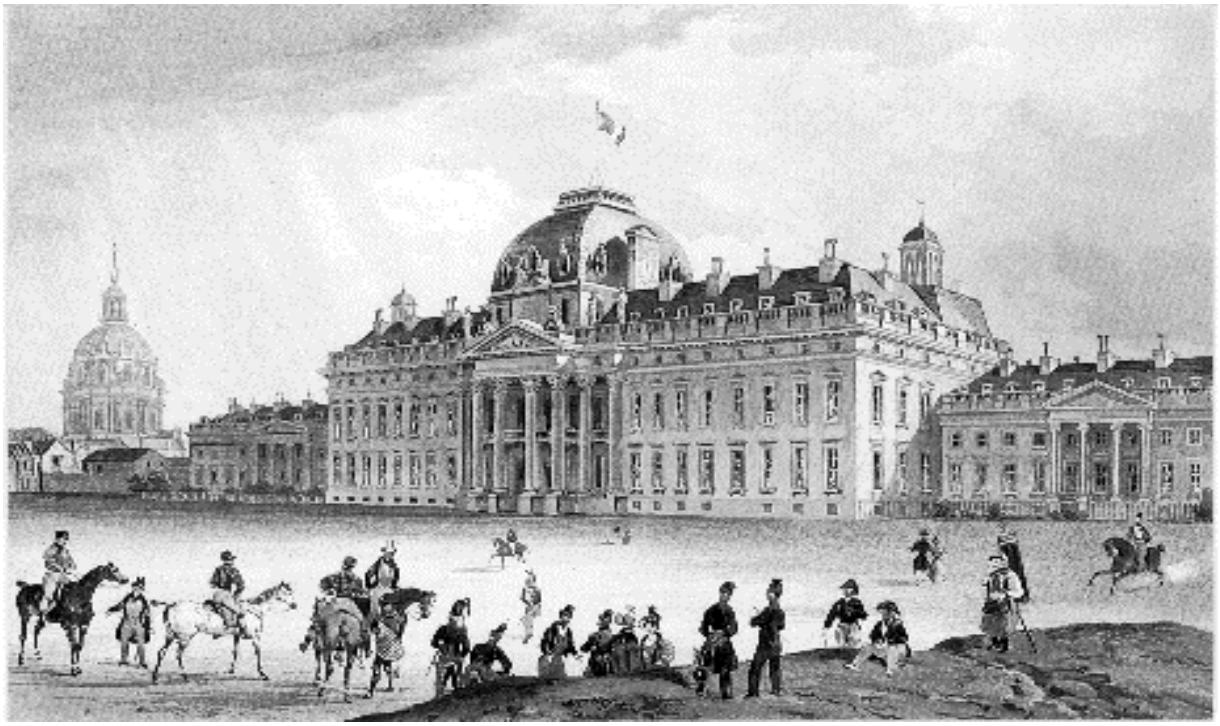
LE « CYBERTERRORISME »
MYTHE OU RÉALITÉ ?



Mémoire de géopolitique

du Lieutenant-Colonel Jean-Marie GRIMAL

dans le cadre du séminaire sur

"Les menaces non militaires de niveau stratégique"

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

Mai 2002

Université Panthéon-Assas
Paris II *Droit - Économie - Sciences Sociales*

SOMMAIRE :

"Cyberterrorisme" : mythe ou réalité ?
"Cybermenaces", oui ! Mais "cyberterrorisme" ?

"Cyberterrorisme" : mythe ou réalité ?
"Cybermenaces", oui ! Mais "cyberterrorisme" ?

<u>Introduction</u> :

"Le cyberespace est 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" Richard TRACY.[1]

"Nous découvrirons hélas qu'un adversaire décidé et doté de moyens financiers importants aura la capacité - j'insiste sur le mot capacité - de faire, de mener des guerres contre des Etats-Nations et des sphères d'influences politiques ou économiques comme jamais auparavant. Nous verrons le conflit international sur les autoroutes mondiales de l'information comme sur nos structures nationales d'information. Dès maintenant nous devons commencer à nous défendre", Winn SCHWARTAU.[2]

Ces propos alarmants sont-ils le fruit d'une imagination paranoïaque ou bien reflètent-ils une inquiétante réalité pour laquelle le "cyberterrorisme" constituerait une menace nouvelle ? La thèse, ici présentée, apporte une réponse médiane.

"Cyberterrorisme" : que recouvre réellement ce néologisme ? Est-il un mythe ou une réalité ? Quelles sont les frontières entre guerre de (pour, contre) l'information, la guerre électronique, le piratage informatique et le terrorisme informatique ? La "cyber-terreur" est-elle une menace pour le monde d'aujourd'hui ou pour celui de demain ? Dans l'ère du numérique, la terreur a-t-elle une place ? N'y a-t-il pas un excès d'alarmisme ? Si oui, à qui profite-t-il ? Une organisation terroriste trouve-t-elle plus d'intérêts à utiliser les réseaux informatiques soit comme cible, soit comme arme, dans le but de poursuivre son combat, habituellement conduit par des attentats ou des enlèvements ?

Autant de problématiques complexes auxquelles j'apporterai une réflexion personnelle, sur un sujet parfois technique mais toujours opaque. Il est, en effet, particulièrement ardu de distinguer dans le "cybermonde", et les commentaires qu'il suscite, ce qui tient du mensonge ou de la vérité, du mythe ou de la réalité, de la désinformation ou de l'information, de la menace ou de la paix. Comme l'écrit F.B.HUYGHE [3] : *"Le plus jeune média du monde réactive le plus archaïque : la rumeur"*. Aussi, cette thèse n'aura pas valeur de dogme ou de vérité révélée et elle n'engage que son auteur. Pour illustrer l'esprit

[1] Auteur de "Cybercrime, cyberterrorisme, Cyberwarfare : Adverting an Electronic Waterloo", 1998. Membre du groupe de travail "Global Organized Crime Project, Information Warfare/Information Assurance" du Center For Strategic and International Studies.

