nous pouvons penser que certaines infrastructures comme les réseaux de transport ou de télécommunications peuvent être la cible du cyberterrorisme. Les infrastructures vitales d'un pays comprennent les moyens de télécommunication, les réseaux de distribution (eau, électricité, gaz ou pétrole), les services d'urgence, les moyens de transport, les services gouvernementaux et l'armée. Ainsi, les cyberterroristes disposent de cibles plus importantes car stratégiques, devenues accessibles par des réseaux qui peuvent être piratés à distance. De plus la privatisation de certaines infrastructures comme les télécommunications ne facilite pas l'harmonisation des moyens de sécurité. De nombreux pays prennent conscience de l'importance de la menace qui pèse sur leurs réseaux et points sensibles.

Ainsi lors d'un congrès sur « la guerre de l'information » qui s'est tenu le 1er novembre 2000 à Munich, August HANNING, chef des services de renseignements fédéraux allemands, a estimé que l'Allemagne est de plus en plus menacée par le manque de sécurité qui règne sur ses réseaux informatiques. Il a ajouté : « De l'approvisionnement énergétique du pays en passant par le transport aérien, la société allemande est de plus dépendante de système d'informations mal sécurisé et se trouve ainsi à la merci d'attaques informatiques de services secrets étrangers ou de groupes fondamentalistes ».

1.4.2 Exemple: Les télécommunications, cible hautement vulnérable

Du fait de leur ouverture propre à leur mission, les réseaux de télécommunications sont particulièrement vulnérables. La complexité des systèmes modernes laisse apparaître un plus grand nombre de failles dans la sécurité de ces systèmes.

Le 3 mai 2000, une panne du réseau téléphonique avait affecté environ la moitié des abonnés de France-Télécom en région parisienne soit plus de deux millions de personnes. France-Télécom avait annoncé que cette panne avait touché un nœud de leur réseau appelé point de transit de signalisation. Une journée après la perturbation, le porte-parole avouait ne pas connaître avec certitude l'origine de la panne et estimait qu'elle serait plutôt de nature logicielle. Nous pourrions penser que cette panne aurait pu être la conséquence d'une cyberattaque ! D'autant plus que quelques semaines plus tard, une nouvelle panne touchait tous les appels passés vers les numéros Verts, Azur et Indigo de France-Télécom. Ces perturbations illustrent bien la vulnérabilité des réseaux de télécommunication.

La connectivité d'Internet, c'est-à-dire la possibilité de joindre deux individus situés à deux points opposés de la planète, en fait aussi sa faiblesse puisque qu'un saboteur peut garder son anonymat tout en pénétrant un site protégé. La source de certains des problèmes de sécurité provient de l'architecture de base du réseau Internet. Développé aux Etats-Unis par le département de défense il y a trente ans, l'Internet était destiné à des usagers connus, et non au grand public, pour partager des informations. De nombreuses mesures pour sécuriser le réseau sont simplement des ajouts à un système déjà ancien. Selon Bruce SCHNEIER, technicien en chef de Counterpane Internet Security Inc., « le système se dégrade plus rapidement que nous sommes en mesure de le sécuriser ». Ainsi Internet, principal vecteur des attaques, pourrait en être également la cible.

1.4.3 Un autre exemple : Les transports

Les transports modernes terrestres ou aériens sont gérés par des systèmes de supervision fortement informatisés. Les transports ferroviaires connaissent des accidents très graves à la suite soit d'erreur humaine dans la gestion de la signalisation mais aussi de l'aiguillage. Ces fonctions informatisées, mises en œuvre à travers des réseaux de télécommunications, peuvent, très certainement, être piratées.

Un rapport de la commission américaine sur la sécurité nationale, publié en septembre 1999, faisait état d'une menace terroriste grandissante contre les Etats-Unis. Ce rapport de 143 pages auquel ont participé 25 experts de plusieurs administrations américaines confirme la possibilité d'une cyberattaque contre les contrôles aériens et conclut qu'il est assez facile de pirater des systèmes.

Alors que les transports aériens font un usage de plus en plus intensif du système de localisation GPS, la revue britannique New Scientist a rapporté dans son édition d'avril 2000 que les communications par satellites, y compris les transmissions militaires et les systèmes de localisation type GPS, pouvaient être totalement brouillées avec un peu de matériel électronique trouvé en magasin, grâce aux recettes disponibles sur l'Internet. En effet l'armée de l'air américaine en avait fait la démonstration pratique : une équipe de l'US Air Force avait été chargée de détecter les failles de sécurité des systèmes de transmission par satellites et il lui avait suffi de taper sur un moteur de recherche Internet les mots-clés « brouillage des communications satellites » pour récolter quantité d'informations. A titre de test, le chef de cette équipe avait chargé deux ingénieurs novices de l'US Air Force de construire un engin de brouillage « maison », uniquement en utilisant l'Internet et tout ce qu'ils pouvaient acheter en liquide. Le résultat était alarmant : pour 7.500 dollars, ils avaient fabriqué un appareil à ultra hautes fréquences, générateur d'un "bruit" électronique capable de brouiller des antennes satellites et des récepteurs militaires.

Les transports publics ont toujours été des cibles privilégiées des terroristes. Leurs vulnérabilités techniques les destinent malheureusement à le rester pour les futurs cyberterroristes.

* * *

Ainsi le cyberterrorisme peut attaquer voire détruire les systèmes informatiques liés au fonctionnement des infrastructures vitales d'un pays. La menace existe et les hommes capables de mener de telles actions s'entraînent librement tous les jours. Jusqu'à maintenant, aucune attaque cyberterroriste d'envergure n'a été révélée, mais la multiplicité des attaques informatiques nous rapproche d'une réalité inquiétante.

*

* * *

*

2 La réalité mondiale: les symptômes d'un mal annoncé

David MARTIN[14], dans une conférence-débat sur le crime informatique et la cyberguerre, classe l'attentat du World Trade Center, à New York le 26 février 1993, comme le seul cas recensé de cyberterrorisme à ce jour. En effet la destruction des réseaux informatiques de cet immeuble de Manhattan a provoqué une paralysie importante de l'économie américaine. Les pertes dues à cet attentat ont été estimées à plus de 700 millions de dollars.

Nous avons vu que les systèmes d'information sont vulnérables. Une catastrophe reste possible. Si elle n'est pas encore arrivée, nous pouvons penser qu'il y a un début à tout. Aujourd'hui nous n'assistons qu'à des attaques isolées. Or il est important de les analyser car les statistiques suggèrent qu'un grand nombre d'attaques aura eu lieu avant qu'une attaque d'importance ne se produise.

2.1 Quelques statistiques

Des structures appelées CERT (Computer Emergency Response Team) ont été mises en place aux Etats-Unis, dès le début des années 1990, suite à des incidents de sécurité de grande ampleur survenus à cette époque sur les réseaux américains de la recherche. Dans les années qui ont suivi, des CERTs ont été installés dans la plupart des autres pays dans lesquels l'Internet s'est développé. Aujourd'hui ces centres reçoivent les déclarations d'incidents informatiques et permettent ainsi de suivre le phénomène. Un centre de coordination CERT/CC[15], basé à l'université de Carnegie Mellon aux Etats-Unis, est chargé de tenir les statistiques mondiales.

Les chiffres présentés par cette organisation ne reflètent qu'une partie du phénomène. Cependant, les incidents remontés au CERT ont un niveau relativement grave.

