COLLEGE INTERARMEES DE DEFENSE

LA CRIMINALITE INFORMATIQUE TRANSNATIONALE

Mémoire de géopolitique

du Chef de Bataillon Antoine SORBA

dans le cadre de l'étude dirigée "Les criminalités transnationales"

Directeur : Commissaire Principal Philippe MIGAUX
de la sous-direction antiterroriste

FICHE DE PRESENTATION

1. La criminalité informatique transnationale

2. Chef de bataillon Antoine SORBA.

3. 06 avril 2001.

4. Division D.

5. Mémoire de géopolitique.

6. Ce mémoire a pour objectif d'étudier une nouvelle forme de criminalité transnationale : « la criminalité informatique ». Caractérisée par sa complexité technique, le nombre d'individus qui y participent et l'impunité que lui confère son caractère d'extra territorialité, la criminalité informatique est un phénomène en pleine expansion contre lequel les autorités ont du mal à lutter. Son organisation progressive fait craindre d'autre part à une augmentation de la menace susceptible de mettre en danger la sécurité nationale.

7. Mots clés : Internet, pirate, cybercriminalité, réseau, informatique, sécurité, intrusion .

Avril 2001

LA CRIMINALITE INFORMATIQUE TRANSNATIONALE

SOMMAIRE

Introduction

La révolution dans les nouvelles technologies de l'information et de la communication a conduit au développement de sociétés fortement dépendantes de l'informatique et organisées en réseaux. Le réseau Internet en particulier joue un rôle capital au sein des sociétés modernes car il tient lieu d'interface à tous les réseaux et leur donne par là une dimension mondiale. A ce titre, il rassemble à travers le monde plus de 200 millions de personnes qui communiquent, passent des commandes, paient des factures ou font des affaires par son entremise.

Cette situation a en retour favorisé, dans les pays les plus développés technologiquement, l'apparition d'une forme de criminalité nouvelle, la criminalité informatique. Cette criminalité, comme son nom le laisse entendre, tire parti des nouvelles et formidables potentialités qu'offrent les systèmes informatiques et les technologies qui leur sont associées. Elle peut donc être caractérisée par le recours aux moyens informatiques comme instruments d'actes illégaux. Elle prend elle-même dans la plupart des cas pour cibles d'autres systèmes informatiques.
Une de ses particularités essentielles est d'opérer en s'affranchissant totalement des frontières. L'informatique offre en effet des possibilités d'actions à distance extrêmement puissantes à quiconque a la volonté d'en faire un usage délictueux. Elle permet notamment et sans grandes difficultés d'accéder aux informations protégées, de porter atteinte à l'intégrité des données, d'exploiter illégalement des services ou d'empêcher leur utilisation normale par les usagers.
L'informatique a pris une place telle dans le fonctionnement de nos sociétés et les attaques contre les systèmes d'information atteignent désormais une ampleur si grande que tous les pays modernes se sont décidés à considérer ce problème comme sérieux. Ils tentent pour cette raison de développer des moyens de lutte spécifiques à cette nouvelle forme de criminalité.
D'autre part, les signes d'organisation de cette criminalité et la puissance de ses effets dévastateurs font que certains Etats y voient même une menace potentielle pour la sécurité nationale. L'ONU de son côté y consacre d'ailleurs une place particulière dans ses travaux sur la prévention du crime.

Dans ce contexte, il apparaît naturel de s'intéresser de près à cette nouvelle criminalité. Il est nécessaire avant tout d'en identifier les différentes formes et de prendre conscience de leur potentiel de nuisance en examinant ce qui se passe aujourd'hui dans le cyberespace. Il est également urgent d'étudier les facteurs de vulnérabilité de notre société face à cette menace. Enfin, il convient de définir la stratégie la mieux adaptée pour se prémunir contre l'éventualité d'attaques informatiques d'envergure susceptibles de désorganiser le pays.

1. Les formes de cybercriminalité

La criminalité informatique croît au même rythme que l'utilisation des réseaux informatiques et connaît donc une croissance exponentielle. Elle est née à l'origine d'individus isolés à l'aise avec l'utilisation des nouvelles technologies de l'information et qui ont profité au gré des opportunités des failles de sécurité des réseaux.
Aujourd'hui, bien que toujours en expansion, cette forme initiale de criminalité n'est plus la seule. Des formes plus structurées tendent à se rajouter à la première. Elles correspondent en réalité bien souvent à des formes anciennes de criminalité qui pour atteindre leurs objectifs spécifiques ont recours aux possibilités nouvelles que leur offrent les moyens informatiques. Les Etats eux-mêmes commencent à percevoir l'atout qu'ils pourraient tirer de l'informatique dans la poursuite de leurs intérêts stratégiques et de leur politique extérieure.
Cette situation conduit à distinguer quatre formes de criminalité informatique : La criminalité informatique due à des individus plus ou moins isolés, l'utilisation frauduleuse de l'informatique au service de la grande criminalité, l'informatique comme support de lutte des groupes terroristes et enfin la guerre informatique entre Etats.

11) Les formes individuelles de criminalité informatique

La cyberdélinquance perpétrée de manière individuelle par certains internautes est sans aucun doute la forme la plus dynamique et la plus créatrice de criminalité informatique. C'est d'elle qu'émergent toutes les nouvelles techniques criminelles, ce qui a pour effet premier de mettre en lumière l'extrême vulnérabilité de la plupart des systèmes d'information, y compris des plus sensibles.

Autre conséquence mais plutôt fâcheuse, les groupes organisés ne manquent pas non plus d'exploiter à leurs fins les brèches de sécurité mises en lumière.
La question de ce qui se passerait si une organisation ou un Etat avait la volonté de récupérer l'ensemble de ces compétences pour une attaque de grande envergure contre un adversaire déclaré reste à ce jour ouverte.

Les pirates informatiques

La forme de criminalité informatique la plus connue, en raison de l'écho qu'en donnent les médias, met aux prises les Etats modernes à des individus qualifiés de pirates informatiques encore dénommés "hackers" dans la terminologie anglo-saxonne.
Les motivations de ces protagonistes ne sont pas nouvelles : elles tiennent principalement à l'acquisition illicite de produits informatiques pour un usage d'abord personnel, à l'appât du gain, parfois au désir de vengeance ou simplement à la recherche d'une forme de défi à caractère technique. La nouveauté de cette criminalité vient plutôt des possibilités sans précédent offertes par la technologie pour franchir le pas de la légalité, la duplication et la diffusion étant par exemple des techniques devenues accessibles à tout un chacun.

Les aspects sous lesquels cette forme de criminalité se manifeste sont extrêmement variés. Parmi les actes illégaux les plus courants, on trouve la contrefaçon informatique. Elle s'applique notamment aux logiciels copiés sur Internet ou issus de la reproduction de CD ROM. Elle pose un sérieux problème dans le domaine de la création artistique et plus généralement dans celui de la propriété intellectuelle. Ce type d'activités donne lieu à de petits trafics de revente ou d'échange entre particuliers. Cette délinquance est si répandue qu'on peut pratiquement considérer qu'elle touche, à des degrés divers il est vrai, l'ensemble des utilisateurs du réseau Internet.
Les copies illégales des systèmes d'exploitation Windows, des suites logiciels de bureautique, de logiciels de jeux, de fichiers musicaux sont devenues monnaie courante au point que beaucoup considèrent qu'un usage privé de ces produits n'expose aujourd'hui l'utilisateur à aucun risque.
Aux Etats-Unis, l'association de l'industrie informatique et du logiciel estime à 7,5 milliards de dollars par an les pertes subies par l'industrie du logiciel américain dans les copies et

distributions illégales de logiciels à travers le monde. Les mondes de l'édition musicale et du cinéma protestent aussi vigoureusement contre ce manque à gagner qui mettrait en danger la création artistique, mais rien ne semble pouvoir stopper ce phénomène.
Une part très importante porte également sur des escroqueries commises en matière de commerce électronique. Ces délits s'effectuent à l'aide des numéros de cartes bancaires récupérés après intrusion sur des bases de données de sociétés ou d'entreprises. Ces numéros sont ensuite utilisés frauduleusement soit pour payer des services de téléchargement de logiciels en ligne, soit pour se connecter sur des serveurs pornographiques ou encore pour effectuer des achats de matériels auprès de sites marchands. On évalue à environ 3 milliards de francs par an les pertes que subissent les consommateurs à la suite de récupération en ligne d'informations sur les cartes de crédit par les pirates informatiques.