[2] "Grand Gourou" de la sécurité informatique, auteur de "Terminal Compromise" 1993.

[3] Dans "L'ennemi à l'ère numérique", Docteur d'Etat en sciences politiques, il enseigne la sociologie au CELSA (école des hautes études en sciences de l'information et de la communication),et à l'Ecole de guerre économique. Il anime l'Observatoire Européen d'Infostratégie.

d'humilité indispensable à l'étude d'un thème de prospective, j'emprunterai à Mark TWAIN la boutade suivante: *"Ne faites jamais de prédiction, si vous pouvez l'éviter, surtout pour l'avenir !»*

Après avoir rappelé les nombreuses vulnérabilités liées aux réseaux informatiques en présentant à la fois les "cybermenaces" et leurs modes d'action, tout en réservant un sort particulier à "l'infoguerre", je préciserai d'une part les limites de la notion de "cyberterrorisme", d'autre part l'exploitation du réseau mondial par le terrorisme non pas tant comme cible mais bien davantage comme outil en soulignant les intérêts financiers, politiques qui concourent à nous convaincre du contraire. En final, j'exposerai la posture des forces armées à l'égard de la "cybercriminalité" et de "l'infoguerre".

◆ ◆

I) Les cyber-menaces : la criminalité informatique, les vulnérabilités des systèmes, la guerre de, pour, contre l'information (descriptions, modes d'action, enjeux).

1-Les menaces.

1.1- La "cybercriminalité".

1.1.1- Définition.

La "cybercriminalité" est multiforme. Elle recoupe tous les domaines de la criminalité habituelle adaptés à l'Internet ainsi que des formes propres à ce type de média (piratage d'informations, intrusions de virus,…).

En d'autres termes la "cybercriminalité" serait la criminalité dont les auteurs, les moyens employés ou les victimes sont liés à la haute technologie. Deux catégories de "cybercriminalité" se distinguent : la 1ère serait constituée par la délinquance classique qui utilise les nouvelles technologies de l'information et de la communication (N.T.I.C.) ; la 2ème rassemblerait les délits spécifiques : piratage, "hacking", décodeurs de TV numérique…

1.1.2- Les cybercriminels selon les lois.

Seraient cybercriminels tous les individus qui mènent des activités considérées comme illégales par les lois dans les démocraties et par les autorités ailleurs.

En France, le code pénal et les lois françaises prévoient :

✶art. L 111-1 du code de la propriété intellectuelle (loi n°92-597 du 1er juillet 1992) :

- *toute utilisation faite sans le consentement de l'auteur est considérée comme illicite et sanctionnée pénalement*

- *la seule exception : le droit de courte citation qui permet de reproduire partiellement une œuvre à condition d'en indiquer clairement l'auteur et la source*

✶les art. L 112-1 et L 112-2 du même code précisent :

"…*sont protégées toutes les œuvres de l'esprit quels qu'en soient le genre, la forme d'expression, le mérite ou la destination…*"

En matière d'intrusion informatique, il convient de consulter le code pénal aux articles 323-1 à 323-7.

-Art 323-1 : "*le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 100 000 francs d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 francs d'amende".*

-Art 323-2 : "*le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 francs d'amende".*

-Art 323-3 : "*le fait d'introduire frauduleusement des données dans un système de traitement automatisé, ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 300 000 francs d'amende".*

1.1.3- Essais de classifications.

1.1.3-1 Selon le mobile : "Dis moi ce que tu veux et je te dirai ce que tu fais !" :

- **les crimes ayant l'argent pour mobile et pour cible.**

Le détournement de fonds : nul besoin désormais d'agresser une personne à la sortie d'une banque ou d'un distributeur de billets, des pirates habiles peuvent récupérer les numéros de compte ou des codes secrets soit par les transactions sécurisées sur Internet, soit grâce à des logiciels qui génèrent les numéros. Par ailleurs, tous les sites commerciaux ne sont pas sécurisés et leurs banques de stockage de numéros de cartes de crédit peuvent s'avérer extrêmement vulnérables. Ainsi l'un des plus célèbres escrocs informatiques, Kevin MITNICK avait volé plus de 17 000 numéros de cartes bancaires aux Etats-Unis. Kenneth H.TAVES, un autre escroc américain, fut arrêté par le F.B.I. en 1999 pour la plus grande fraude de cartes de crédit connue jusqu'à ce jour sur Internet, soit un préjudice supérieur à 45 millions de dollars. Muni de ces numéros, il lui suffisait ensuite de les exploiter pour obtenir un service auprès des commerces en ligne. Le "cybercash", c'est à dire l'argent électronique qui circule sur Internet entre des clients et leurs banques, présente également des vulnérabilités. Cet argent est stocké sur un disque dur, véritable porte-monnaie électronique, qui est sensible aux attaques. De plus, l'anonymat lié à ces transactions favorise non seulement les risques de blanchiment d'argent et de contrôle mafieux, mais aussi ceux liés à l'évasion fiscale. Enfin, le "cyberhold-up" consiste après pénétration dans les fichiers d'une banque à transférer des fonds d'un compte tiers sur son propre compte.

Il convient d'ajouter à ces risques délictuels le chantage, qui amène à monnayer des données sensibles dérobées, soit dans des entreprises, soit dans des établissements bancaires en menaçant de les divulguer ou de les utiliser pour nuire.