Années	1988	1989	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999*	2000
Incidents	6	132	252	406	773	1334	2340	2412	2573	2134	3734	9859	21756

Total des incidents déclarés (1988-2000): 47711

Nous pouvons noter que, depuis 1997, le nombre d'incidents double tous les ans. En France, sur le réseau RENATER utilisé pour la Recherche, la Technologie, l'Enseignement et la Culture, les responsables sécurité avouent 5 ou 6 problèmes graves, la prise de contrôle d'un ordinateur, et 50 à 70 incidents plus bénins par mois. En 2000, la police française a traité une centaine d'affaires liées à des intrusions sur des réseaux.

[14] Daniel Martin est commissaire divisionnaire, directeur sécurité de l'OCDE et fondateur du Cybercriminstitut.
[15] Le CERT/CC fournit les statistiques sur son site www.cert.org, un document analysant les incidents de sécurité sur l'Internet entre 1989 et 1995 est disponible à la même adresse.

Dans une synthèse sur les vols d'information dans les entreprises américaines, les consultants du cabinet Michael Kessler & Associates estiment que 35% de l'information dérobée résultent d'actes de malveillances imputables à des employés, sans qu'ils agissent obligatoirement pour des adversaires. 28% proviennent de hackers qui réussissent à pénétrer les réseaux informatiques mais opèrent sans mobile particulier. 28% trouvent leur origine dans des opérations menées par des concurrents américains, et 11% dans des opérations réalisées pour le compte d'entreprises étrangères. Ainsi le risque pour les entreprises n'est pas seulement exogène mais aussi endogène.

Les statistiques montrent également que les pirates informatiques amateurs représentent à ce jour la plus grande menace pour le réseau l'Internet. Ils sont responsables d'environ 90 % des incidents informatiques. 10% est attribué à des pirates professionnels.

2.2 Les attaques les plus médiatisées

Certaines attaques informatiques ont connu une médiatisation sans précédent depuis que l'Internet s'est popularisé. Il devient le terrain de jeu de plus en plus prisé des hackers au fur et à mesure que le commerce électronique se développe et que des informations sensibles y circulent.

2.2.1 L'attaque de février 2000 sur les sites américains de Yahoo! et Amazon

Le lundi 7 février 2000, le géant de l'Internet Yahoo! a été victime d'une attaque de grande envergure de type « déni de service »[16] qui a bloqué son service pendant près de trois heures, soulignant la fragilité de ces sites face à la détermination des pirates informatiques. Les serveurs du portail, installés en Californie, ont été subitement pris d'assaut par un flux énorme de demandes d'information, venus d'une cinquantaine d'adresses Internet, auxquels ils n'ont plus réussi à répondre, un signe évident que le manipulateur utilisait des ordinateurs dispersés pour mener son attaque. Submergé, le site, qui a accueilli 120 millions de visiteurs uniques en décembre, s'est alors brutalement effondré, paralysant surtout la consultation aux Etats-Unis. Seuls certains services, comme le courrier électronique, ont été épargnés. En seulement 10 minutes, tous les internautes surfant sur le site virent s'afficher sur leurs écrans des messages d'erreur. Le serveur informatique californien était envahi par d'immenses vagues d'informations, il recevait par seconde l'équivalent de données perçue en période normale pendant une semaine.

[16] Le « Distributed Denial of Service » (DdoS) consiste à rendre une ressource inaccessible par saturation ou par destruction. Cette attaque est souvent réalisée par un envoi massif de requêtes. Deux techniques d'attaques communément appelée « Smurf » et « Syn Flood » sont possibles. L'une comme l'autre consistent à inonder de demandes de connections l'ordinateur, appelé serveur, permettant d'accéder à un site Internet. Dans la technique du « Syn Flood », ces demandes sont assorties d'une adresse d'origine qui est fausse, ce que les experts appellent le « spoofing », augmentant la confusion du serveur, suivi de son engorgement voire de son arrêt. Des programmes comme TFN, TFN2K, Trin00 ou Stacheldraht sont conçus spécialement pour réaliser ce type d'attaque et sont totalement disponibles sur Internet.

Cette première tentative délibérée de vouloir fermer le réseau s'est poursuivie dans la même semaine sur d'autres grands sites américains. Les sites du portail ZDnet et du courtier boursier Datek Online, Buy.com (commerce en ligne), eBay (enchères), CNN.com (information) et le géant de la distribution sur Internet Amazon.com ont été l'objet d'attaques informatiques, le mercredi 9 février. Cette attaque s'est déroulée au moment même où la bourse américaine ouvrait pour sa séance officielle. Le site a été difficilement accessible entre 14h35 et 15h05 GMT, a expliqué Mike DUNN, porte-parole du quatrième courtier boursier en ligne américain. E-Trade, autre site de courtage en ligne avec 1,5 millions de comptes, a également été l'objet d'une attaque peu avant 11h00 GMT avec de grandes difficultés d'accès pour les clients. Le tort économique causé par ces attaques n'a pas été communiqué. Les seuls réels préjudices subis ont été un retard dans les transactions et peut-être l'évasion de quelques clients vers des sites concurrents. Cependant des chiffres ont été avancés, mais il existe un réel décalage en fonction des sources. Selon la police montée canadienne, l'attaque aurait coûté plusieurs centaines de millions de dollars, alors que certains médias parlaient même d'un milliard de dollars. En prenant les chiffres d'affaires des quatre plus gros sites touchés, ce chiffre tombe à 3,9 millions de dollars pour trois heures de manque à gagner.

L'incident a été jugé suffisamment grave pour que le président américain Bill CLINTON convoque une réunion d'urgence sur la sécurité informatique et déclenche une enquête du F.B.I.. Ces événements ont entraîné de fortes perturbations sur le marché des valeurs de haute technologie, le Nasdaq. Ainsi cette attaque peut être considérée comme une démonstration de force de pirates isolés, d'un groupe idéologique désirant s'attaquer aux entreprises américaines de commerce électronique ou même éventuellement d'un groupuscule ayant des intérêts boursiers. Certains spécialistes ont souligné que l'attaque par saturation qui visait les serveurs de Yahoo! coïncidait avec le vote du budget du F.B.I. au congrès américain.

Cependant l'enquête du F.B.I. appuyé par la Gendarmerie Royale du Canada a permis de mettre en cause un hacker surnommé Mafiaboy. Ce Montréalais de 15 ans aurait mené les attaques contre le site de CNN et se serait vanté de son exploit sur un forum de discussion Internet fréquenté par des hackers. Ainsi pour la police, cette affaire importante serait seulement le fait d'un jeune adolescent isolé.

2.2.2 Le virus « I Love You » parcourt le monde en une journée.

Une autre affaire a été particulièrement médiatisée en mai 2000.

Le jeudi 4 mai 2000, le virus ILOVEYOUa paralysé de nombreux systèmes de courrier électronique dans le monde, comme ceux du Congrès américain, de la Chambre des communes

londonienne, et de grands groupes comme Ford, un an après la panique causée par le virus MELISSA. L'Europe, notamment la Grande-Bretagne, l'Allemagne, la Suisse, la France et le Danemark, a été la deuxième région la plus touchée. Le virus pourrait avoir touché 10 millions d'ordinateurs dans le monde. Ce virus appartient au genre « ver de terre »[17]. Une première version identifiée de ce type de virus avait déjà perturbé, en juin 99, les services de courrier électronique de nombreuses sociétés. La dernière version renvoyait des informations vers un site aux Philippines. Les enquêteurs de ce pays ont soupçonné une jeune femme d'être le pirate qui a diffusé ce virus dans le monde entier.