Mais les pirates sont parfois animés de motivations autres que mercantiles. Ils sont poussés par une sorte de soif d'exploration de ce fabuleux espace qu'est Internet. Ils revendiquent même un droit d'exploration et de libre accès à ce réseau. Ce droit étant selon eux conforme à l'esprit d'Internet à son origine, ils n'ont donc pas réellement le sentiment de transgresser les lois. De plus, souvent doués d'un grand talent technique, vivant quelquefois en marge de la société, ils aspirent à la célébrité et font valoir avec le plus de retentissement possible leurs exploits.
Une de leur passion favorite consiste à pénétrer sur tout type de réseaux et à visiter les sites les plus emblématiques et les mieux protégés. Les sites du Pentagone font à ce titre l'objet d'intrusions régulières sans qu'il soit possible aux services de sécurité de les empêcher.
La NASA, qui représente une sorte d'étendard pour les États-Unis, est la cible d'un nombre croissant de cyberattaques. En 1999, on en a compté plus de 500 000.
Malheureusement, le vandalisme fait aussi partie de leurs actions et les intrusions sont régulièrement suivies de destructions de données ou de programmes. Les virus sont un autre moyen de dégradation gratuite sensé là encore démontrer une habileté technique hors du commun. Ce sont de petits programmes mis au point par les pirates qui sont transmis par les réseaux et qui dégradent les fonctionnalités des ordinateurs sur lesquels ils s'installent. Ils se dissimulent souvent dans des messages électroniques (mails) ou des programmes téléchargés à partir d'Internet. Leurs effets sont parfois redoutables et leur propagation foudroyante. Ce fut le cas, pour donner un exemple, du virus "I love you" qui a semé une véritable panique en mai 2000 en infestant en quelques heures des milliers voire des millions d'ordinateurs. Il avait la propriété d'accéder aux carnets d'adresses des victimes et de renvoyer lui-même des messages

vers ces nouveaux destinataires lui permettant ainsi de se reproduire. Il agissait de surcroît sur les fichiers du disque dur des ordinateurs l'hébergeant. Les dégâts qu'il a provoqués sont difficiles à chiffrer et les chiffres parus ça et là sont difficilement vérifiables. Ils pourraient tout de même se monter à quelques milliards de dollars d'après certains experts.

Les mercenaires

Un des aspects les plus préoccupants de cette forme de criminalité est la mise en commun spontanée des informations à caractère technique quant aux moyens de perpétrer des actes illégaux. Par esprit de défi vis-à-vis des autorités, les pirates éprouvent en effet le besoin malsain de se vanter de leurs exploits et d'en donner des preuves. L'existence de milliers de forums d'échange diffusant sans restriction sur Internet les failles des systèmes d'informations visités, les techniques d'attaques avec de surcroît la fourniture de programmes d'intrusion ou de destruction prêts à l'emploi en témoignent.
Il est par exemple possible de trouver en ligne un guide de la fraude Internet sur un site dénommé "Ad Cops" situé aux Etats-Unis. Ce site explique en détail comment s'emparer de numéros de cartes de crédits et des mots de passe puis les réutiliser sans se faire prendre.
D'autres donnent avec forces détails: les dernières techniques d'intrusion, la façon d'implanter des dispositifs de type "chevaux de Troie" permettant d'accéder au moment opportun à un ordinateur, les programmes les plus perfectionnés pour casser les mots de passe, ceux les mieux adaptés pour générer des numéros de cartes de crédit ou les données sur de nouveaux types de virus.
Donner ici une liste détaillée de l'ensemble des techniques d'attaque (Le « social engineering », le « crackage » de mots de passe, le « sniffing » des mots de passe, l'intrusion au moyen d'un « cheval de Troie », l'attaque par virus, le déni de service…) n'est pas possible tant son contenu serait riche et en perpétuelle évolution (cf. Annexe2).

Il se crée par le biais de ces échanges des communautés virtuelles de circonstance dont les membres s'émulent mutuellement. A l'occasion, ils s'investissent même d'une mission, unissant alors leurs talents pour parvenir aux fins qu'ils se sont fixés. Au nom de revendications libertaires, ils s'en prennent par exemple aux infrastructures gouvernementales, accusant les autorités de menacer la vie privée des citoyens. Ce fut le cas du "Chaos Computer Club" dans

les années 84-85 qui soupçonnait le gouvernement allemand, sous couvert de lutte antiterroriste, de mettre en place un fichier des individus. D'autres, comme "2600.com", réclament avec force la libération du plus célèbre pirate Kevin Mitnick qui avait entre autres délits dérobé 17 000 numéros de cartes de crédit avant de se faire arrêter.

Il peut parfois s'agir d'un combat de nature beaucoup moins pacifique puisque certains forums n'hésitent pas à diffuser des informations sur des sujets tels que : Propagande raciste, techniques de fabrication d'engins explosifs, techniques de harcèlement…
Les pirates informatiques qui participent à ces communautés virtuelles sont susceptibles de se transformer en mercenaires. Ils s'unissent alors temporairement pour vendre leurs services sans aucun scrupule.
D'après des informations publiées dans la revue "Jane's Intelligence Review', les cartels de la drogue en Colombie ont loué les services de pirates pour installer et gérer un système sophistiqué de communications sécurisées ; cette revue donne aussi le cas de gangs hollandais qui ont utilisé des pirates professionnels pour paralyser le système d'information et de communication des services de police chargés de la surveillance de leurs activités.

12) L'informatique au service de formes de criminalité organisées

Pour les organisations criminelles, l'informatique s'est rapidement imposée comme une aide extrêmement efficace pour faciliter leurs activités traditionnelles. L'informatique procure aux entreprises criminelles en plus d'une envergure mondiale des prises de risques moindres car elles peuvent agir sans violence physique et avec un maximum de discrétion.
Exploitant sans Etat d'âme et à une échelle bien supérieure le réservoir d'informations et de techniques constitué par les pirates informatiques, nombre d'organisations criminelles se lancent dans la cybercriminalité tandis que d'autres cybergangs naissent, alléchés par les perspectives de gains faciles et rapides.
Il est fort probable que dans l'avenir le crime organisé utilisera de plus en plus les nouvelles technologies pour générer des revenus supérieurs grâce à plus de pornographie, plus de fraudes, plus d'escroqueries et des possibilités nouvelles de casses informatiques. Enfin, le blanchiment de ces revenus sera lui-même facilité par le truchement des moyens informatiques.

La pornographie

La diffusion de supports pornographiques a été et reste parmi les premières applications d'Internet. Or, si la pédophilie fut longtemps restreinte à un cercle très fermé, l'arrivée d'Internet a malheureusement provoqué presque instantanément l'expansion brutale du problème en permettant de diffuser ou d'acquérir dans le monde entier du matériel photo ou vidéo par de simples commandes au clavier d'un ordinateur ; d'autant que certains pays comme le Japon ne possèdent aucune législation relative à la publication d'images pornographiques impliquant des enfants.

L'attention des services de sécurité est mobilisée sur cette forme de délinquance en raison notamment de l'émotion légitime que suscite ce type d'affaire dans l'opinion publique.

Cependant, la lutte contre cette criminalité est difficile car, pour dissimuler leurs activités aux yeux des autorités, les pédophiles ont recours à des procédés de chiffrement des communications et de stockage des documents pornographiques. Ils restreignent de plus les accès de leurs sites par mots de passe et conditionnent parfois également l'accès à la fourniture d'un nombre de photos à caractère pédophile.

Les investigations menées dans ce domaine ont démontré l'existence de réseaux internationaux structurés. A titre d'illustration, elles ont mis à jour en 1998 un vaste réseau, du nom de "Wonderland Club", qui impliquait 14 pays dans le monde appartenant à l'Europe, l'Amérique du Nord et l'Australie. Son démantèlement coordonné par Interpol a entraîné l'arrestation d'environ 100 personnes et la saisie de plus de 100 000 images.

Le blanchiment d'argent et l'évasion fiscale

Le développement des nouvelles technologies entourant le commerce électronique a largement facilité le blanchiment d'argent et l'évasion fiscale au point que ce procédé n'est plus de nos jours réservé aux seules grandes entreprises criminelles comme la mafia ou encore aux grands groupes industriels soucieux de dissimuler une partie de leurs avoirs pour le compte d'intérêts particuliers. Désormais, les petites bandes organisées comme les petites sociétés ont les instruments en leur possession pour recycler ou dissimuler au fisc une part de leurs revenus. Les transferts de fonds entre Etats et par conséquent entre systèmes législatifs différents ne nécessitent que quelques secondes.

D’autre part, la constitution d’un réseau d’organismes bancaires non officiels permet d’échapper encore plus facilement au contrôle des Etats, en particulier de celui mis en œuvre par le biais des banques centrales.

Les extorsions ou détournements de fonds

Certains groupes désireux de s’enrichir par la voie la plus rapide s’en prennent directement aux organismes bancaires. Il s’agit en quelque sorte d’une version moderne de l’attaque de banque, à laquelle on pourrait donner le nom de “hold up électronique”.
Ils sont pour nombre d’entre eux originaires des Etats-Unis et des autres pays occidentaux, mais pas uniquement. Des pays tels que l’Inde, le Pakistan et même l’Indonésie sont en train de devenir de véritables repaires de pirates. Il faut noter que ces derniers ont souvent été diplômés dans les meilleures universités occidentales et y ont acquis leur expertise en sciences informatiques. La Russie foisonne également de pirates depuis la chute du communisme. Des milliers d’informaticiens de haut niveau se sont en effet brusquement retrouvés sans emploi du jour au lendemain après avoir fait partie des privilégiés du régime et s’être impliqués dans les programmes les plus en pointe de leur pays. Ils ont pu voir alors dans ce type d’activités le moyen le plus simple de retrouver une source de revenus décente.
Parmi les cas répertoriés, la banque du Vatican s'est fait pirater par une vingtaine de personnes qui ont tenté d'extorquer 7 milliards de francs. La technique utilisée fonctionnait avec de petites sommes mais la tentative a échoué lorsqu’ils ont cherché la complicité d'un directeur de banque en Suisse.
Autre détournement mais réussi cette fois, en 1994, un pirate russe Vladimir Levin, opérant depuis St Petersbourg a réussi à accéder au système d’information de la Citibank de New York et à transférer des fonds sur des comptes ouverts par des complices aux Etats-Unis, en Hollande, Finlande, Allemagne et Israël. Ce jour là, ce sont quelques 10 millions de dollars qui se sont volatilisés, détournés vers des comptes personnels. Des milliers d’épargnants américains se sont vus dépossédés du contenu de leur compte. De cet argent, seulement 400 mille dollars ont été récupérés depuis.