En outre, l'industrie frauduleuse de la copie se développe. Elle ne concerne pas seulement les fichiers d'enregistrement sonores copiés sur des sites gratuits dans un format MP3 (type Napster). Il s'agit aussi des logiciels informatiques, des D.V.D., des œuvres littéraires voire des bandes dessinées. Enfin, certains produits sont commercialisés sur le Net soit parce qu'ils sont indisponibles et interdits en vente libre, soit parce qu'ils sont vendus nettement moins chers que dans le réseau officiel. C'est particulièrement le cas de certains produits pharmaceutiques contrefaits comme le "Viagra" ou de certains produits dopants comme la créatine.

- **les crimes ayant le pouvoir pour mobile et pour cible.**

La cyberpropagande ou l'utilisation du cyberespace à des fins de propagande par des mouvements terroristes, sectaires, extrémistes religieux ou politiques est une évidence. L'utilisation du NET par les zapatistes reste aujourd'hui encore exemplaire en la matière. Ces opposants mexicains ont rendu célèbre leur cause en touchant l'opinion internationale en 1994 par des rumeurs terrifiantes sur la situation au Chiapas.

La classification peut s'opérer différemment.

1.1.3-2 La classification du Professeur CARTER[4].

-1ère catégorie : l'ordinateur est la cible, par exemple, la prédation de données accompagnées ou non de chantage ; le sabotage et le vandalisme de données avec ou sans mobile vénal ; l'intrusion sans destruction…

-2ème catégorie l'ordinateur est l'outil d'un crime conventionnel. Il facilite la commission de l'infraction en tant que moyen et non en tant que cible : par exemples, les détournements de fonds, la pornographie enfantine et la pédophilie…

-Enfin 3ème catégorie, l'ordinateur génère de nouveaux types de crimes, en réalité des crimes "classiques" mais adaptés à l'informatique : par exemple, les copies de logiciels, de musique et les contrefaçons de matériel…

En fait, quelle que soit la classification retenue, l'intérêt du Net pour les criminels repose sur la rapidité avec laquelle ils peuvent installer leurs structures sur le réseau, le nombre considérable de victimes potentielles, l'étendue géographique de leurs méfaits, les possibilités accrues d'effacer rapidement toutes traces, la multiplication des sites utilisés et les difficultés pour les enquêteurs de rassembler des moyens de preuves suffisants dans des délais contraints.

[4] Professeur au département de justice pénale de l'université de l'Etat du Michigan et auteur de "Computer Crime Categories : How Techno-Criminals Operate ?" F.B.I. Law Enforcement Bulletin, 1992.

Mais à la marge de cette première forme de criminalité informatique, selon des frontières pas toujours très nettes et précises, coexiste une autre type de cybercriminels aux aspirations et aux motivations plus complexes : les "hackers" et les "hacktivistes".

1.2- Les "Hackers".

Le " hacker ", terme générique, recouvre des réalités contrastées.

1.2.1- Le "hacking".

Au départ un "hacker" est une personne qui a du plaisir à explorer en détail un système programmable et qui cherche à étendre au maximum ses connaissances dans ce domaine. Aujourd'hui, le terme est généralement employé pour désigner des personnes s'introduisant illégalement dans des systèmes informatiques. En outre, les "crackers" sont des spécialistes de la "casse" des protections de programme et le "phreaking" constitue une variante du "hacking".

1.2.2- Le "phreaking" consiste à pirater les réseaux téléphoniques.

La plupart des "hackers" pratiquent aussi cette activité d'autant que les techniques mises en œuvre pour pirater un central téléphonique informatique sont identiques à celles employées contre un ordinateur classique. Les "phreakers" les plus habiles peuvent utiliser les réseaux téléphoniques à la manière d'un agent technique d'une compagnie de téléphone.

1.2.3- Un cas d'école permet d'illustrer les incroyables vulnérabilités des systèmes face à "ces petits génies de l'informatique".

Un "hacker", Mickael SINERGY, dans les années 80 pénétra le système informatique de l'agence de crédit nationale (TRW) qui détient les informations financières de près de 80 millions d'américains, à la recherche du fichier de Ronald REAGAN. Non seulement il le découvrit, mais il s'aperçut que 63 autres personnes l'avaient également consulté le même jour. De plus, il vit que près de 700 personnes semblaient posséder la même carte de crédit avec un historique de compte très étrange. Il en conclut qu'il était parvenu à pénétrer le programme gouvernemental de protection des témoins. En bon citoyen, il signala au F.B.I. ces dysfonctionnements. Mais tous les "hackers" n'ont pas les mêmes scrupules.

1.2.4- La motivation des "hackers" se fonde le plus souvent sur le défi intellectuel.

Les vrais "hackers" auraient même un code éthique leur interdisant la destruction de données. Néanmoins, tous ne respectent pas ces règles. Certains ont compris rapidement l'intérêt mercantile qu'ils pouvaient retirer de leurs prouesses techniques. Le docteur Frederick B. COHEN[5] propose une liste de motivations incitant les personnes à rentrer dans le monde de la criminalité informatique : l'appât du gain, le défi pour une

[5] Auteur de « Protection and Security on the Information Superhighway », John Wiley & Sons, Inc.,1995.

reconnaissance sociale non seulement au sein d'un groupe de "hackers", mais aussi parfois auprès d'entreprises recherchant des as pour leur sécurité informatique, la vengeance d'un employé licencié ou en conflit avec sa firme, la prévoyance et la garantie d'un programmeur à l'égard d'une éventuelle indélicatesse de son employeur, l'avantage économique dans le cadre d'une concurrence impitoyable amplifiée par la mondialisation.

1.3- Les "hacktivistes": mélange de "hacking" et d'activisme.

"L'hacktivisme" adopte les techniques du "hacking" dans un but délibéré : nuire pour défendre une cause. Dans la majorité des cas les cibles sont constituées par des sites WEB. L'intention y est soit d'interrompre le fonctionnement normal, en engendrant un déni de service par des blocages d'ordinateurs, par des virus et autres vers, soit de dénaturer un site, "defacing", mais le plus souvent sans créer de véritables dommages aux matériels "hardware". Ces attaques ont néanmoins un coût financier important pour les victimes.