Ce cas montre la vulnérabilité et les faiblesses de la sécurité informatique des entreprises qui, plusieurs mois après l'identification d'un nouveau virus, n'ont pas protégé leurs ordinateurs.

2.3 Les cyberattaques concernent presque tous les continents

Après ces deux cas particulièrement médiatisés, parcourons le monde à la découverte de quelques incidents relatés par les agences de presse AFP, AP et Reuter, au cours des deux à trois dernières années. Cela nous permettra de mieux localiser l'origine, la destination ainsi que la nature de ces cyberattaques. Ce cyberterrorisme ne connaît pas de frontière.

2.3.1 L'Amérique

Les Etats-Unis

Tous les organismes officiels américains ont été victimes d'attaques de la part de hackers. La Maison Blanche n'échappe à la règle. Le 12 mai 1999, le site Internet de la présidence a été piraté par des hackers localisés à Hong Kong. Ils y ont laissé des cybergraffitis dénonçant le bombardement de l'ambassade de Chine à Belgrade.

Le Pentagone est particulièrement visé. En mars 1999, ce sont ses serveurs Web qui font l'objet d'attaques systématiques. Les traces de connexion pointent vers la Russie, mais cela ne veut pas dire que les pirates étaient en Russie. C'est devenu un défi de s'introduire dans les systèmes de défense du pays le plus puissant. Le jeu est tellement pratiqué que, le 8 août 2000, le directeur de la sécurité du Pentagone a demandé publiquement aux hackers de toute nationalité d'arrêter de s'en prendre à ses systèmes informatiques afin de pouvoir se concentrer sur les

[17] Un ver (worm) peut se transmettre rapidement et détruire certains fichiers d'une machine infectée. Le virus arrive sous forme d'un courrier électronique portant dans la ligne du sujet « ILOVEYOU ». Il ne se propage qu'une fois que le destinataire a ouvert le contenu du message, et uniquement si la victime utilise le logiciel de courrier électronique Microsoft Outlook, avec un système d'exploitation Windows. Dans ce cas il va infecter la liste des destinataires contenus dans le logiciel de courrier. Le volume de courrier ainsi envoyé risque d'engorger les réseaux informatiques. Le virus cherche aussi dans l'ordinateur de la victime certains fichiers qu'il va réécrire avec son propre contenu. Il peut ainsi détruire des fichiers contenant des images ou du son, et infecter ceux renvoyant à des pages internet.

attaques en provenance d'adversaires « sérieux ». En 1999, le Pentagone avait détecté 22144 incidents informatiques.

La NASA, symbole de la puissance technologique des Etats-Unis, connaîtrait des défaillances dans la protection de ses systèmes informatiques. Le 3 juillet 2000, un responsable de l'agence a annoncé qu'un pirate informatique avait mis en danger l'équipage de la navette spatiale américaine en attaquant les ordinateurs de la NASA en 1997. Le pirate aurait surchargé les systèmes informatiques contrôlant notamment l'état de santé des astronautes. Des hackers opérant à travers un serveur en Suède auraient aussi volé, en décembre 2000, les codes sources d'un logiciel de guidage de missiles qui doit équiper une station de contrôle du système NAVSTAR. La NASA a été victime de plus de 500 000 attaques en 1999.

Les sites du FBI, du Sénat et de l'US Army sont eux aussi régulièrement attaqués. Le site du Sénat américain a été attaqué par deux fois, le 28 mai 1999 et le 11 juin 1999, alors que sa sécurité avait été renforcée après la première attaque.

En octobre 2000, Microsoft annonçait qu'un pirate s'était introduit dans son réseau informatique commettant un acte d'espionnage industriel. Le pirate a passé les défenses de Microsoft avec un simple virus pourtant connu du type cheval de Troie. Les autorités américaines s'inquiètent et expliquent que le piratage du réseau interne de Microsoft fait peser un risque insoutenable sur l'intégrité des réseaux gouvernementaux américains. Trois mois plus tard, cette société a été victime d'une attaque du type « déni de service ». Des pirates ont réussi à bloquer l'accès à certains sites Microsoft pendant quelques heures.

Un incident grave mais très peu médiatisé est intervenu à la fin de l'année 1998 ou au début de l'année 1999 au laboratoire américain de recherche sur les armes nucléaires de Los Alamos. Le Washington Post a révélé le 12 juin 2000 que des pirates soupçonnés de travailler pour la Chine sont parvenus à voler des informations sensibles. En divulguant cette information, les Etats-Unis mettent en relief que « des gouvernements étrangers cherchent toujours à se procurer des armes nucléaires américaines » et focalisent leur communication sur le cyberterrorisme. Quels intérêts ont les Américains de dramatiser le sujet ? Nous essaierons d'y répondre dans la dernière partie de ce document.

Le Brésil : Les Etats-Unis ne sont pas les seuls touchés. Le 21 novembre 2000, un pirate informatique s'est introduit dans le courrier électronique du président brésilien Fernando Henrique Cardoso et a envoyé plusieurs dizaines de courriers électroniques aux autorités fédérales sous cette identité.

2.3.2 L'Europe

L'Europe est concernée aussi par les cyberattaques. Cependant les faits sont moins médiatisés. En Europe occidentale, la Belgique, l'Italie et l'Espagne sont touchés officiellement et des communiqués de presse en font état.

Espagne : En juillet 1999, un pirate informatique espagnol de 22 ans a été arrêté pour s'être introduit dans le réseau informatique du ministère de l'Intérieur afin d'y voler des données. Le jeune homme avait forcé les protections des ordinateurs et tenté, sans succès, de détourner des informations confidentielles vers une adresse de courrier électronique gratuit dont il disposait auprès d'une importante société informatique de Californie. En août 1999, un groupe de pirates informatiques, sous le nom d'Alliance Z3, s'était aussi introduit sur le site Internet de la présidence du gouvernement espagnol pour y critiquer sa politique, caricaturant au passage la photo du chef de l'exécutif.

Belgique : Les banques sont des cibles vulnérables notamment avec la mise en service des banques à domicile. En août 1999, un pirate informatique Belge a réussi à violer le secret de certains comptes bancaires de la première banque du pays, la Générale de Banque. Le pirate était parvenu à consulter des informations en principe confidentielles relatives aux comptes bancaires de clients qui utilisent le système Internet de "banque à domicile". Il s'agissait de numéros de compte, de mots de passe et de numéros d'identification.

Suisse : Le cyberterrorisme vise les intérêts économiques. Les pirates défient le marché économique. Fin janvier 2000, ils ont défié les dirigeants mondiaux en s'introduisant dans les systèmes informatiques du Forum économique mondial à Davos. Ils se seraient procurés des informations confidentielles telles que des numéros de carte de crédit appartenant à des membres du Forum et à des personnalités invitées. Une copie de ces informations avait été transmise par les hackers à un journal suisse.

Italie : Les administrations étatiques font l'objet des défis lancés entre pirates. En février et mai 2000, un groupe se présentant sous le nom « Cyber Fuckers » a lancé une attaque contre les sites Internet de trois ministères italiens, Santé, Transport, Agriculture ainsi que celui de la Cour des comptes. Ils ont simplement modifié la page d'accueil par un message de propagande.

Rien n'arrête les pirates. Le Vatican est aussi une cible idéologique pour certains hackers. Le site Internet du Comité central pour le Jubilé a été paralysé, en novembre 2000, par la diffusion d'un virus qui paralyse les logiciels. De même en janvier dernier, un groupe de jeunes pirates brésiliens a revendiqué une attaque contre le site de Radio Vatican.

Comme dans le terrorisme conventionnel, les cyberterroristes n'hésitent plus aujourd'hui à revendiquer leurs actions.