Les escroqueries

De même que les sollicitations à caractère frauduleux sont devenues banales par téléphone ou par courrier, le cyberespace foisonne de propositions d'investissements illégales. Il faut reconnaître qu'il se prête particulièrement à ce type de pratique parce qu'il permet d'entrer en contact instantanément avec des millions de personnes, d'afficher une apparence de respectabilité sans gros efforts et de disparaître tout aussi instantanément sans laisser de traces. On y trouve par exemple une foule d'offres de vente, de demandes d'arrhes pour des services qui ne seront jamais honorés, de loteries, de sites d'enchères, de ventes pyramidales, etc.

Un service de réclamations en ligne a récemment lancé un avertissement contre un site de petites annonces automobiles du réseau Internet. En échange d'une commission fixe de 399 dollars, ce site offrait de placer sur une page web le descriptif des voitures des particuliers désireux de les mettre en vente. Au cas où le véhicule ne serait pas vendu dans les 90 jours, il promettait de restituer au propriétaire la commission.
Evidemment, plusieurs voitures de clients, présentées sur page web, n'ont pas été vendues durant le délai imparti, mais ces derniers n'ont trouvé personne sur le site d'annonces pour leur rembourser leur argent. Ce site Internet a fermé depuis.

13) La criminalité informatique d'origine terroriste

Avec la fin de l'affrontement Est-Ouest, le terrorisme international a changé de nature, laissant la place à un terrorisme transnational. En même temps qu'il perdait ses soutiens traditionnels venant des Etats,. il s'est mis à agir indépendamment des frontières et des logiques politiques des grandes puissances, frappant seulement au gré de ses intérêts.
Les membres de ces groupes terroristes regroupent plusieurs nationalités et leurs actions ne se limitent pas à une seule région du monde. Ils peuvent tout aussi bien frapper au proche Orient que sur le territoire des Etats-Unis. En ce sens, les nouvelles technologies leur offrent des possibilités inégalées de fédérer leurs réseaux.

L'arme informatique

Dès les années 90, les groupes terroristes et paramilitaires ont eux aussi perçu les avantages que pouvait leur offrir l'informatique comme support de leurs luttes.
Internet est avant tout apparu comme un formidable outil de propagande permettant d'atteindre à bon compte un public constitué de millions de personnes.
Autre avantage de taille, il offre une infrastructure de communication très sécurisée permettant de correspondre dans le monde entier. Ainsi, il favorise le recrutement, la collecte de fonds ou encore la coordination des actions violentes à distance et à l'abri des actions des services de sécurité.
Enfin, il a rendu possible d'attaquer sans risque les infrastructures informatiques d'un pays, les institutions gouvernementales, l'armée, les grosses industries et les banques.

Les groupes islamistes l'ont parfaitement compris et se montrent particulièrement actifs sur le réseau mondial. Ils enregistrent d'ailleurs des succès non négligeables. Le Hezbollah par exemple possède un site Internet sur lequel il publie quotidiennement son idéologie et les actions violentes que ses membres portent aux forces israéliennes. Il entretient de la sorte la mobilisation et la motivation de ses sympathisants. Comme d'autres groupes terroristes acquis à la cause palestinienne, il encourage également les attaques informatiques contre Israël et ses intérêts à l'étranger. Ces dernières se multiplient notamment depuis la rupture du processus de paix. De nombreux sites officiels sont paralysés momentanément, leurs contenus étant modifiés au profit de slogans favorables à la cause palestinienne (le jeudi 26 octobre 2000, le site du ministère israélien des affaires étrangères a du être fermé, à la suite d'une salve d'attaques provenant du monde entier). Les banques et marchés de change n'échappent pas non plus aux agressions, obligeant les autorités à la vigilance et à des réactions rapides.
Le Groupe Islamique Armé algérien, qui recherchait la dispersion géographique pour assurer sa sécurité, a également eu recours à Internet pour communiquer avec ses membres. Au plus fort de son engagement, son centre de commandement était localisé en Grande-Bretagne, tandis qu'une partie de ses membres fabriquait les bombes en Belgique, les attentats étaient perpétrés quant à eux en Algérie et même en France. Il n'hésitait pas non plus à faire publier ses déclarations et revendications par ce canal.

Un nouveau terrorisme

D'après certains analystes, un type nouveau de terrorisme est en train de se constituer. Fait original, ces mouvements émergeants n'ont pas derrière eux un passé ponctué d'attentats meurtriers et ne revendiquent pas nécessairement le passage à la violence physique. Ils inscrivent néanmoins leur combat dans une lutte implacable contre la mondialisation. Les nouvelles technologies de l'information viennent à point nommé pour amplifier la puissance de leurs actions.

Certains groupes écologistes aux actions agressives et médiatiques ont le profil pour porter leur combat sur Internet. Leurs membres maîtrisent les nouvelles technologies et le crime informatique leur fournirait un excellent moyen de s'attaquer aux infrastructures des pays qu'ils dénoncent dans leur lutte. Leur arrivée dans le cyberespace sous des formes autres que pacifiques est donc annoncée pour un avenir proche.
L'Organisation Mondiale du commerce (OMC) quant à elle est déjà aux prises avec ce type de terrorisme. La présence de sites Web imitant le sien en apporte un élément de preuve. En octobre 2000, les " Yes Men ", des activistes anti-mondialisation, ont réussi grace à leur site à se faire passer pour des représentants de l'OMC. Cette situation leur a valu de recevoir une invitation officielle adressée au président de l'OMC afin de participer à une conférence sur la mondialisation des marchés
Ils y ont répondu sans hésiter par la participation d'un de leurs membres en remplacement du président prétendument dans l'impossibilité de s'y rendre. Cette tribune leur a permis de tenir un discours extrêmement caricatural mettant en exergue les avantages de l'ultra libéralisme et dénonçant en réalité implicitement ses méfaits (cf l'article et le contenu de cette conférence rocambolesque à l'adresse suivante : http://www.rtmark.com). Si cet épisode possède un aspect anecdotique, il n'en révèle pas moins l'irruption dans le cyberespace et les capacités de nuisance de ce nouveau terrorisme.

14) La criminalité informatique du fait des Etats

La dernière forme de criminalité informatique est moins connue mais bien réelle. Les Etats en sont les acteurs directs. Tandis que les sociétés deviennent de plus en plus dépendantes des

technologies de l'information et des télécommunications, la guerre de l'information s'est imposée comme un moyen crédible d'acquérir la supériorité sur l'adversaire. La suprématie ne passerait donc plus tant par la conquête ou la mise sous influence de territoires mais bien par le contrôle de l'information.
On peut distinguer deux types d'affrontement de nature plus ou moins belliqueuse.

La guerre informatique entre Etats

Des pays tels que Taiwan et la Chine cherchent à s'intimider mutuellement par des démonstrations de capacités offensives sur ce nouveau champ de bataille. Taiwan est en avance technologiquement et dispose de nombreux spécialistes en informatique. Elle n'hésite pas d'ailleurs à consacrer un budget de 300 millions de dollars à ce domaine et possède la réputation d'avoir été à l'origine de certains des virus les plus redoutables qui ont sévi sur la toile. De son côté, la Chine possède un certain retard par rapport à Taiwan mais affiche officiellement sa volonté de développer significativement ses capacités offensives et intègre désormais des scénarios de guerres informatiques dans ses exercices opérationnels.
Il existe même un courant de pensée américain avec des stratèges tels que John Arquilla et David Ronfeld qui ont conceptualisé le principe de cyberguerre. Selon eux, la révolution de l'information que vient de connaître notre époque change radicalement la nature des conflits comme l'ère industrielle l'avait fait en fournissant aux armées des moyens de destruction de masse. Leurs théories, bien que faisant l'objet de controverses, obtiennent un certain écho au Pentagone. Les budgets consacrés à ce domaine et chiffrés en milliards de dollars le prouvent.

L'intelligence économique

Les objectifs sont plus généralement d'ordre économique. Le but consiste à s'emparer de secrets industriels d'un pays tiers. Une cinquantaine de pays se livrerait de manière méthodique à ce type d'activités et parmi eux il semblerait que la Russie soit bien placée.
Les Etats-Unis ne sont pas non plus les derniers à se livrer à ce type d'activités; il suffit de considérer le programme Echelon pour s'en convaincre. Formidable outil d'envergure mondiale, d'interception et d'analyse de toutes les formes de communication dont les courriers

électroniques, il permet de fournir à la National Security Agency (NSA) des quantités d'informations d'intérêt stratégique: données économiques, stratégie des décideurs, identifications des parties prenantes en sont quelques exemples.