Il conviendrait, toutefois, de distinguer l'activisme du "cyberterrorisme" et de "l'hacktivisme" sur Internet.

1.3.1- L'activisme, prolongement de la démocratie sur le réseau.

Il consiste à utiliser le réseau pour échanger des informations et défendre des thèses, ou pour coordonner des actions militantes (mouvements d'opinion, préparation de manifestation…). Ainsi, Internet sert à faire par d'autres moyens ce que les militants politiques faisaient par des tracts, des communiqués, des meetings, des radios clandestines, etc…Ici les facilités de communication, offertes par la toile, multiplient les modes d'action traditionnels.

1.3.2- Le "cyberterrorisme" viserait à provoquer de véritables dommages économiques, stratégiques voire humains en usant de moyens informatiques. Cette notion fera ultérieurement l'objet de plus amples développements.

1.3.3- Entre les deux, le domaine encore mal défini de "l'hacktivisme".

Ici, le piratage informatique se met au service de causes morales ou politiques et mène des actions agressives contre des sites d'organismes politiques, notamment en bloquant ou altérant les sites et les services WEB. Le piratage de sites par des "hacktivistes" représente un degré de plus dans l'escalade. Le résultat se limite fréquemment à un déni de service de quelques heures ou un "tag" soit revendicatif, soit humoristique. Tout nouveau conflit et toute tension internationale sont accompagnés d'une floraison d'attaques par "defacing" : par exemple entre chinois et américains au printemps 2001, lors de la mort d'un pilote chinois abattu par l'aviation américaine.

Mais sommes nous dans le domaine du "cyberterrorisme" ou dans celui de la guerre de l'information ? La réponse américaine est globalisante : les Etats-Unis font facilement l'amalgame.

Pour certains spécialistes, il serait, en effet, dangereux de totalement sous-estimer cet aspect. Car ayant un message politique, ces groupes "hacktivistes" pourraient s'attaquer à des Etats, ou à des sociétés effectuant des affaires avec ces Etats. Cette hypothèse fut très sérieusement examinée en 1998 par les autorités américaines lors d'une simulation appelée "Cyber Receiver". Les résultats de cette simulation incitèrent le Président Clinton à solliciter 2,8 milliards de dollars auprès du Congrès pour combattre cette nouvelle menace hâtivement qualifiée de "cyberterrorisme".

Le NET peut toutefois générer des incitations à la commission de crimes. Pour s'en convaincre, rappelons-nous l'épisode tragique de la "liste noire" des médecins avorteurs aux Etats-Unis. Le Dr Barnett SLEPIAN, assassiné en 1998, constituait la 8ème victime sur une liste diffusée "en ligne" par un groupuscule nommé "the Abortion Rights Activist". Sur cette liste, tenue à jour, les noms des médecins blessés figuraient en gris, les médecins morts étaient barrés et ceux encore vivants étaient signalés par la mention "travail". Les défenseurs des animaux adoptent des pratiques comparables en incitant les internautes à attaquer les sites des entreprises pharmaceutiques afin de s'opposer aux expérimentations animales et à la vivisection.

En somme, les limites entre l'activisme, "l'hacktivisme", la propagande ou l'incitation au crime y compris terroriste sur le Net peuvent s'avérer extrêmement ténues dans la pratique. En revanche, tous ces phénomènes relèvent indiscutablement des délinquance et criminalité informatiques.

2-Les modes d'actions de la criminalité informatique.

(Mélissa, Kournikova, I love you, Tchernobyl…)

2.1- Virus.

2.2.1- Définition.

Un virus est un programme capable d'une part de se reproduire dans un ordinateur, d'autre part d'infecter d'autres programmes et ainsi de se transmettre d'un ordinateur à l'autre, à condition toutefois de copier initialement le programme infecté sur un ordinateur sain. De plus, il peut être programmé pour détruire les données contenues dans l'ordinateur soit à un moment précis, soit dès l'ouverture d'une session.

2.2.2- Typologie des virus.

Le "rétro-virus" constitue une variante qui s'attaque également aux logiciels anti-virus installés sur une machine.

Le ver diffère du virus, car il se transmet par lui-même d'un ordinateur à l'autre au travers d'un réseau, généralement par la messagerie électronique. Le ver le plus connu est celui qui paralysa le réseau ARPANET[6] en 1988. Plus récemment, "I love you" fonctionnait également selon le même principe et sema l'émoi dans la communauté Internet.

Notons en outre l'existence de virus "caméléon" qui change d'aspect c'est à dire de signature informatique dans sa ligne de programme afin d'échapper aux mécanismes de détections des logiciels d'anti-virus.

En marge de ces virus bien réels, il existe le "virus imposteur" ou "hoax" qui propage des fausses rumeurs. Elles mettent faussement en garde contre de terribles virus aux effets apocalyptiques. Ces canulars encombrent, saturent parfois les boîtes aux lettres et ralentissent les réseaux tout en générant la paranoïa.

En résumé, à quelques exceptions près, il faut que l'utilisateur démarre lui-même le programme ou le document infecté pour que le virus soit activé. Une intervention humaine est donc nécessaire, à ce stade mieux vaut donc faire preuve de prudence avant le "clic fatal" ! Néanmoins, selon une étude réalisée par "Symantec Anti-Virus Research Center[7]", en 1993 seulement 10% des virus étaient considérés comme destructeurs, en 1997 cette proportion était déjà passée à 35%. En mai 2000, cette société recensait environ 47 000 virus différents.

2.2- La "bombe logique".

La "bombe logique" est un programme contenant une fonction malveillante généralement associée à un déclenchement différé et qui modifie un des programmes du système sur lequel elle est implantée.