Europe de l'Est : Les conflits existant entre les peuples sont aussi à l'origine des motivations de certains groupes de hackers qui souhaitent défendre leurs idées. Le 30 août 1999, des pirates informatiques russes ont attaqué et neutralisé les deux principaux sites Internet qui diffusaient les idées des séparatistes islamistes venus de Tchétchénie.

Dans ces pays en marge de l'économie de marché, les sites occidentaux de commerce électronique sont sources de convoitise. Par nature connectés au réseau Internet, ces sites sont accessibles depuis des pays comme la Russie et l'Ukraine. Ainsi pendant l'année 2000, des groupes organisés n'ont pas hésité à pirater plus de quarante sites de commerce électronique américains. Ils seraient parvenus à voler au passage au moins un million de numéros de cartes de crédit.

Yougoslavie : Les pays à peine sortis de crise peuvent être la cible des hackers. La cyberpropagande voire la désinformation reste l'objectif de certains pirates. En juillet 2000, le site Internet de Politika, principal quotidien pro-gouvernemental de Yougoslavie, a été victime d'une attaque. Un faux article annonçant la mort du président serbe Slobodan MILOSEVIC dans un attentat à la bombe a été publié sur ce site.

Roumanie : La Roumanie n'est pas en retard dans le domaine de la criminalité informatique. La police de Timisoara a interpellé et écroué, le 27 septembre 2000, un pirate informatique qui faisait chanter une société américaine après avoir pénétré par effraction dans son réseau informatique et voler des données confidentielles sur ses clients. Il avait par la suite contacté les patrons de la compagnie pour leur demander 5.000 dollars, menaçant dans le cas contraire de révéler que le système informatique de la société était peu sûr. Les pirates ont compris que la sécurité est un enjeu important pour les sociétés qui ne souhaitent pas communiquer sur leur faiblesse. De plus le gouvernement roumain, qui estime que les cyber-pirates nuisent à l'image de son pays, a engagé une coopération étroite avec le FBI américain.

Tchécoslovaquie : Le site du ministère tchèque de l'Intérieur et de la police n'a lui aussi pas échappé à l'attaque des pirates. Le 6 décembre 2000, les pirates ont mis sur le site un message ironique en allemand. Ils auraient pu également accéder aux courriers électroniques des fonctionnaires.

Bulgarie : Le site de la présidence bulgare a été détruit dans la nuit du 16 au 17 janvier 2001. Dans cette attaque, les pirates ont utilisé un mot de passe utilisé par des collaborateurs du président pour actualiser le site. Cet exemple montre que la vulnérabilité des organisations peut

venir des personnels qui y travaillent et peuvent ainsi céder des renseignements ou encore ne pas appliquer les consignes de sécurité.

2.3.3 L'Asie

Inde : En mai 1998, The Milworm, un groupe de jeunes hackers s'est introduit dans le réseau du centre indien de recherches nucléaires de Bhabha, vole des travaux sur les essais nucléaires récemment pratiqués par ce pays et détruit 2 des 8 ordinateurs du centre.

En février 2001, les policiers indiens ont arrêté deux hommes accusés d'avoir bloqué un site Internet spécialisé dans les offres et demandes d'emploi. Le blocage d'un site est une infraction prévue par une loi indienne sur les technologies de l'information qui peut être punie d'une peine de 3 ans de prison.

Japon : Au début mars 2000, la police japonaise dévoila l'origine du « group M », une entreprise de software dont les propriétaires seraient liés à la secte Aoum qui provoqua en 1996, une attaque au gaz dans le métro japonais. Au début de l'année 2000, les sites gouvernementaux japonais ont été victimes de 11 attaques. Il semblerait ainsi que la secte Aoum s'oriente vers une stratégie de cyber-attaque. L'armée japonaise a dû reporter le lancement d'un nouveau système informatique après avoir découvert que certains logiciels utilisés avaient été fabriqués par cette entreprise. Cet exemple montre comment les sectes ou groupuscules peuvent pénétrer les organismes gouvernementaux à travers des sociétés informatiques.

Taïwan : Les hackers taïwanais profitent du conflit qui oppose leur pays à la Chine pour lancer des attaques. Ce pays a un potentiel élevé en pirates informatiques. En effet le père du célèbre virus « Tchernobyl »[18] apparu en 1999 était un jeune ingénieur en informatique taïwanais du nom de Chen Ing-hau. Les sites gouvernementaux de ce pays sont aussi régulièrement l'objet d'attaques. Mais l'origine de celles-ci serait plutôt chinoise.

2.3.4 Le Moyen-Orient

Les pays du Moyen-Orient, que l'on pourrait penser quelque peu à l'abri des ravages des cyberpirates du fait de la plus faible informatisation de leur population, connaissent eux aussi les infections dues aux virus informatiques. Ceux-ci ne connaissent pas de frontières et ainsi le 26

[18] Le virus CIH (les initiales de Chen Ing-hau) est plus connu sous le nom de "Chernobyl" (selon l'orthographe anglo-saxonne) car il est programmé pour se déclencher une fois par an, le jour anniversaire de l'accident de la centrale nucléaire ukrainienne, le 26 avril 1986. Ce virus particulièrement dévastateur provoque le reformatage du disque dur des machines infectées et donc la perte de toutes les données. Il aurait contaminé plus de 500 000 machines, notamment en Corée du Sud, en Chine, en Turquie et, dans une moindre mesure, en Inde, aux États-Unis, en Israël et en Égypte.

février 1999, le virus Tchernobyl a affecté de nombreux pays du Moyen-Orient. Dans ces pays, il faut toutefois relativiser l'événement, car il ne s'agissait que de quelques dizaines d'ordinateurs touchés dont quelques ordinateurs au siège de l'ONU à Bagdad. Dans ces pays, ce sont surtout les tensions locales qui sont à l'origine des attaques.

Conflit Israélo-Palestinien : En octobre 2000, plusieurs milliers d'internautes pro-palestiniens ont lancé une attaque concertée contre le site officiel du ministère israélien des Affaires étrangères et sont parvenus à bloquer totalement le service pendant quelques heures. Le site du Parlement israélien, la Knesset, a également été bloqué. Le site de l'armée israélienne est aussi la cible d'attaques informatiques intenses. A la suite de ces attaques, l'armée et le Parlement israéliens se sont adressés à une firme américaine spécialisée dans la protection de sites Internet pour renforcer les dispositifs de sécurité de leur site.

Conflit Israélo-Libanais : Le site Internet d'une entreprise libanaise a été attaqué, au cours du mois de janvier 2001, par des pirates informatiques. Ce site est resté indisponible pendant six heures. Cette attaque serait un acte de vengeance d'internautes israéliens contre la société qui a créé le site de la télévision du Hezbollah.

Turquie : En marge de ces conflits, le piratage de site Internet peut devenir aussi un bon moyen de protestation sociale. C'est ainsi que des pirates, se disant les enfants de fonctionnaires turcs sous-payés, se sont introduits en décembre 2000 sur le site du Premier ministre turc et y ont laissé un message de protestation contre la politique économique du gouvernement.

Emirats Arabes Unis : Le réseau Internet de ce pays a été saboté et paralysé par des pannes majeures au cours de deux premières semaines du mois de juin 2000. Ce réseau est géré par une compagnie nationale qui accuse un européen travaillant pour une société informatique de Dubaï. Les pannes successives ont fait monter la pression pour la fin du monopole de l'Etat sur les télécommunications dans ce pays.