2. Les vulnérabilités

Le développement d'Internet se poursuit, touchant tous les secteurs de la société, en faisant notamment un espace extraordinaire de commerce, de présence des services publics, d'échange d'informations de toute nature. Tout naturellement se pose alors la question de la sécurité liée à ce média. La confrontation à la réalité du cyberespace indique que le nombre, la variété et la portée des coups infligés au quotidien aux systèmes d'information dans le monde ne peuvent être tenus pour négligeables. L'informatique est devenue une source de vulnérabilité importante dans notre société. Pour autant, le danger qu'elle sous-tend n'est pas uniforme et doit s'apprécier au regard des principales activités pratiquées sur Internet.
Après avoir donc analysé les principaux acteurs et les armes qu'ils emploient, nous nous attacherons à évaluer la nature de la menace par domaine.

21) Les facteurs généraux de vulnérabilité

L'information électronique est bien plus menacée qu'une information classique du type document papier enfermé dans un coffre. Il n'est pas nécessaire pour les contrevenants de pénétrer physiquement dans le lieu ou celle-ci est stockée ; ils peuvent même agir tout en se trouvant à l'étranger. Lorsqu'il s'agit d'un vol, il se réalise en quelques secondes par simple copiage électronique de fichiers et ne laisse quasiment aucune trace.
La criminalité informatique possède aujourd'hui au moins trois caractéristiques générales qui la rendent particulièrement redoutable et laissent les autorités plutôt démunies.

La faiblesse inhérente de la sécurité

Internet n'a pas été conçu à l'origine en intégrant les problèmes de sécurité car il se voulait un espace ouvert favorisant les échanges. Les protocoles qui le composent ont peu évolué et conservent aujourd'hui cette faiblesse de nature. A cet inconvénient s'ajoute le caractère dynamique du réseau Internet qui ne cesse de croître et au sein duquel des technologies émergeantes apparaissent régulièrement.
Les experts s'accordent donc à reconnaître qu'aucun réseau informatique, surtout s'il est connecté à Internet, ne peut être considéré comme sûr à cent pour cent. Les cas de cyberdélinquance sur les sites officiels sont d'ailleurs là pour le rappeler.

La facilité d'accès aux voies de la criminalité

A la différence de la plupart des autres formes de criminalité, la cyberdélinquance ne requiert que très peu de moyens pour des effets particulièrement spectaculaires. Un ordinateur et un modem sont dans ce domaine des armes tout à fait redoutables. Au faible coût de mise en application s'ajoute un niveau technique moyen facile à acquérir. Il suffit pour ce faire de s'intéresser à la question, de parcourir les journaux de pirates que l'on trouve dans toutes les presses, de visiter leurs sites et d'appliquer fidèlement leurs recommandations sans même saisir les principes de fonctionnement ou encore pour les plus passionnés de se rendre aux salons qu'ils organisent. Ce partage des connaissances et des outils logiciels a pour effet d'augmenter continuellement le nombre des pirates, la puissance de leurs effets et globalement leur niveau de compétence.

L'impunité

L'impunité est sans aucun doute un des facteurs qui contribue le plus à l'expansion de la délinquance informatique. Les systèmes juridiques ne sont pas aujourd'hui adaptés pour faire face à la variété des délits qui peuvent être perpétrés sur les réseaux informatiques. A cela s'ajoute la possibilité d'agir à distance, c'est-à-dire depuis des lieux où la législation reste laxiste. Les autorités philippines par exemple se sont aperçues que leur législation ne leur permettait pas de poursuivre le responsable du virus "I love you" à l'origine, comme il a été dit précédemment, de milliards de dollars de dégâts dans le monde entier.

L'impunité s'explique également par des raisons techniques. Il existe une réelle difficulté à détecter, identifier, apporter les preuves avant de mener enfin des poursuites à l'encontre du contrevenant. Le temps joue lui aussi souvent en faveur du criminel car il peut s'écouler des délais importants avant qu'une intrusion soit détectée ou qu'un virus s'active. Le contrevenant a donc bien souvent toute latitude pour disparaître.

22) La vulnérabilité de l'économie

La cybercriminalité se manifeste dans tous les secteurs d'activité de la société mais c'est dans les secteurs économiques qu'elle cause le plus de dommages, bien que ceux-ci ne soient pas toujours visibles au premier examen.
Pour les entrepreneurs, cela signifie dans un avenir proche des investissements plus lourds qu'ils ne le pensaient initialement pour assurer la sécurité de leurs réseaux.

L'intelligence économique

La cybecriminalité participe grandement, en contribuant à la fourniture de secrets industriels, à la compétition acharnée que se livrent les entreprises. Dans ce cas, il n'est plus question de pirates amateurs suivant le gré de leur inspiration dans leur exploration, mais bien de véritables professionnels entraînés, au service parfois d'un Etat étranger, et qui ciblent précisément leurs objectifs.
L'espionnage scientifique et industriel est en effet en plein essor et l'outil informatique se révèle le plus puissant moyen d'acquérir de l'information confidentielle. D'après les enquêtes de la Direction de la Surveillance du Territoire, il progresse d'environ 20% par an. Toujours d'après ce service, 19% des entreprises innovantes auraient reconnu avoir été victimes d'espionnage industriel et 40% de contrefaçon. Le montant minimum du préjudice par sinistre est de 1,7 millions de francs pour la moitié des victimes. 200.000 personnes et entreprises seraient surveillées électroniquement. Les pertes des entreprises françaises consécutives à des opérations de renseignement se chiffreraient entre 135 et 300 milliards de francs.
Aux Etats-Unis, la situation n'est pas meilleure loin s'en faut. Même Microsoft, le numéro un mondial du logiciel, a été victime d'un piratage extrêmement grave à la fin de l'année 2000.

Des intrus auraient réussi, selon les aveux de Steve Ballmer, PDG de Microsoft, à accéder au code source du système d'exploitation Windows ; ce qui, si l'information devait être confirmée, donne aux pirates tous les éléments pour reproduire à leur guise un système d'exploitation concurrent à ceux de Microsoft. Ce cambriolage informatique a déclenché une enquête du FBI. La piste actuelle privilégie l'hypothèse d'un pirate russe qui aurait eu recours à un programme de type cheval de Troie pour s'introduire dans le réseau interne.

Malgré ces chiffres et exemples édifiants, il est encore courant dans le monde de l'entreprise de rencontrer des responsables qui n'ont aucune conscience de l'exposition de leur entreprise à une pénétration de leur réseau informatique et du risque qui lui est associé.
Ils considèrent généralement avec légèreté qu'ils ne sont pas une cible intéressante ou bien que les précautions mises en œuvre sont suffisantes. Mais même les meilleures solutions techniques ne peuvent rester efficaces indéfiniment dans un contexte technologique évolutif et face à des techniques d'attaques qui elles-mêmes se perfectionnent.
D'autre part, le réseau informatique des entreprises est devenu si complexe et les flux entre les divers services si nombreux que la plupart des gens ne savent pas bien l'employer et encore moins le maîtriser, ouvrant ainsi la porte à des comportements dangereux du point de vue de la sécurité.
Enfin, la nature du vol électronique d'informations protégées est pernicieuse parce qu'il procède par copie et ne laisse pas de traces d'effraction apparente. De fait, l'information, le secret de fabrication, le carnet d'adresse des clients et les projets stratégiques restent toujours disponibles mais ils ont perdu tout ou partie de leur valeur.

La fraude informatique

Le secteur économique doit également faire face à la fraude informatique. En la matière, le domaine le plus touché est celui des télécommunications, suivi par le milieu de l'informatique.
Pour la France, le préjudice comptabilisé se chiffre en centaines de millions de francs, mais le montant exact de la fraude semble être ignoré dans la quasi-totalité des cas recensés.
Concernant les affaires spécifiquement liées au réseau Internet, la très grande majorité des cas de fraudes porte sur des escroqueries commises en matière de commerce électronique. Leur nombre est en augmentation exponentielle, ce qui n'a rien d'étonnant lorsque l'on songe que le

commerce mondial sur Internet représente un marché de centaines de millions de francs. Ces délits s'effectuent le plus souvent à l'aide des références de cartes bancaires utilisées frauduleusement.
Les moyens proposés pour sécuriser complètement les échanges entre commerçants et clients sont nombreux mais aucun d'entre eux ne semble en réalité complètement fiable.

Le sabotage informatique

La malveillance informatique n'est pas un phénomène marginal: 40% des entreprises françaises ont reconnu avoir subi, au cours des 5 dernières années, plus de 5 actes de malveillance ayant entraîné une perte financière ou d'actifs.
Ses conséquences peuvent être dramatiques lorsque l'on sait que pour la grande majorité des entreprises au-delà d'une semaine sans système informatique, elles ne savent plus travailler et que près de 80 % des P.M.E. qui subissent un sinistre informatique important déposent le bilan dans les 2 ans qui suivent.