Exemple : un jeune appelé, pour se venger d'une sanction prise à son encontre dans une unité des forces armées, avait programmé une "bombe logique". Elle s'est déclenchée six mois après sa libération en provoquant l'impression simultanée sur toutes les imprimantes du réseau local et de manière répétitive toutes les dix minutes d'un message insultant à l'encontre de ses anciens chefs.

2.3- Le "cheval de Troie".

Sous l'aspect d'un logiciel parfaitement anodin, téléchargé gracieusement, se dissimule parfois un programme perfide qui à l'insu de l'opérateur soit exécute des opérations destructrices de données, soit cède le contrôle à distance de l'ordinateur à un pirate par une "backdoor"[8]. Ainsi le pirate peut d'une part visualiser ce qui se trouve sur votre écran, d'autre part utiliser vos logiciels, enfin capter vos mots de passe par le biais d'Internet.

[6] Ancêtre du réseau Internet crée par les militaires américains en 1969.
[7] Les éditeurs de Norton, le plus important concepteur de logiciels de sécurité informatique.
[8] Passage secret dans un système informatique qui permet d'y pénétrer à l'insu de l'utilisateur.

2.4- La prédation de données.

S'agissant du vol de données, ce n'est pas un hasard si le premier incident documenté concernait Arpanet en 1986 lors d'une tentative pour accéder à des informations militaires américaines. Néanmoins, les attaques et les tentatives de pénétrations sont quotidiennes. Elles ne proviennent pas uniquement de professionnels.

En effet, il est aujourd'hui très simple de se procurer des "toolkits" qui regroupent un échantillonnage de programmes de pénétration. Certains sont gratuitement disponibles sur le Net, soit sur les sites dédiés aux pirates, soit dans les "chats" traitant du sujet.

Il existe ainsi des logiciels très répandus et populaires capables d'une part de neutraliser des programmes d'encodage, d'autre part de créer des virus et des numéros de cartes de crédits. Ainsi le logiciel "Superhacker 99" se vendait moins de 4 € dans les rues des grandes métropoles européennes.

3- "information warfare" et guerre économique, enjeux pour "l'info-dominance".

Une grande confusion règne sur la signification précise du concept "maîtrise de l'information". Qu'est-ce qu'une information ? Qu'est-ce que maîtriser : est-ce contrôler et connaître ou bien est-ce dominer et imposer sa loi ?

La guerre de l'information est un sujet de prédilection pour de nombreuses armées surtout aux Etats-Unis. Elle regroupe plusieurs concepts dont la guerre électronique, la guerre psychologique, le renseignement et la guerre des "hackers". Il n'est pas surprenant que la guerre de l'information soit un concept initié par les Etats-Unis qui trouvent dans ces nouveaux affrontements du XXIème siècle à la fois le fondement et l'objectif de la révolution des affaires militaires et son corollaire : l'option "zéro mort".[9]

En effet, *"la guerre de l'information est plutôt la guerre des zéros : zéro mort, zéro incertitude, zéro adrénaline, zéro distance, zéro contact, zéro frontière et demain zéro coût, zéro arme, zéro soldat et avec résultat zéro paix"*[10].

Mais il serait réducteur et donc erroné de croire que le monde de la défense militaire serait seul concerné par cette lutte. Car, la compétition économique justifie le recours à des pratiques impitoyables et comparables pour maîtriser l'information économique, industrielle et commerciale.

Aujourd'hui, en somme, *"Le champ de bataille est d'abord un champ de perception"*.[11]

---

[9] Doctrine qui envisage l'engagement des troupes américaines uniquement lorsque les risques de pertes humaines sont proches du seuil nul. Les attentats du 11/09/2001 semblent remettre en cause ce principe.
[10] Tiré "L'ennemi à l'ère numérique" de F.B. HUYGHE.
[11] VIRILIO dans "Cybermonde, la politique du pire".

3.1- Définition et concept.

3.1.1- La définition du Dr John ALGER.[12]

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

En d'autres termes, la guerre de l'information recouvre l'ensemble des champs conflictuels où l'information est utilisée comme une arme offensive pour affaiblir, déstabiliser ou détruire un adversaire. Les techniques offensives de la guerre de l'information peuvent prendre la forme de la désinformation, de la manipulation, de la rumeur, de la propagande. Il s'agit donc de méthodes subversives pouvant être efficacement déployées sur l'ensemble des canaux de communication à disposition (internes, externes, Internet, intranet, prolifération orale etc..).

3.1.2- Le concept de guerre de l'information (G.I.).

La G.I. est un concept militaire très vaste qui englobe indistinctement toutes les actions humaines, techniques et technologiques (opérations d'information) permettant de détruire, de modifier, de corrompre, de dénaturer ou de pirater l'information, les flux d'informations ou des données d'un tiers (états ; entités administratives, économiques ou militaires voire terroristes) en vue de brouiller, d'altérer sa capacité de perception, de réception, de traitement, d'analyse et de stockage de la connaissance.

Les opérations informationnelles (O.I.) ciblent autant les moyens technologiques de commandement et de communications que les individus. La G.I. contre des individus ou des groupes d'individus correspond en fait à ce que l'on désignait autrefois sous les termes de "guerre subversive" ou de "guerre psychologique". Elle comprend des actions de propagande, de manipulation, de désinformation et de déception. Bien qu'ancien, le concept retrouve une seconde jeunesse grâce au développement des Nouvelles Technologies d'Information et de Communication (N.T.I.C.).

3.1.3- Les enjeux.

Ils résident à la fois dans l'information, le savoir et la connaissance afin d'obtenir le pouvoir. La manipulation de l'information à des fins malveillantes contre des acteurs économiques, contre un Etat, contre des entreprises ou contre des individus est aujourd'hui facilitée et amplifiée notamment par l'émergence des N.T.I.C.