2.4 Une réalité sous estimée due au silence des entreprises attaquées

Les faits décrits sont pour la plupart mineurs. Mais nous n'avons connaissance que d'une infime partie du phénomène. Selon Christian HARBULOT, directeur de l'Ecole de Guerre Economique, « la meilleure protection contre le piratage est encore de le passer sous silence, comme l'a fait Master Card l'année dernière ». En effet les enjeux économiques sont très forts. Ainsi mis à part les Etats-Unis qui médiatisent de manière alarmante les attaques dont sont victimes ses administrations et entreprises, les autres pays restent beaucoup plus prudents. La France a choisi cette voie. Les informations restent très protégées. Seules les forces de police communiquent des statistiques mais ne s'étendent pas sur les faits.

* * *

Le silence ne devant pas être la seule réponse des entreprises aux prises avec ce phénomène, les Etats cherchent des solutions. Ces actions nationales et internationales tendent à prouver que la menace est bien réelle. Après une prise de conscience du risque, les solutions recherchées portent sur une meilleure protection, une surveillance des réseaux avec ses atteintes possibles à la vie privée et aussi sur des technologies de riposte.

*

* * *

*

3 Les moyens de lutte contre le cyberterrorisme

3.1 Une nécessaire prise de conscience du danger.

Aujourd'hui, les infrastructures vitales d'un pays dépendent de plus en plus d'entreprises privées. A ce titre, les Etats doivent prendre conscience du danger et faire adopter des mesures protectrices non seulement pour leurs organismes officiels mais aussi pour les entreprises privées.

Un gros travail reste à faire dans ce domaine. Les ennuis du site Yahoo! auraient pu être évités car les serveurs pouvaient être configurés pour ne pas répondre aux requêtes qui ont fini par les bloquer. Le manque de vigilance et le refus de consacrer des moyens suffisants à la sécurité facilitent les catastrophes. En effet, le RSA Data Security[19] rapporte que plus de 50% des entreprises n'ont pas téléchargé les correctifs logiciels censés réparer les 200 failles les plus connus dans la sécurité informatique des ordinateurs utilisés pour le commerce électronique. Une des priorités majeures des entreprises devrait être leur budget dédié à la sécurité.

Aussi l'ensemble des acteurs mondiaux doit préparer une politique de prévention du cyberterrorisme. Depuis trois ans, de nombreux pays commencent tout juste à s'éveiller à cette nouvelle réalité. Ils mettent en place des structures gouvernementales chargées de suivre le phénomène et tester la sécurité des infrastructures. Ils cherchent à protéger les entreprises et à mieux surveiller les réseaux de télécommunications. Les Etats-Unis, le Canada ainsi que les pays Européens préparent leur politique de lutte contre le cyberterrorisme.

3.1.1 Les Etats-Unis se lancent dans la lutte contre le cyberterrorisme

Les Etats-Unis ont été les premiers à prendre conscience de ce danger. Dès octobre 1997, une commission présidentielle américaine a rendu un rapport sur le cyberterrorisme et conclu que les infrastructures cruciales des Etats-Unis étaient vulnérables aux attaques informatiques. Cette commission a recommandé au gouvernement d'intensifier ses mesures pour se protéger contre les menaces potentielles. Elle constate que les systèmes informatiques, qui dirigent les aéroports, les réseaux de commandement et les systèmes de communications, sont ouverts aux cyberattaques.

On peut constater aussi que les corps policiers réagissent seulement au coup par coup et en sont ainsi réduits à un rôle de prévention trop peu pro-actif. La création d'unités spécialisées à côté du FBI dans la lutte reste récente aux Etats-Unis.

Le président CLINTON a annoncé, en janvier 2000, la prochaine mise en œuvre d'un plan national de protection des techniques américaines de l'information contre le cyberterrorisme. Vingt-deux agences fédérales collaborant avec des entreprises privées du secteur des

[19] La société RSA Data Security fournit des produits de sécurisation et cryptage du commerce électronique.

communications font partie de ce plan. Une importance particulière a été accordée à la recherche et au développement. Ce plan prévoit notamment l'octroi de bourses scolaires dans le domaine de la technologie de l'information en échange d'un temps de service public. Il permettrait également de financer la création d'un nouvel institut rassemblant des scientifiques et des informaticiens venus du secteur privé, des universités et des laboratoires afin d'accélérer et d'élargir la recherche dans le domaine de la sécurité informatique. Le président CLINTON souhaite « la création d'un système d'alarme à l'échelle du gouvernement fédéral pour déceler toute tentative d'infraction dans ses systèmes avec comme but la protection de la vie privée des citoyens. » 1,4 milliards de dollars serait nécessaire pour construire ce système.

3.1.2 La France fait évoluer ses structures officielles.

Par décret du 15 mai 2000, la France a créé un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication afin d'assurer la sécurité et la confiance dans le cyberespace. Il est également chargé de renforcer la coopération internationale en matière judiciaire. L'Etat français confit également au Secrétariat Général de la Défense Nationale la définition de la politique de protection des infrastructures vitales du pays. A cet effet, le SGDN doit mettre en place un centre de veille, de prévention et de secours, destiné à renforcer et à coordonner la lutte contre les intrusions dans les systèmes informatiques des administrations et des services publics (CERT/A[20]). Il se voit aussi rattacher la Direction Centrale de la Sécurité des Systèmes d'Information. La DCSSI a une fonction de régulation et d'autorité nationale de sécurité. Pour prévenir les attaques portées aux systèmes d'information, la direction a également une fonction opérationnelle pour évaluer les menaces, donner l'alerte et développer les capacités à les contrer et les prévenir et une fonction d'expertise scientifique et technique, en s'appuyant sur des laboratoires agréés. La DCSSI assume en outre une fonction de conseil aux sociétés comme à l'appareil d'Etat. La France cherche ainsi à se repositionner en matière de sécurité informatique par rapport à ses voisins européens.

3.1.3 Des structures adaptées et des forces de police spécialisée.

Le gouvernement japonais a annoncé vouloir amener son pays au niveau de la sécurité informatique des Etats-Unis à compter de 2003 et prépare un plan de lutte contre le cyberterrorisme. L'Inde a annoncé, le 14 février 2000, la création d'une commission formée d'experts des technologies de l'information tant gouvernementaux que privés chargés de donner des conseils en matière de sécurité.

---

[20] CERT/A: Computer Emergency Response Team / A pour Administrations

De nombreux pays mettent en place des forces de police spécialisée. La police turque a créé une brigade électronique chargée de faire la chasse aux pirates informatiques et recrute de jeunes informaticiens. Le Royaume-Uni souhaite également sa police cybernétique.

Afin de se protéger certains pays prennent des mesures radicales. Selon des Reporters Sans Frontières, 45 pays limitent l'accès de leurs citoyens à l'Internet, typiquement en les forçant de souscrire à un FAI[21] officiel, qui peut filtrer les sites jugés répréhensibles pour le régime. Ces pays à tendance autoritaire reconnaissent les bénéfices de l'Internet à la croissance économique, mais s'estiment en même temps menacés par le degré de liberté de discours sans précédent. Cela n'est que partiellement efficace, en effet les activistes chinois ont trouvé les moyens de faire passer l'information à travers ces contrôles. Le pays le plus radical reste la Corée du Nord, seul pays au monde où Internet n'existe pas.

Ainsi face à la cybermenace, les services gouvernementaux s'organisent et doivent recruter parmi les jeunes hackers ou les jeunes informaticiens afin d'avoir une réelle attitude active.