La malveillance informatique procède généralement d'actes irréfléchis de pirates qui agissent directement sur le contenu des disques durs après y avoir pénétré par effraction ou par le biais de virus informatiques.
Cependant, il se pourrait que certains cas de sabotage aient d'autres motivations comme celles par exemple d'obtenir un avantage économique sur des concurrents.
Les attaques coordonnées en février 2000 des sites Internet les plus populaires laissent les enquêteurs perplexes, d'autant que les groupes de pirates parfois si prompts à revendiquer leurs exploits se montrent discrets ou condamnent. Citons parmi les sites visés, Yahoo, premier moteur de recherche sur Internet, CNN grande chaîne de télévision internationale ou Amazon premier libraire en ligne. Ces attaques d'un nouveau type ont bloqué les serveurs des sites visés pendant plusieurs heures en les submergeant d'informations: la quantité moyenne d'informations reçue par seconde dépassait dans certains cas celle reçue pendant toute une année. Le succès obtenu et l'impact médiatique ont été tels que l'image de marque des sites visés en a été dégradée, faisant baisser par contrecoup leurs cours boursiers et entraînant même une baisse du Nasdaq puis de l'ensemble des places boursières internationales.

23) La vulnérabilité des institutions

Les institutions sont obligées, sous peine de perdre leur légitimité, de suivre l'évolution de la société et de se positionner sur ce nouvel espace de vie qu'est Internet. Ce dernier peut s'apparenter à un instrument puissant d'exercice du pouvoir démocratique comme moyen d'information et de gestion quotidienne des relations entre le citoyen et l'Etat.
Cependant, comme le monde de l'entreprise, les institutions souffrent d'agressions informatiques importantes en raison précisément de l'existence des passerelles Internet qui les lient aux usagers.

Des tribunes d'opposition au pouvoir

Représentant sur Internet le pouvoir en place, elles deviennent effectivement la cible de ses opposants, qu'ils soient sur le territoire national ou à l'extérieur de celui-ci comme cela a toujours été le cas des symboles de l'Etat.
Les pages officielles des sites gouvernementaux de nombreux pays ont déjà dans un passé récent fait l'objet d'actes hostiles.
Récemment, des pirates probablement de nationalité chinoise ont visité en quelques jours une quinzaine de sites d'organismes gouvernementaux au Japon. Ils ont modifié leur contenu par des messages en anglais et en chinois insultants, dénoncé le massacre de Nankin perpétré par les troupes japonaises en 1937 ou tout simplement redirigé les utilisateurs vers des sites pornographiques.
Nul ne peut garantir qu'une situation analogue ne se produise un jour en France du fait de tel ou tel groupe indépendantiste et de ses soutiens extérieurs hostiles à notre présence dans une région donnée du monde. La pénétration d'un ministère comme celui de l'Intérieur ou encore de celui de la Santé avec atteinte à l'intégrité de données confidentielles aurait des implications plus que fâcheuses et certainement un impact politique. Cette hypothèse d'agression est d'ailleurs prise très au sérieux au sommet de l'Etat et explique la décision d'intégrer le Service

Central de la Sécurité des Services d'Information au SGDN depuis 1998 et de confier à ce dernier cette nouvelle dimension de la sécurité du pays.
Le Japon quant à lui s'est brutalement aperçu de l'extrême vulnérabilité de ses réseaux informatiques.
Pour avoir tardé à prendre conscience du problème, il est probablement aujourd'hui le pays le plus exposé aux attaques des pirates.
Autre exemple, pendant l'été 1996, des pirates se sont introduits sur le serveur web de l'US Justice Department et y ont plaçé des croix gammées et des images d'Adolf Hitler. Ils voulaient protester contre la position du gouvernement américain à contrôler l'Internet (.cf. Annexe 3)

Des détournements d'images

Mais les institutions sont également confrontées à une autre difficulté sérieuse en terme d'image. En effet, des sites choisissent des noms d'institutions qui leur donnent un caractère officiel, s'assurant ainsi une fréquentation importante, mais pratiquent en réalité des activités sans lien direct avec cette institution et contribuent à les décrédibiliser fortement.
A l'adresse suivante : " http://www.whitehouse.com/ " qui laisse penser en toute bonne foi à celle de la Maison Blanche on trouve en réalité un site pornographique.

24) La vulnérabilité des forces armées

La vulnérabilité des infrastructures

Initialement, les réseaux militaires étaient inaccessibles de l'extérieur à des utilisateurs civils. Pourtant, insensiblement les armées n'ont pas pu résister totalement aux facilités offertes par Internet en particulier en tant qu'outil de communication efficace et bon marché. Son emploi se trouve en principe limité aux sites officiels informant le grand public des activités des armées qui sont vulnérables au même titre que tous les sites officiels. On peut également douter de la parfaite séparation de tous les réseaux et qu'il n'existe pas dans quelques organismes dépendant du ministère de la Défense des ordinateurs connectés simultanément sur des réseaux

internes et sur Internet. La proximité de postes Internet et Défense est d'autre part favorable à la transmission de virus du premier réseau vers le second.
L'utilisation du courrier électronique, en particulier lors des opérations extérieures, équivaut à un véritable réservoir de renseignements déterminants pour qui voudrait se donner la peine d'y puiser. Ce fut pense-t-on le cas d'un groupe de pirates hollandais pendant la guerre du Golfe. Il aurait offert ses services mais heureusement sans succès à Saddam Hussein contre un million de dollars.

Internet n'est pas le seul facteur de vulnérabilité pour les armées. Un mouvement d'informatisation générale des équipements est en cours dans les armées. Ce processus qui n'en est encore qu'à son début touche les systèmes d'information nationaux, pour lesquels il s'agit de passer d'une logique de réseaux dédiés à une logique de réseaux interconnectés multiservices.
Ce processus concerne également les forces pour lesquelles l'intérêt de la numérisation du champ de bataille s'est fait jour. Les systèmes de commandement des forces ne sont déjà plus des projets mais existent bel et bien et agissent comme de véritables multiplicateurs de forces. Ils participent effectivement à accroître les capacités de recueil, de traitement et de transmission de l'information.
Les avantages que procure cette informatisation générale sont énormes et aucune armée moderne ne pourrait en faire l'économie. Elle favorise cependant aussi la vulnérabilité de nos forces, dans la mesure où les interconnexions sont nombreuses et ne se limitent pas uniquement à des liens nationaux. Les risques de pénétration indirecte de notre système de défense s'accroissent donc parallèlement à la montée en puissance des réseaux, le maillon le plus faible servant de porte d'entrée.
Un autre point de vulnérabilité est l'adoption maintenant quasi-systématique d'architectures à base de systèmes civils se voulant de plus en plus ouverts et donnant accès à des bases de données distantes. Les techniques de piratages existantes ne peuvent que s'en trouver renforcées puisqu'elles deviennent dès lors directement applicables aux réseaux des armées.

Le risque asymétrique

Les derniers conflits ayant consacré la supériorité technologique et numérique des forces occidentales dans un affrontement direct, il devient évident que la recherche de nouveaux champs de bataille s'impose pour un adversaire déterminé et avisé. Nos systèmes d'information feront probablement partie des cibles visées car, sans en exagérer les effets et lui conférer à elle seule le moyen de renverser l'équilibre des forces, une attaque informatique d'envergure soigneusement préparée possède une capacité de nuisance pouvant porter atteinte à la sécurité nationale sans grand péril pour celui qui la mène. De fait, une cyberguerre devient aux mains du faible un instrument particulièrement adapté pour s'en prendre au fort.

Avantage de premier ordre, une cyberguerre donne à son utilisateur l'initiative d'une attaque de niveau stratégique car elle peut toucher d'emblée des centres vitaux de l'adversaire. Ce type d'attaque a de plus l'avantage de n'exposer l'agresseur qu'à des risques réduits. La phase de montée en puissance peut être extrêmement discrète en raison de la nature même des matériels utilisés. En outre sur le plan technique, il n'est pas toujours aisé d'identifier l'origine des attaques. En supposant que ce soit le cas, il est également fort probable qu'elles apparaissent provenir de points multiples du monde sans relations directes apparentes avec les belligérants. Même formellement reconnu, si l'auteur appartient à la catégorie des pays en voie de développement, il devient quasiment insensible à des représailles de même nature. Quant à une réponse par des frappes militaires, elle serait difficilement justifiable de la part d'une démocratie et l'opinion publique serait susceptible de les condamner fermement.

Enfin, en terme d'effort de défense à consentir de la part d'un pays pour s'y préparer, la cyberguerre constitue une véritable aubaine. Elle ne requiert en effet pour l'équipement des forces que des budgets modestes puisqu'elle ne fait appel qu'à des matériels de la gamme civile. En comparaison des coûts engendrés par les grands programmes d'armement conventionnels tels que chars ou avions de chasse, autant dire que cela est tout à fait négligeable. D'autre part, les techniques d'agressions à mettre en œuvre sont directement disponibles sur Internet et ne demandent donc pas des programmes de recherche, des expérimentations et des mises au point longues et incertaines. Seules la formation des spécialistes et surtout la planification des opérations correspondent à un investissement véritable.

3. Le défi de la lutte contre la cybercriminalité

La lutte contre la cybercriminalité est un défi difficile à relever d'autant que les gouvernements commencent seulement à prendre conscience des enjeux réels pour la société.
Cette lutte soulève, entre autres difficultés, la complexité des problèmes techniques, la prise en compte d'un nombre de délinquants extêmement élevé et le caractère d'extra-territorialité lié à la plupart des délits.
D'autre part, cette lutte ne prend tout son sens que si elle traite effectivement toutes les formes de criminalité informatique et en particulier celles susceptibles de mettre en péril la sécurité nationale. En ce sens, la maîtrise des formes organisées de criminalité informatique est sans doute le véritable objectif à atteindre si l'on veut garantir la pérennité des infrastructures informatiques.