De surcroît, la maîtrise, le contrôle et la diffusion de la connaissance ainsi que la protection des capacités de maîtrise, de contrôle et de diffusion de l'information sont utilisés

[12] Cité par HAENI Reto dans "An Introduction to Information Warfare".

non seulement comme un vecteur de connaissance et d'anticipation, mais également comme une arme offensive.

Ainsi l'information, les systèmes d'information et les capacités informationnelles deviennent l'enjeu "politico-militaro-économique" du XXIème siècle.

La parfaite reconversion du "système Echelon", conçu d'une part initialement dans le cadre de la guerre froide pour espionner le bloc communiste et devenu d'autre part depuis la disparition de la menace soviétique un puissant "Big Brother" économique, illustre remarquablement la proximité entre "l'infoguerre" et la guerre économique. Ce dispositif d'écoutes électroniques s'intéresserait, entre autres aux entreprises européennes. Il contribuerait à lutter contre des pratiques commerciales illicites (corruption, pots de vin, etc) en fournissant aux firmes américaines les renseignements utiles à leur protection contre ces crimes et ces délits. En fait, il pratique allègrement l'espionnage économique et sert les intérêts économiques américains… Thompson-CSF, Airbus et Siemens en ont été victimes en leur temps.[13]

En résumé, aujourd'hui, la principale matière première de l'économie, de la politique et du militaire est bien l'information. Elle peut alors être traitée, analysée, diffusée et exploitée aux dépens des uns ou des autres, en vue d'obtenir une longueur d'avance majeure. Cette situation marque l'avènement de la course à "l'information domination" (info dominance). *"Le conflit ne se déroulerait plus sur le territoire mais sur la carte et surtout pour la carte…".*[14]

3.2- Classifications selon W. SCHWARTAU.

Winn SCHWARTAU, dans "Information Warfare", propose la classification suivante :

3.2.1- "classe 1" : Guerre de l'information contre les personnes.

Dans cette catégorie figurent les atteintes à la sphère privée de l'individu. La divulgation ou la prédation de données individuelles et nominatives issues des différents fichiers dans lesquels nous apparaissons forcément au titre de nos cartes de crédit, de nos fiches de salaires, de notre casier judiciaire, de notre sécurité sociale, de nos factures de téléphones reste préoccupante. Ces informations n'apparaissent pas toujours exactes et elles ne sont pas aisément accessibles afin d'exercer un éventuel droit de correction. Chacun d'entre nous possède une "image numérique" qui lui confère une identité numérique.

[13] Deux rapports commandés par le Parlement Européen en 1998 et 1999 au journaliste britannique Duncan CAMPBELL confirme le rôle occulte "d'Echelon" dans la compétition économique au profit des Etats-Unis.
[14] Tiré de "L'ennemi à l'ère numérique" écrit par F.B. HUYGUE.

3.2.2- "classe 2" : Guerre de l'information contre les entreprises.

Cette classe correspond à la farouche concurrence des entreprises. L'espionnage industriel est une des activités envisageables. Mais, la désinformation demeure un procédé moins coûteux et très efficace pour se débarrasser d'un concurrent à peu de frais.[15] Avec Internet, il est facile de lancer des rumeurs de portée mondiale pour lesquelles tout démenti apparaîtra comme vain.

3.2.3- "classe 3" : guerre globale de l'information.

Ce type de conflit vise l'architecture d'un pays, ses fondements industriels économiques et sociaux. Avec des investissements ridicules aux regards de ceux consentis pour des armes de destructions massives, il serait théoriquement possible pour un groupuscule ou un Etat de mettre à genoux une grande puissance économique en s'attaquant à ses réseaux informatiques contrôlant les flux énergétiques, boursiers, financiers et monétaires par exemple. Par ailleurs, si l'attaquant n'a pas atteint un seuil de développement tel qu'il serait, lui-même, très dépendant des flux de l'information les mesures de rétorsion de même nature à son encontre demeurent limitées et donc peu dissuasives. De plus, la réponse militaire à ce type d'attaque dans une démocratie occidentale serait peut-être mal admise par l'opinion publique et la communauté internationale ; en conséquence l'agresseur pourrait espérer une certaine impunité.

3.3- La simulation conduite par la "Rand Corporation".

Aux Etats-Unis, à la demande du Département de la Défense, la "cybermenace" a été étudiée au travers d'un scénario comportant six exercices menés entre janvier et juin 1995. Les conclusions ont été les suivantes : "*n'importe qui peut attaquer, il est impossible de savoir ce qui est réel, il est même difficile d'avoir conscience de l'attaque*". Extrapolations excessives, paranoïa ! ? Peut-être ! Peut-être pas !

En somme, pour de nombreux observateurs, le plus souvent américains, les hostilités ont déjà commencé. Selon les TOFFLER,[16] nous sommes déjà rentrés dans les conflits de la "troisième vague". D'après Winn SCHWARTAU, le risque de "Pearl Harbor électronique» est bien réel.

La description de quelques procédés techniques utilisés dans le cadre de la guerre de l'information conforte cette thèse de grande vulnérabilité et de danger imminent.

[15] Voir Jean GUISNEL dans "Guerres dans le cyberespace" au sujet de la lutte entre Boeing et Airbus.
[16] Célèbres futurologues américains, auteurs de "War and Antiwar" Fayard, Paris , 1993.

3.4- Techniques de cyberguerre.

3.4.1- Le "chipping".

Il consiste dans l'implantation matérielle d'un "cheval de Troie". Il s'agit de rajouter une fonction à l'insu de l'acheteur dans un composant électronique d'une arme (ou d'un autre matériel), de sorte que si un jour cette arme doit être utilisée contre le vendeur, elle puisse être neutralisée à distance.

3.4.2- Bombes E.M.P.-T.