3.2 Mise en place de moyens de protection

3.2.1 Mieux se protéger

Il est probable qu'un jour des firewalls[22] et des détecteurs d'intrusion fonctionneront. Hormis réinventer les protocoles de transport d'information comme IP (Internet Protocol) et les systèmes d'exploitation comme Unix ou Windows NT Microsoft, la plupart des méthodes de sécurité reposent sur des briques logicielles ajoutées aux systèmes existants comme les firewalls et dans l'avenir les détecteurs d'intrusion. Or aujourd'hui , aucun des deux procédés n'est totalement fiable. Mais ces logiciels s'améliorent au fur et à mesure des défauts constatés.

3.2.2 Les défenses techniques

Les administrations et les entreprises doivent adopter une politique de sécurité rigoureuse.

Les défenses techniques existent pour se protéger des failles de sécurité connues. Dans un premier temps, il s'agit de sécuriser les accès servant à la télémaintenance des serveurs informatiques qui ont des « portes dérobées » appelées back-doors[23] pouvant être exploitées par les hackers. Il faut corriger les logiciels qui présentent des graves défauts de sécurité. Des

[21] FAI: Fournisseur d'Accès à Internet, société gérant les connexions à Internet.
[22] Les firewalls - pare-feux - sont des dispositifs filtrant les accès entrant et sortant des réseaux d'entreprise.
[23] Le but de ces portes dérobées est, lors de la conception des logiciels, de permettre aux programmeurs de pénétrer dans les systèmes client pour les déboguer ou en assurer la maintenance.

correctifs existent pour les problèmes signalés, mais il faut inciter les entreprises à les installer. Les entreprises connectés à Internet doivent protéger leur installation en filtrant les accès vers l'extérieur avec des pares-feux (firewall). Les mots de passe peuvent être à usage unique et générés dynamiquement mais cela est contraignant pour les personnels. Les serveurs connectés à Internet doivent disposer des outils contre le « déni de service ». Avec tout cet arsenal technique, les entreprises seront un peu plus à l'abri des attaques, du moins ne faciliteront-ils plus l'intrusion des hackers. Enfin des outils de traçage des connexions pourront être mis en œuvre afin de donner des éléments précieux aux forces de police.

Enfin le cryptage des informations échangées permet d'empêcher leur utilisation par d'éventuels voleurs. Ceci est facilité depuis que les pays ont libéralisé l'usage des logiciels de cryptage.

3.2.3 Tester ses défenses

Des pays ont fait le choix de recruter des « commandos » de hackers afin de tester la sécurité de leurs installations. C'est notamment le cas de l'Inde, de la Chine qui organise également des concours d'intrusion afin d'éprouver les solutions techniques retenues.

3.3 Une surveillance nécessaire des réseaux en particulier Internet

Les logiciels étant de plus en plus complexes, il devient difficile de garantir l'absence de failles. Ainsi il sera toujours nécessaire d'intervenir a posteriori pour traquer les pirates. C'est dans cette optique, que les Etats organisent la mise sous contrôle du réseau Internet.

3.3.1 Les réseaux sous surveillance

Le gouvernement australien a adopté en décembre 1999 une loi autorisant le piratage légal de systèmes informatiques privés ainsi que la copie et l'altération des données. Ce pays avait déjà autorisé un de ses organismes, l'ABA (Australian Broadcasting Autority), à parcourir l'Internet pour rechercher des contenus illégaux ou offensifs.

Le Royaume-Uni a suivi très rapidement. Le 26 juillet 2000, le parlement britannique a adopté définitivement la Rip Bill[24], loi qui autorise les autorités du pays à surveiller les e-mails et les communications cryptées sur l'internet. La Rip Bill, accorde le pouvoir aux autorités de police d'intercepter et de surveiller les communications sur les réseaux informatiques. Tout comme pour les écoutes téléphoniques, il leur faut cependant l'accord d'instances supérieures telles que le ministère de l'Intérieur. Pour permettre ces écoutes, des boîtes noires reliées à un centre d'observation, sont installées chez les fournisseurs d'accès internet. Même les mails cryptés

[24]Le texte est disponible sur le site www.homeoffice.gov.uk/oicd/ripbill.htm

pourront être saisis si nécessaires à la demande d'un juge. Et toute personne refusant de livrer les codes de cryptage pourra être sanctionnée de deux ans d'emprisonnement.

Tous les services de renseignement souhaitent des centres de surveillance du Net. Ainsi le service de contre-espionnage britannique, le MI5, prépare l'installation d'un centre permettant le suivi du trafic. La Russie a également étendu les prérogatives de contrôle de la FSB (ex KGB) sur le réseau Internet. Il leur faut tout de même fournir un mandat pour accéder aux informations…

Les Etats-Unis ont une réelle avance dans le domaine du contrôle du réseau Internet. La NSA, agence pour la sécurité nationale, a une longue pratique dans les interceptions de communications. Quant au FBI, il a déjà fait développer des outils informatiques pour surveiller les communications sur Internet. Il a avoué, en juillet dernier, disposer d'un logiciel permettant d'intercepter le courrier électronique des criminels. Le système surnommé « Carnivore » est déployé depuis deux ans auprès des fournisseurs d'accès à Internet et peut surveiller un volume très important de courriers. Il nécessite une autorisation judiciaire.

3.3.2 Les aspects légaux de la surveillance

La France n'a pour l'instant adopté aucun nouveau texte de loi. Il existe pourtant un projet de loi sur la société d'information. Le respect de la vie privée reste aussi un objectif majeur. En France, la loi du 10 juillet 1991 relative au secret des correspondances émises par les télécommunications garantit les particuliers contre les interceptions de leur communications, notamment au travers de l'action de la commission nationale de contrôle des interceptions de sécurité (CNCIS).

Ainsi tous ces nouveaux systèmes de surveillance et de contrôle, mis en place dans le cadre de la sécurité des Etats, peuvent porter atteinte aux libertés humaines. Des associations britanniques de défense des droits civiques et certains hommes d'affaires l'ont bien compris et s'insurgent contre la loi autorisant les surveillances.

Le Conseil de l'Europe va proposer un Traité pour uniformiser les pratiques. Ce projet de convention[25] sur la cybercriminalité devrait être adopté pendant l'été. Ce texte pourrait devenir d'ici la fin de l'année le premier traité international en la matière. Il devrait être adopté pendant l'été et ouvert en septembre non seulement à la signature des 43 Etats membres de l'organisation européenne, mais aussi des pays qui comme les Etats-Unis, le Canada, le Japon ou l'Afrique du Sud ont étroitement collaboré à sa conception depuis 1997. La future convention est destinée à aider les Etats à faire face aux attaques des cybercriminels ou cyberterroristes. Elle prévoit entre autre de sanctionner le piratage informatique, l'interception illégale de données. La convention

traite aussi de la répression, prévoyant la possibilité de perquisitionner des systèmes informatiques, de saisir des données, d'obliger des personnes à livrer des données en leur possession, de conserver des données vulnérables ou de les faire conserver par les personnes concernées.

3.4 Développement des capacités de détecter les cyberattaques et de riposter

La répression ne peut s'appliquer qu'a posteriori. Aussi, il peut être nécessaire de proposer des capacités de riposte.

Le directeur de l'agence de la sécurité nationale américaine (NSA), a déclaré dans un article « Défendre la nation contre les cyberattaques : la sécurité de l'information dans l'environnement mondial » que l'agence de la sécurité nationale « fait appel à ses compétences spécialisées pour élaborer la technologie fondamentale qui établira des capacités nationales de détection des cyberattaques et de riposte à ces attaques». Il a ajouté : « la supériorité des moyens informatiques à l'âge de l'information est de toute évidence un impératif national ».