31) Le cas des formes individuelles de cybercriminalité

L'idée du renforcement des protections est intéressante. Elle doit être conduite à plusieurs niveaux et repose au départ sur de simples notions de bon sens. Ainsi, le principe du cloisonnement des réseaux à protéger avec Internet est une option à privilégier chaque fois que possible. La formation des utilisateurs est également une voie à ne pas négliger et de simples conseils sur l'emploi de mots de passe constituent déjà un pas important vers la sécurité de l'ensemble du réseau.
Les moyens techniques viennent ensuite pour compléter ces dispositions de base. Ce sont aujourd'hui des instruments très puissants mais il faut quand même savoir que malgré toute leur sophistication, ils ne permettent pas de protéger les réseaux dans leur intégralité.

Le renforcement des barrières techniques

Toute une panoplie de technologies a été développée pour aider les organismes à sécuriser leurs systèmes d'information contre les intrusions et les attaques virales. Ces technologies détectent les activités suspectes ou inhabituelles et réagissent contre les événements qui affectent la sécurité.

Le but de ces dispositifs est de garantir à la fois l'authentification des utilisateurs des moyens informatiques d'une part et la confidentialité, l'intégrité et la disponibilité des informations détenues d'autre part.

Trois voies offrent des perspectives de sécurité intéressantes. La première concerne les dispositifs « pare-feu » (firewall). Il s'agit d'une technologie de contrôle d'accès qui empêche précisément les accès non autorisés aux ressources en plaçant un filtre entre le réseau à protéger et le réseau Internet. Il est intéressant de noter que dans nombre d'organismes les pare feux ne prennent pas en compte le courrier électronique et laissent donc la porte d'entrée favorite des pirates ouverte.

Les pare-feu ne sont en général pas efficaces contre les virus. Les possibilités de dissimuler ces petits morceaux de code exécutable que constituent les virus sont presque infinies aussi est-ce la raison qui les fait passer inaperçus dans les échanges sur les réseaux. Il est donc nécessaire d'adjoindre aux pare-feu des outils d'éradication des virus. Ces derniers ne demeureront eux-mêmes opérationnels que si leurs bases de données d'identification de virus sont remises à jour régulièrement.
Il est de même recommandé de se doter d'instruments d'audit du réseau qui ont pour vocation d'enregistrer toutes les activités et d'analyser l'ensemble des opérations afin de déceler celles de nature suspecte (échange d'informations avec un correspondant à l'étranger, pics d'activité en dehors des heures habituelles de travail en sont quelques illustrations).

Enfin, le renforcement de la sécurité gagnerait beaucoup à un usage plus répandu de la cryptographie[1]. Le succès des actes de piraterie tient en effet largement à l'accesssibilité de l'information lorsque l'intrusion a réussi. Il n'y a qu'à songer aux millions de messages

[1] La cryptographie est le processus de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes dont l'effet est réversible.
Les techniques de cryptographie représentent des enjeux économiques, stratégiques et juridiques considérables. Procédé d'origine militaire, la cryptographie est également considérée comme un enjeu de sécurité intérieure et extérieure par un certain nombre de gouvernements.
Les besoins légitimes en cryptographie des utilisateurs ont été reconnus par la loi du 26 juillet 1996, qui fait référence à la protection des informations et au développement des communications et des transactions sécurisées.
Cependant, la France, invoquant la nécessité de préserver les intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, a maintenu, malgré plusieurs réformes successives, une réglementation contraignante de la cryptographie.

électroniques qui sont véhiculés sur Internet chaque jour et il est facile d'imaginer la collecte d'informations que les dispositifs de détection ("sniffer") sont à même d'opérer.
Le recours à la cryptographie serait un moyen puissant d'empêcher les cybercriminels de saisir le contenu de l'information volée, que ce soit dans une mémoire d'ordinateur ou dans un échange d'informations entre ordinateurs. En plus de la préservation de la confidentialité des données, la cryptographie présente l'avantage supplémentaire de pouvoir dans certaines conditions protéger leur intégrité et srervir à l'authentification des signatures électroniques.
Il faut souligner toutefois le caractère à double tranchant de cette technique qui donnerait également aux criminels la possibilité de protéger une partie de leurs activités.

La levée de l'impunité

Le cyberdélinquant compte beaucoup, pour commettre ses méfaits, sur l'impréparation des législations actuelles à traiter les délits informatiques. Il se joue habilement des ambiguïtés pour évoluer aux frontières du droit et des Etats. Toutes les facilités lui sont d'ailleurs offertes lorsque l'on sait que plusieurs pays ne mentionnent dans leur code pénal aucun délit lié à l'informatique.
En fait, il y aurait lieu d'harmoniser d'urgence les législations internationales car le problème de la criminalité informatique ne peut se satisfaire d'une seule approche territoriale. Le cyberespace devra à terme se voir appliquer une réglementation juridique du type de celle que l'on réserve aux activités spatiales ou à des questions de dimension mondiale telles que le transport des produits pétroliers et la pêche.
Des initiatives sont déjà prises en ce sens depuis quelques années en Europe. C'est ainsi que le Conseil de l'Europe a présenté en 2000 un projet de convention internationale sur la cybercriminalité. Le texte proposé a pour objectif d'harmoniser les législations et permettrait notamment la lutte contre le piratage, la fraude financière, l'usage des virus informatiques ou la pédophilie sur Internet.
Il faut toutefois préciser que ce projet a provoqué une impressionnante levée de boucliers de la part de nombreuses associations de défense des droits des internautes.

Toujours dans cette optique de levée de l'impunité, il devient important d'organiser la surveillance du réseau Internet et des activités qui s'y pratiquent. En France, les services de

police se sont investis dans cette mission, même si les efforts consentis demeurent modestes. Parmi les organismes responsables, on trouve la BCRCI de la gendarmerie(Brigade Centrale de Répression de la Criminalité Informatique), le SEFTI de la police judiciaire (Service d'enquêtes sur les fraudes aux technologies de l'information) et la DSSI de la Direction de surveillance du territoire (Directoire de la Sécurité des Systèmes d'Information).
Toutefois, ces activités de surveillance ne doivent pas se restreindre aux seuls services de police mais doivent mobiliser l'ensemble des utilisateurs.
Des exemples existent déjà : des institutions comme la Direction Générale de l'Armement, le ministère de l'Intérieur, ou encore la banque BNP se sont regroupées en 1993 au sein d'un organisme, le RECIF (Recherche et Etudes sur la Criminalité Informatique Française), pour réagir aux menaces d'intrusion. Les citoyens ayant également un rôle à jouer, la police hollandaise les encourage à signaler par courrier électronique les cas de pornographie, impliquant des enfants, qu'ils pourraient rencontrer.

32) Le cas des formes organisées de cybercriminalité

Si la prise de mesures de protection sérieuses est la condition première de sécurité des réseaux informatiques, il est évident que cette attitude a des limites. Les défenses finiront toujours par être franchies par les pirates qui conserveront toujours un temps d'avance sur les systèmes de protection.
La recherche de solutions alternatives est donc nécessaire, dans le cas de la cybercriminalité organisée, en raison de son potentiel de nuisance. Celles-ci doivent s'envisager en terme de capacité d'action offensive visant à prévenir le plus possible les menaces avant qu'elles ne se matérialisent.

La connaissance de la menace

C'est en premier lieu par une connaissance précise de la menace qu'il faudrait commencer pour en mesurer par avance les effets possibles si elle devait se matérialiser. Il faut pour cela s'intéresser aux techniques d'attaque en cours aujourd'hui. Dans ce but, il est nécessaire de créer de nouvelles spécialités au sein des services de sécurité mais également au sein des

armées et de former au plus vite les experts correspondants. Assurer simultanément, avec ces spécialistes, une veille technologique permanente sur Internet s'avère indispensable, pour suivre l'évolution constante à laquelle sont soumis les systèmes d'information et détecter les nouvelles armes que l'imagination sans limites des pirates ne cesse de mettre au point et d'expérimenter.

La dissuasion

Enfin, le développement d'une capacité d'agression informatique crédible serait en lui seul un facteur dissuasif venant d'un pays aussi moderne que le nôtre. Il ferait en effet peser un niveau de menace difficilement mesurable sur un adversaire également dépendant vis-à-vis de l'informatique. Il lui laisserait penser que la supériorité dans ce domaine ne lui est pas nécessairement acquise et qu'il pourrait avoir plus à perdre qu'à gagner à engager la lutte sur ce terrain.

Il faut donc être en mesure d'acquérir des armes de guerre informatique comme des moyens d'intrusion ou des virus par exemple, les perfectionner et bien sûr mettre au point les défenses correspondantes.

Il est également nécessaire d'étudier les systèmes d'information des pays ou des groupes terroristes susceptibles de représenter une menace, afin d'identifier par avance leurs principales vulnérabilités et peut-être même pour quelques-uns d'y installer des dispositifs de type chevaux de Troie en mesure d'être activés si la nécessité s'en faisait sentir.

Le principe de recruter dans la population des pirates informatiques pour des programmes bien spécifiques, bien entendu en s'entourant d'un maximum de précautions, n'est pas non plus à rejeter sans une réflexion plus approfondie. Les Etats-Unis ont fait ce choix, comme souvent pragmatique, après s'être aperçus de tout le parti que l'on pouvait tirer de l'extrême compétence de certains de ces individus, qui parallèlement cessaient leurs activités illégales et déstabilisantes.