D'après Winn SCHWARTAU, des bombes "Electro-Magnetic Pulse Transformer" peuvent être construites pour quelques poignées de dollars. Elles sont capables d'effacer les informations stockées sur un support magnétique à 200 mètres à la ronde. A noter que des "dégausseurs" de faible encombrement permettent aussi d'effacer irrémédiablement des disques durs en les démagnétisant par simples contacts de proximité. Les américains maîtrisent ces technologies notamment les "Directed Energy Weapons", (D.E.W.).[17]

3.4.3- Radiations Van Eck.

Un ordinateur peut être vulnérable même sans être relié à un réseau informatique local ou à un réseau à distance par téléphone. Un ordinateur coupé du monde peut donc être espionné à partir des radiations émises par ses composants. Avec un matériel adéquat, il est possible de reconstituer le contenu de l'écran à distance. Ce procédé a été utilisé par le F.B.I. pour confondre Aldrich AMES, agent du K.G.B. infiltré au sein de la C.I.A. La technologie utilisée porte le nom de "TEMPEST monitoring". L'utilisation de "TEMPEST monitoring" est possible sans autorisation, alors qu'il est illégal pour un particulier ou une société privée de s'en protéger. Cette technologie est à la portée de n'importe quel bureau d'ingénieur et par conséquent des criminels peuvent se la procurer sans grande difficulté.

Bien que les moyens techniques employés peuvent s'apparenter à des armes, la guerre de l'information se distingue de la guerre classique car les opérations de "l'infoguerre" sont bien souvent des opérations inavouées, non revendiquées, illégales, clandestines et parfois non décelées. Elles ressemblent davantage au raid qu'à une guerre continue. Certaines de ces batailles ne permettent d'identifier ni les auteurs, ni leurs motivations, ni même parfois les atteintes qui peuvent être différées. En cas d'attaque, il est difficile de savoir s'il s'agit d'une opération militaire, d'un canular, d'un jeu, d'une malveillance de la concurrence, ou d'un acte de vandalisme idéologique.

[17] Voir article écrit par le C.E. MANIN dans le n°25, décembre 2001 de la "Tribune du C.I.D." sur les "Directed Energy Weapons ".

Il convient de noter que les grandes démocraties ont également recours à ces procédés offensifs. Ainsi une opération avortée a été révélée par "Newsweek" en mai 1999 : elle consistait à "cyberpirater" les comptes à l'étranger de S. MILOSEVIC. Par ailleurs, "U.S.A. Today" évoquait une action identique contre les fonds de BEN LADEN.

◆

En résumé, l'informatique et les réseaux informatiques, par "l'intelligence" que l'on y a placée, ne sont pas tant des biens à protéger que des services et des capacités de service dont il faut maintenir la propriété, l'intégrité et l'état de fonctionnement.

La diversité des supports physiques, le caractère immatériel des informations et la vitesse d'évolution des technologies et des matériels rendent pratiquement imprévisibles les attaques informatiques. L'identification de l'attaquant est rendue difficile par la prolifération, la densité des réseaux informatiques et leur organisation actuelle. La diffusion des agressions peut être quasiment instantanée à cause de la vitesse de fonctionnement des systèmes informatiques à base d'électronique et la vulnérabilité d'un réseau est directement liée à la vitesse de réaction de ses administrateurs. De plus, l'interopérabilité des réseaux est une exigence forte en matière de sécurité des systèmes, car le point le plus faible de l'ensemble est constitué par le réseau le moins bien protégé ou le plus vulnérable.

Les menaces génériques demeurent donc : l'agression physique, la capture d'information, l'usurpation de droits ou d'identité sur les réseaux, la capture de rayonnements compromettants, la substitution, le vol, l'interception ou la copie de supports ; la destruction, le piégeage ou l'altération de logiciels et de données ; la prise de contrôle d'équipements actifs ; l'attaque de saturation. Toutefois, pour le moment, la paralysie d'un pays entier soumis à une attaque de "hackers" reste un fantasme.

Après avoir énuméré les principales vulnérabilités logicielles et matérielles des systèmes informatiques, puis démontré que semer le chaos à distance s'avérait en théorie possible, il convient maintenant de répondre à la question : pourquoi n'y a-t-il pas eu un seul attentat terroriste informatique médiatisé ?[18]

◆ ◆

[18] Sauf à considérer, l'attentat contre le World Trade Center en 1993 comme le premier du genre. Il engendra environ 700 millions de dollars de pertes financières. Thèse avancée par D. MARTIN, ex-Commissaire de la D.S.T. (Direction de la Surveillance du Territoire).

II) Réflexions sur terrorisme et terrorisme informatique ?

Les terroristes ont-ils un intérêt égal à frapper les réseaux informatiques d'une part, à heurter les opinions publiques par des violences caractérisées génératrices de peur d'autre part ? Les éléments de réponse sont consubstantiels à la nature, aux méthodes et aux objectifs du terrorisme.

Que signifie le terme "cyberterrorisme" ? En réalité, il recouvre essentiellement dans les faits l'utilisation du Net à des fins de propagande, de préparation, de coordination d'actions ou d'échange d'informations entre divers groupes ou entre cellules d'un même groupe éclatées à travers le monde. Mais le véritable "cyberterrorisme" ne serait-il pas à la fois plus ciblé, plus visible et plus violent ? Il consisterait à semer la "terreur" par des moyens informatiques, comme les terroristes la répandent déjà par des attentats sanglants et spectaculaires.

Il semblerait toutefois que cette situation ne se soit pas réellement posée jusqu'à présent. Pourtant, les Etats-Unis et de très nombreux observateurs ont promu ce risque au rang de menace stratégique. Tâchons de comprendre pourquoi ?

2.1- Tentative de définition du terrorisme.