Face aux cyberattaques, les techniques de diagnostic, de détection et de riposte sont aujourd'hui en développement. La capacité d'identifier une cyberattaque stratégique visant un ou plusieurs éléments vitaux d'infrastructure et d'y réagir de manière appropriée est à l'évidence une question primordiale de sécurité nationale pour tous les Etats. Il faut en effet posséder la capacité de détecter les attaques au moment où elles se produisent et la capacité de riposte immédiate afin de faire cesser l'attaque pour permettre la reprise d'activité.

3.4.1 Les systèmes de détection d'intrusion

La détection d'intrusion dans les systèmes informatiques est un domaine déjà exploré par les chercheurs. Les premiers systèmes ont été proposés vers 1980 par James Anderson. Mais ces premiers systèmes très lourds à mettre en œuvre connaissent de nombreuses imperfections. En 1999, Stephano MARTINO[26] a proposé un nouveau type d'approche analogue au système immunitaire humain, où des « agents mobiles », programmes informatiques mobiles entre ordinateurs et coopérant entre eux, devront combattre les intrus avant qu'ils ne deviennent une menace pour le système. Les recherches se poursuivent toujours aujourd'hui afin de fiabiliser ces systèmes.

[25] Le texte est disponible sur le site de conseil européen : http ://conventions.coe.int/treaty/FR/cadreprojets.htm
[26] Stéphano Martino, "A mobile agent approach to intrusion detection", 1999.

3.4.2 Les technologies de riposte

Des outils de riposte existent déjà. Un programme du type Zombie_Zapper[27] permet de stopper une attaque à sa source, en frappant le système émetteur. Dans son dictionnaire technique et critique des nouvelles menaces, Xavier RAUFER fait état de l'existence d'un nouveau type de virus, un « algorithme non linéaire » nommé Blitzkrieg[28]. Cet outil conçu en 1998 pour lutter contre la pénétration illicite des hackers dans les réseaux informatiques, via Internet, peut émettre en cas d'intrusion un « virus tueur » qui causerait des dommages irréversibles aux logiciels et au matériel informatique de l'intrus.

Cependant, les atteintes à l'intégrité des systèmes informatiques, considérées comme des actes délictueux ou criminels, relèvent des compétences des forces de police. Aussi, il devient nécessaire de revoir la législation et d'instaurer une « légitime défense » autorisée à la suite d'une attaque informatique. Une autre voie serait de définir de nouvelles règles d'engagement afin de permettre une collaboration ouverte et dynamique entre le secteur privé, les administrations et les forces de l'ordre. L'action combinée d'une surveillance améliorée du réseau et d'une alerte immédiate des forces de l'ordre pourrait leur permettre de riposter et de repérer plus rapidement les intrus.

3.5 Le jeu ambigu des Etats-Unis :

Comme nous l'avons vu, les Etats-Unis se lancent avec des budgets considérables dans cette lutte contre le cyberterrorisme. Après la très forte médiatisation du bug de l'an 2000, le fameux Y2K, qui n'a causé aucun des ravages annoncés, nous pouvons légitimement nous interroger sur la motivation réelle qu'ont les Etats-Unis pour investir autant face à une menace émergente qui n'a pour l'instant tué personne.

3.5.1 Quel intérêt ont les Etats-Unis de dramatiser le cyberterrorisme ?

Les Etats-Unis resservent régulièrement le spectre de la guerre électronique dévastatrice. Ils annoncent la menace d'un « cyber-jihad ». Certains groupes de hackers palestiniens, qui seraient liés au terroriste international Ben LADEN, seraient sur le point de lancer des cyberattaques contre les Etats-Unis. Les Américains jouent à se faire peur. Pour son congrès, les attaques potentielles de cyberterroristes constitueraient une menace plus grande qu'une guerre chimique, car cette menace est révolutionnaire.

---

[27] Description disponible sur le site http://razor.bindview.com/tools/desc/ZombieZapper_readme.html

[28] Voir article datant du 6/8/98 « Blitzkrieg server computer virus » sur le site www.info-sec.com/viruses/viruses_060898a_j.html-ssi

Jusqu'à aujourd'hui comme nous l'avons décrit, le cyberterrorisme n'a causé aucune mort humaine. L'objectif des Etats-Unis serait de préparer une répression sans faille en créant la peur, l'incertitude et le doute dans les esprits. Les Etats-Unis ont une politique fortement interventionniste dans le monde. Ils craignent que des pays cherchent à neutraliser leur capacité de riposte. En 1999, Sandy BERGER, le principal conseiller du président CLINTON pour la sécurité nationale, n'a pas hésité à annoncer: « Nous avons la certitude que des gouvernements construisent des systèmes destinés à pénétrer nos réseaux informatiques.»

Si les Etats-Unis, la nation la plus technologique de la planète, sont si peu préparés à confronter ces nouvelles menaces, il y a de quoi s'inquiéter. La réalité est certainement économique. Le manque à gagner par grande société américaine de commerce électronique se chiffre en million de dollars par heure de déni de service.

A travers les actions entreprises, nous pouvons estimer que les Etats-Unis veulent contrôler le réseau Internet et toutes les communications. Ils seraient ainsi non seulement les « gendarmes du monde » mais aussi les gendarmes du Cyberespace, ce nouveau territoire dont la géopolitique semble aujourd'hui leur échapper. Cette volonté est clairement perçue et leur ambition doit aboutir sans se soucier du respect de la vie privée. La suprématie économique de cet Etat ne doit pas connaître de limite.

Une étude du Congrès des Etats-Unis sur les sites gouvernementaux américains montre que seuls 3% d'entre eux se conforment aux règles sur le respect de la vie privée proposées par la Commission fédérale du Commerce (FTC) concernant le commerce électronique. L'analyse révélée en septembre 2000 a été rejetée par l'administration CLINTON.

La NSA, la célèbre agence pour la sécurité nationale, s'est spécialisée depuis des dizaines années dans les écoutes. Intéressons nous à cette agence et à ses pratiques.

3.5.2 Les pleins pouvoirs de la NSA

Depuis un an, on connaît un peu plus les pratiques de la NSA. L'existence du système ECHELON[29] a été dévoilée au monde. Les moyens et les méthodes présentés dans le film Ennemi d'Etat ne doivent pas être loin de la réalité. La NSA traite autant d'informations qu'il y a dans la plus grande bibliothèque toutes les trois heures.

Un rapport d'information[30] sur ce système a été déposé à l'Assemblée Nationale par la commission de la défense nationale. Il traite des systèmes de surveillance et d'interception

[29] Le système Echelon est un réseau d'écoutes téléphoniques à l'échelle mondiale.
[30] Rapport disponible à l'adresse Internet : www.assemblee-nationale/2/rap-info/i2623.htm

électroniques pouvant mettre en cause la sécurité nationale. Le député Arthur PAECHT conclut dans ce document :

« Oui, il existe bien un vaste système d'interception et de traitement des informations nommé Echelon. Il est organisé en réseau. Il s'agit d'ailleurs du seul système multinational connu.

Oui, les capacités d'un tel système sont réelles et elles le rendent performant, compte tenu des multiples vulnérabilités des systèmes d'information et de communication. .....

Oui, le système Echelon a "divergé" par rapport à ses objectifs initiaux, qui étaient fondamentalement liés au contexte de la guerre froide et par rapport même aux conditions du pacte initial UKUSA entre les cinq partenaires. Il n'est pas impossible que des informations recueillies soient utilisées à des fins politiques et économiques, voire à l'encontre de certains membres de l'Alliance atlantique. Si les preuves manquent pour évoquer l'espionnage industriel, les propos d'anciens responsables d'agences de renseignement constituent autant d'aveux. ...