CONCLUSION

La criminalité informatique n'est pas une criminalité classique. Sa nature virtuelle et l'absence de violence dans ses modes d'action font qu'elle ne suscite pas encore réellement de sentiment d'insécurité ni même d'image négative du délinquant. Au contraire, ce dernier force la plupart du temps le respect par son ingéniosité. L'image qu'en donnent d'ailleurs les médias se résume à celle de l'informaticien isolé se livrant de manière totalement gratuite à quelques démonstrations techniques spectaculaires mais sans gravité réelle.

Ce serait pourtant une erreur de ne pas prendre cette forme de criminalité au sérieux. Elle se traduit déjà par des pertes financières énormes, notamment dans le domaine de la contrefaçon et du commerce électronique, sans compter que son coût est aujourd'hui largement sous-évaluée. En effet, la plupart des délits échappent à toute plainte, tant les victimes se sentent gênées de reconnaître une agression informatique qui nuirait à l'image de leur société ou de l'organisme financier qu'elles représentent.
Mais il ya plus grave: des formes organisées de criminalité informatique sont en train de se constituer, démontrant des capacités tout à fait redoutables et hors de tout contrôle gouvernemental.
Au service de la grande criminalité, elles organisent différents trafics transnationaux ou réseaux pornographiques. Parfois aux mains de groupes terroristes, elles accroissent l'efficacité de leurs actions et compliquent grandement la tâches des services de sécurité qui éprouvent des difficultés à reconstituer leur structure hiérarchique. Les Etats eux-mêmes sont impliqués, aujourd'hui par le biais de l'intelligence économique pratiquée parfois à grande échelle, et bientôt probablement par le biais de la guerre informatique à laquelle certains Etats se préparent sérieusement.

Les moyens de lutte passent nécessairement par un large éventail de dispositions, qui vont de l'adoption généralisée de technologies de protection comme la cryptographie à la coordination des efforts au niveau international, en particulier dans le domaine législatif.

Cependant le traitement des formes organisées de criminalité informatique demande probablement un investissement supplémentaire. Les services de sécurité et les forces armées doivent s'efforcer d'acquérir par la veille technologique une compétence technique de la menace mais aussi des capacités informatiques offensives de même nature que les cybercriminels auxquels ils sont opposés.

Ce n'est qu'au prix d'un tel effort qu'un effet dissuasif pourra fonctionner et limiter les ardeurs de ces derniers. Le cas échéant, cette option permettrait également, face à l'éventualité d'une cyberattaque, d'appliquer une riposte véritablement efficace et seule en mesure de faire cesser l'agression.

BIBLIOGRAPHIE

« Guerres dans le cyberespace » éditions de La Découverte, Jean GUISNEL

Penser la cyberguerre – Le monde diplomatique Août 1999 – Francis PISANI
http://www.monde-diplomatique.fr/1999/08/PISANI/12382.html/

Petits débats sur Echelon – Le monde diplomatique
http://www.monde-diplomatique.fr/dossiers/echelon/

Un ver de terre chinois à l'origine du piratage de Microsoft – Le Monde interactif
http://interactif.le monde.fr/article/0,3649,2865—111077-0,FF.html

Les nouveaux pirates - Le Monde interactif 10 février 2000
http://interactif.le monde.fr/article/0,2320,dos-42183-MIA-4-2039-,00.html

Bracing for guerrilla warfare in cyberspace
http://www.cnn.com/TECH/specials/hackers/cyberterror/

Intelligence collection for asymetric threats – Part two – Jane's Intelligence Review November 2000

Cyberspace : A new medium for Communication, Command and Control by Extremists – Michael Whine - http://www.ict.org.il/articles/cyberspace.htm

La menace de cyberguerre appelle tous les secteurs a une vigilance constante – Entretien avec le sénateur Jon Kyl –
http://www.usinfo.state.gov/journal/itps/1198/ijpf/frkyl.htm

Cyberespace et Droit International : pour un nouveau Jus Communicationis – Jean Jacques LAVENUE Professeur à l'université de Lille II –
http://www.univ-lille2.fr/droit/enseignants/lavenue/cyberart.htm

Résumé du projet de loi relative à la criminalité informatique – Conseil des ministres du 14 octobre 1999 – http://www.users.skynet.be/sky94987/fgov/99104comf.htm

Les législations nationales sont « trop archaiques » pour lutter contre le cybercrime
http://interactif.lemonde.fr/squelette/pour_imprimer/0,5614,2866—128088-0,00.html

Computer Crime : A Criminological Overview- Peter GRABOWSKY Australian Institute of Criminology –
http://www.univ-lille2.fr/droit/enseignants/lavenue/cyberart.htm

Cyberguerre et sécurité nationale –
http://www.ifrance.com/Scpolundi/Cyberguerre/Cyber-guerre.htm?

L'armée chinoise envisage de recruter des hackers – ZDNET
http://www.zdnet.fr/actu/soci/a0010356.html

Securite sur Internet
http://xtream.online.fr/project/securite.html

L’hacktivisme : petite histoire de la contestation dans le cyber-espace – L’ornithoN°16
http://www.ornitho.org/numero16/articles/hack.html

Annexe 1 : Sécurité sur Internet

- **INTERNET DANS LE MONDE**

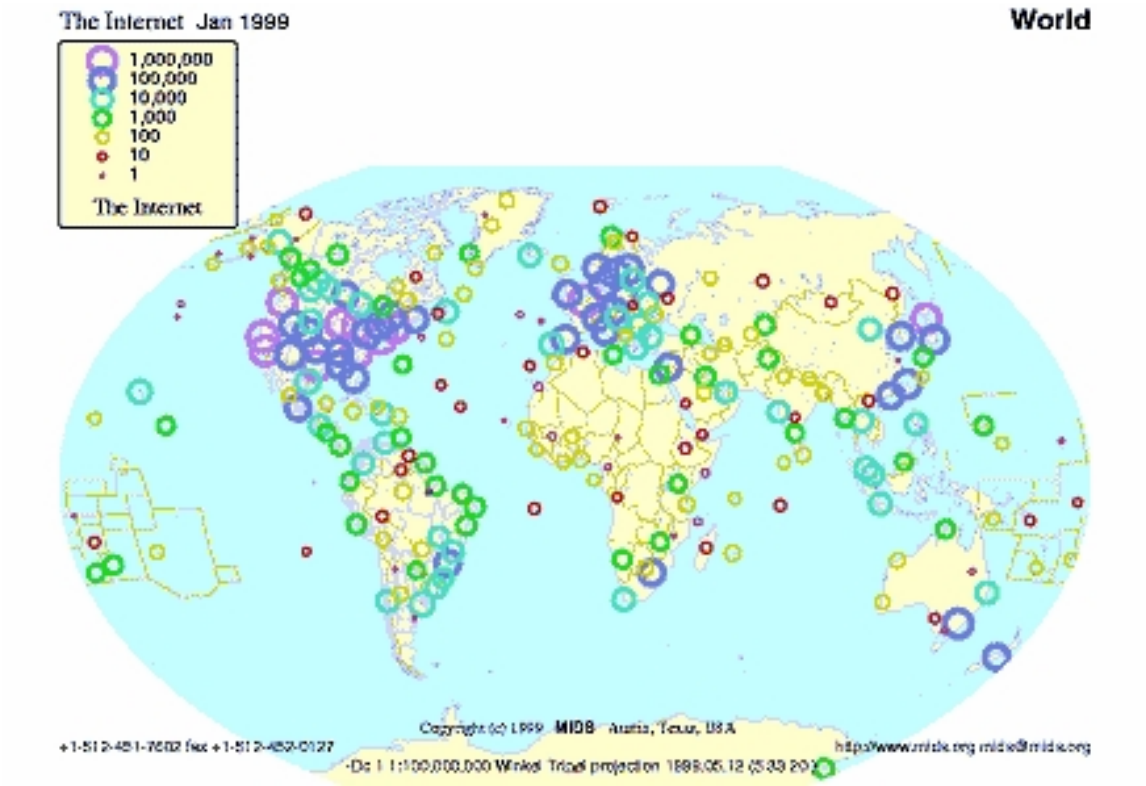
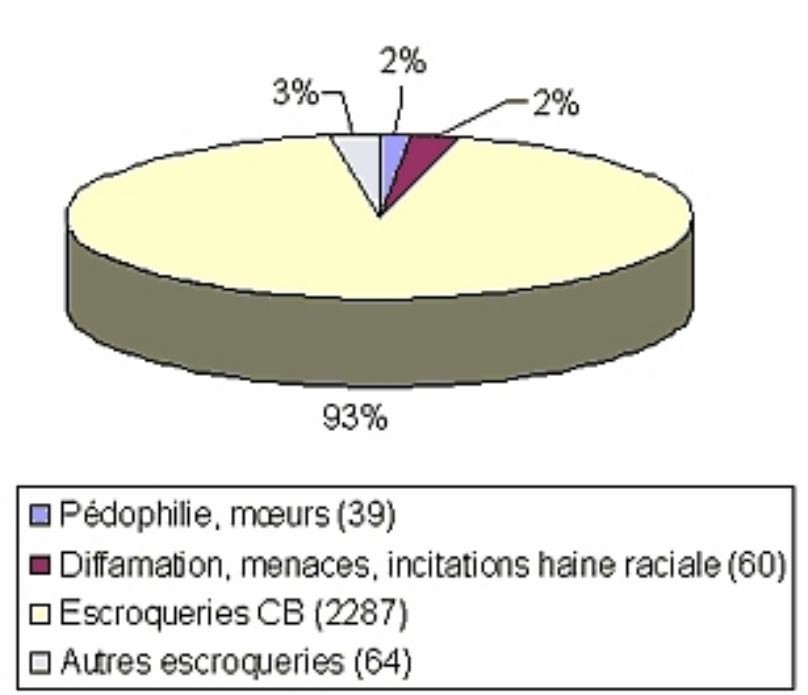


Illustration des principales connections Internet

- **DONNEES STATISTIQUES SUR LA CRIMINALITE EN FRANCE**

Source : Document officiel du ministère français de l'Intérieur - Direction centrale de la police judiciaire

Les chiffres disponibles, fournis par la police et la gendarmerie nationales permettent d'avoir une vision sur les actes délictueux commis en France. Ils montrent une forte proportion d'escroqueries liées à la carte bleue. Il faut cependant remarquer que beaucoup de délits ne font pas l'objet de plaintes et ne rentrent donc pas dans les chiffres de la criminalité.