Oui, Echelon peut constituer un danger pour les libertés publiques et individuelles. ...Le système d'ailleurs évolue et s'adapte. Plusieurs indices semblent inciter à croire qu'un nouveau système s'est constitué pour dépasser les limites d'Echelon grâce à de nouveaux moyens et sans doute de nouveaux partenariats. »

A travers ces conclusions, nous pouvons penser que la NSA souhaite surveiller toutes les communications y compris Internet aussi à des fins d’espionnage.

3.5.3 Les outils d’un espionnage industriel mondial

L’espionnage des communications par la NSA bénéficierait aussi de la complicité de sociétés américaines. Si cette agence travaille dans le domaine de l’espionnage industriel et économique, elle peut apporter des aides précieuses aux entreprises américaines pour remporter des appels d’offre.

L’édition du Monde du Renseignement du 7 octobre 1999 annonce que le pentagone et la NSA auraient engagé ces derniers mois des négociations secrètes, directement avec les patrons de IBM et de Microsoft, pour mettre en place des dispositifs leur permettant d'accéder à des données cryptées.

Ces informations se recoupent avec celles fournies par un consultant en sécurité de la société Cryptonym installé dans l'Ontario, au Canada. Andrew Fernandez, croit avoir découvert une “porte dérobée” (back-door) dans le module de sécurité de Windows NT 4.0, logiciel d'exploitation réseau, utilisé par plusieurs dizaines de millions d'utilisateurs professionnels. Cet

accès permettrait à la puissante National Security Agency (NSA) de décrypter (par l'intermédiaire d'une clef _NSAKEY) les communications protégées.

Ces révélations ont bien évidemment été démenties par un porte-parole de Microsoft. La NSA s'est contentée de renvoyer les curieux vers Microsoft. Pourtant un rapport réalisé pour la Délégation aux Affaires Stratégiques (DAS) du ministère français de la Défense soupçonne fortement l'existence de liens entre le groupe Microsoft et les services de renseignements américains. Le rapport soupçonne l'existence de programmes espions ou de back-doors dans les produits vendus par Microsoft. Selon ce document, cité par Le Monde du Renseignement, des membres de NSA travailleraient dans des équipes de Microsoft.[31]

* * *

La lutte contre le cyberterrorisme s'appuie sur une politique de sécurité tant des administrations que des entreprises privées. Les systèmes d'information doivent être protégés et des organismes de contrôle sont créés. Les outils de riposte doivent être étudiés, ils pourront servir aux armées. Mais la surveillance des réseaux doit rester une prérogative des forces de police habilitées par la justice sous peine de laisser se développer, derrière des enjeux de sécurité, un espionnage technologique sans limite.

* * *

*

[31] Cette information a été reprise dans une dépêche AFP du 18 février 2000

Conclusion

Des spécialistes prédisent que les réseaux seront complètement sécurisés d'ici à 10 ans. Ils s'appuient sur les évolutions technologiques à venir et les logiciels qui permettront le transport sécurisé des informations. Il faut néanmoins tempérer leurs espoirs. En effet, une équipe de scientifiques de 6 pays a annoncé avoir réussi à casser une clé numérique d'une longueur de 512 bits. Cela confirme la menace qui plane sur les systèmes d'information même très sécurisés. Dans le domaine complexe de l'informatique, la protection et la fiabilisation d'un système coûtent beaucoup plus chers que les outils parfois primitifs qui parviennent à les arrêter.

Les armées, tout comme les entreprises, doivent prendre des dispositions pour ne pas être la cible de ce cyberterrorisme. Nous ne sommes qu'au début de la guerre de l'informatique. Le secret qui entoure l'implication des armées dans ce domaine sera certainement levé le jour, où une intervention nécessitera l'utilisation de ces nouveaux moyens. Nous découvrirons alors un type d'armes révolutionnaires mais seulement à travers ses effets générés. Elles sont en effet impalpables physiquement et tout juste apercevrons-nous la disquette qui a contenu la bombe logique avant qu'elle ne vienne à bout des systèmes d'information adverses, permettant à nos soldats d'intervenir face à un adversaire aveugle.

Pourquoi n'y a-t-il jamais eu d'attentat informatique jusqu'à présent ? Des spécialistes ont tenté d'apporter une réponse. Certains estiment que les groupes terroristes rejetant l'occidentalisation rejettent par conséquent la technologie qui en est le corollaire. Pour ma part, je pense que les groupes de terroristes d'hier ne seront peut-être pas ceux de demain. Quels seront les revendications d'un monde où l'interventionnisme américain est appelé pour calmer les conflits locaux ? Certains groupes aspirant à plus de liberté seront certainement tentés de s'en prendre aux Etats qui tentent de trop les surveiller. Alors leurs actions toucheront des intérêts essentiellement économiques ou les systèmes étatiques de contrôle.

Comme le souligne le rapport parlementaire sur le système ECHELON, il est nécessaire d'élaborer une véritable déontologie du renseignement afin de protéger les libertés humaines. La dérive qui s'amorce avec les systèmes américains de contrôle des réseaux doit être surveillée. La sécurité doit rester le seul objectif des réseaux de surveillance d'Internet. Il est nécessaire de traquer les criminels et d'y mettre les moyens suffisants. Mais la détection et la mise sous surveillance de la vie privée d'un individu, à partir de seuls mots-clés entrés au travers d'un clavier d'ordinateur, doivent être proscrites.

Table des matières

Bibliographie

Livres

Dictionnaire technique et critique des nouvelles menaces.	1999	Xavier RAUFER (ed PUF).
Guerres dans le cyberespace	1996	Jean GUISNEL (ed La découverte)
Menaces sur Internet.	1999	Grégory DESTOUCHES (Michalon).
Conférence débat sur le crime informatique et la cyber-guerre	1999	Daniel MARTIN (Centre universitaire juridique de recherche sur les menaces criminelles contemporaines)
La criminalité informatique	1997	Daniel MARTIN (ed PUF)
Information Warfare and Security	1998	Dorothy DENNING (ed Addison Wesley)
La prochaine guerre		James ADAMS
Rapport d'information au nom de la commission de la défense, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale (système Echelon)	2000	M. le député Arthur PAECHT (Rapport de l'Assemblée Nationale)

Sites Internet

www.frstrategie.org :	Cyberterrorisme : entre mythe et réalité . Article de Marc Bouvier consultant Fondation pour la Recherche Stratégique
www.cert.org	Site officiel du Computer Emergency Response Tean
www.infowar.com/civil_de/civil_c.html-ssi	Les dangers et l'avenir du cyberterrorisme
www.csis	Center for Strategic & International Studies
www.u-paris2.fr/mcc	Centre universitaire juridique de recherche sur les menaces criminelles contemporaines : Conférence-débat sur « crime informatique et cyber-guerre » du 18 février 1999 Intervention de Daniel Martin
www.usinfo.state.gov/journals/itps/1198/ijpf/frminih.htm	Article du général Kenneth Minihan Directeur de la NSA pour la revue électronique de l'USIA novembre 1998
www.guill.net/reseaux/ids.htm	Synthèse d'article de recherche sur la détection d'intrusion datant de février 2000 préparé par Guillaume Desgeorge, étudiant en DEA.
www.assemblee-nationale.fr	Site de l'Assemblée Nationale
www.nipc.gov	FBI : National Infrastructure Protection Center