Annexe 2 : Desription de quelques techniques d'attaques en cours

- **Le « social engineering »:**

C'est un terme utilisé parmi les pirates pour une technique d'intrusion sur un système qui repose sur les points faibles des personnes qui sont en relation avec un système informatique plutôt que sur le logiciel. Le but est de piéger les gens en leur faisant révéler leur mot de passe ou toute autre information qui pourrait compromettre la sécurité du système informatique.

Le piège classique est de faire croire aux utilisateurs du système que leur mot de passe est demandé d'urgence par l'administrateur du réseau.
Une autre forme de social engineering va jusqu'à deviner le mot de passe d'un utilisateur. Les gens qui peuvent trouver des informations sur un utilisateur, peuvent
utiliser ces informations pour deviner le mot de passe de ce dernier. Par exemple, le prénom de ses enfants, leur date de naissance ou bien encore la plaque

- **Le « crackage » de mot de passe :**

Les mots de passe sont très important parce qu'ils sont la première ligne de défense contre les attaques sur un système.
La manière la plus classique pour un pirate d'obtenir un mot de passe est par l'intermédiaire d'une attaque avec un dictionnaire. Dans ce genre d'attaque, le pirate utilise un dictionnaire de mots et de noms propres, et il les essaie un à un pour vérifier si le mot de passe est valide. Bien évidemment, ces attaques ne se font pas « à la main », mais avec des programmes qui peuvent deviner des centaines voire des milliers de mots de passe à la seconde.
De plus la communauté des pirates a construit de gros dictionnaires spécialement conçus pour cracker les mots de passe.

- **Le « sniffing » des mots de passe:**

Si un pirate ne peut pas deviner un mot de passe, alors il a d'autres outils pour l'obtenir. Une façon qui est devenue assez populaire est le « sniffing » de mots de passe. La plupart des réseaux utilisent la technologie de « broadcasting » ce qui signifie que chaque message qu'un ordinateur transmet sur un réseau peut être lu par n'importe quel ordinateur situé sur le réseau. En pratique, tous les ordinateurs sauf le destinataire du message vont s'apercevoir que le message n'est pas destiné pour eux et vont donc l'ignorer.
Les piratess ont des programmes qui lisent tous les messages qui circulent et repèrent les mots de passe des personnes qui se connectent sur un ordinateur à travers un réseau.

- **L'intrusion au moyen d'un cheval de Troie.**

Un cheval de Troie est une série d'instructions qui se cache dans un autre programme apparemment au dessus de tout soupçon. Quand la victime lance ce programme, elle lance par la même le cheval de Troie caché.
Le cheval de Troie installé à l'intérieur du programme peut permettre quand il est exécuté

d’ouvrir l’accès au système, il peut tout aussi bien activer un virus.

- **l’attaque par virus**

Un virus est une séquence d’instructions informatiques, glissée clandestinement dans un ordinateur, ayant pour conséquence une modification des données internes et pouvant se manifester par une baisse de performances, des pertes de données et, pour les plus sévères une mise hors service totale de l’ordinateur.
Le courrier électronique est devenu aujourd’hui le vecteur principal de leur dissémination.

- **le déni de service**

Une autre technique apparue récemment est celle de l’inondation du serveur visé sous une avalanche de messages entrant et le paralysant ainsi totalement.

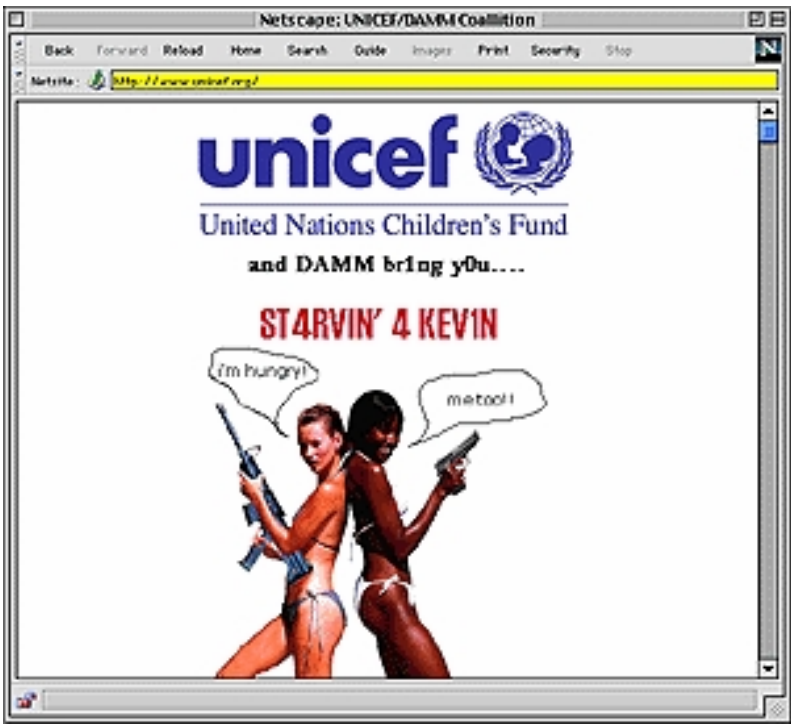
annexe 3 : Exemples d'attaques de sites officiels

- **Le New York Times**

La page principale du journal New York Times s'est fait piraté le dimanche 13 septembre 1998 par un groupe se dénommant « Hacking for Girlies » (HFG). Le texte, écrit dans un anglais hésitant mais ordurier, est aussi agrémenté de photos de femmes nues réclamait la libération de Kevin Mitnick, un célèbre hacker emprisonné depuis 3 ans. Le New York Times décidera finalement de fermer le site pour la journée, faute de faire mieux.
Ce quotidien avait la réputation d'être l'un des mieux protégés.

- **L'Unicef**

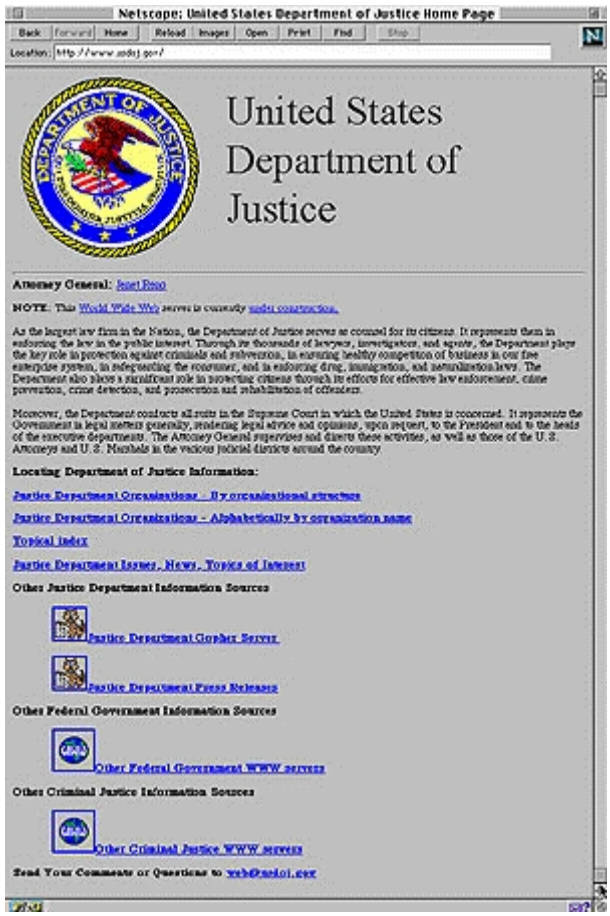
Le site Web de l'Unicef a été piraté le 7 janvier 1998. Là encore les pirates réclament la libération de Kevin Mitnick.



- **Le Département de la Justice américain**

Le site du Département de la Justice américain (US Department of Justice) a été piraté samedi 17 août 1996. Ce piratage était une protestation contre les efforts de l'administration de réglementer l'Internet.

Page d'accueil avant le piratage :



Page d'accueil après le piratage :