Le terrorisme est une méthode de combat fondée sur le recours à la violence et destinée à semer la terreur, il s'inscrit dans une stratégie dite du "faible au fort". Depuis 1945, il a été impossible d'en donner une définition universelle et cohérente. Il en existerait près de 212 dont 72 différentes dans les seuls états anglo-saxons. Les plus communément admises sont les suivantes :

2.1.1- Définition F.B.I.

"Le terrorisme est l'utilisation illégale de la force ou de la violence contre des individus ou des biens pour intimider ou forcer la main à un gouvernement, aux membres du public, ou toute partie de ces deux éléments, et ainsi poursuivre des objectifs politiques ou sociaux".

2.1.2- Définition Département d'Etat américain.

"L'usage calculé de la violence ou de la menace pour créer la peur ; destiné à contraindre ou à intimider des gouvernements ou des sociétés afin d'atteindre des objectifs généralement politiques, religieux ou idéologiques".

2.1.3- Définition de l'Union Européenne :

Déclaration cadre de l'U.E. à l'issue du "sommet de Laeken" :

"Art 3 - infractions terroristes :

*-1- ,chaque état membre prend les mesures nécessaires pour faire en sorte que les infractions suivantes, définies par son droit national**, commises intentionnellement** par un individu ou un groupe contre un ou plusieurs pays, leurs institutions ou leur population, et **visant à les menacer et à porter gravement atteinte ou à détruire les structures politiques, économiques ou sociales d'un pays,** soient sanctionnées comme des infractions terroristes :*

- (a) le meurtre,

- (b) les dommages corporels,

- (c) l'enlèvement ou la prise d'otages,

- (d) le chantage,

- (e) le vol simple ou qualifié,

- (f) la capture illicite d'installations étatiques ou gouvernementales, de moyens de transports publics, d'infrastructures, de lieux publics et de biens (publics ou privés) ou les dommages qui leur sont causés,

- (g) la fabrication, la possession, l'acquisition, le transport ou la fourniture d'armes ou d'explosifs,

- (h) la libération de substances contaminantes, ou la provocation d'incendies, d'inondations ou d'explosions, la mise en danger de personnes, de biens, d'animaux ou de l'environnement,

- (i) la perturbation ou l'interruption de l'approvisionnement en eau, en électricité ou toutes autres ressources fondamentales,

- (j) la commission d'attentats en perturbant un système d'informations,

*- (k**) la menace de commettre** l'une des infractions énumérées ci-dessus,*

- (l) la direction d'un groupe terroriste,

- (m) l'encouragement ou le soutien d'un groupe terroriste ou la participation à un groupe terroriste.

*-2- aux fins de la présente décision cadre on entend par **"groupe terroriste"** une association structurée, de plus de deux personnes, établie dans le temps, et agissant de façon concertée en vue de commettre des infractions terroristes visées au paragraphe 1".*

Le caractère novateur de cette "décision cadre" tient d'une part à l'avènement d'une définition commune à l'U.E. sur le terrorisme et d'autre part à la prise en compte pour la première fois des motivations des auteurs d'infractions informatiques. Ces motivations sont soulignées par les termes "intentionnellement" et "visant à…". Par ailleurs, la réalisation d'attentats commis en perturbant les systèmes informatiques est expressément visée. Ces précisions doivent permettre la distinction entre le "hacker du dimanche" et le "cyberterroriste". De plus, la notion de groupe terroriste est également précisée dans l'alinéa

2. Elle recèle l'idée de structure établie dans le temps et possédant un dessein : commettre des infractions relevant du terrorisme.

Malgré la diversité de ces définitions, certains traits dominants méritent d'être isolés et soulignés.

2.1.4- Des critères communs.

Des constantes se révèlent donc au terme de ces définitions et de la pratique contemporaine du terrorisme :

- le déchaînement d'une **"violence en apparence aveugle"** ;
- provoquant toujours **"la terreur" ou la psychose** ;
- sur **des acteurs variés** (Etats, décideurs, groupes, individus…) ;
- **dans un but précis** (politique, social, religieux,…) ;
- s'appuyant sur **l'effet de levier et d'amplification des médias** afin de frapper et manipuler les opinions publiques.

En résumé, il s'agit de générer et d'entretenir la peur.

Or, le monde numérique n'est pas propice au déchaînement de la violence physique, ni au développement de la terreur. Toutefois, la rumeur peut brouiller les perceptions et entretenir un climat de psychose. Le célèbre précédent constitué par l'émission radiophonique d'Orson WELLES, illustre l'influence des médias sur les réactions de l'opinion publique. Même si en l'espèce, il s'agissait d'un média moins performant et d'une autre époque !

Le terrorisme numérique ne semble pas une menace actuelle, il demeure cependant un risque pour le futur. En effet, le jour viendra peut-être où le niveau d'équipement informatique à la fois des états et des particuliers notamment par la généralisation de la domotique pour ces derniers, sera tellement développé, que chacun d'entre nous sera une victime potentielle d'acte de violence visant à provoquer à distance l'explosion, l'incendie de son habitation ou de son ordinateur. La concrétisation de cette menace, pour l'instant virtuelle, constituerait une action "cyberterroriste" proprement dite, car elle sèmerait effectivement la peur.

Pour l'heure, les créateurs de la menace évoquent la possibilité de bloquer les infrastructures vitales par des attaques informatiques. L'occurrence de ce risque semble bien plus faible et théorique que celle des pannes bien réelles des systèmes. Dans un cas comme dans l'autre, on imagine que toutes les mesures de prévention et de précaution sont prises pour sinon en éviter la survenue, du moins pour en limiter les effets les plus nuisibles. Les partisans du "doomsday" évoquent souvent les attaques visant à provoquer la rupture des flux

énergétiques, financiers (neutralisation des places boursières) ou visant à semer le chaos dans le trafic aérien. Mais le chaos informatique ne se produit-il déjà pas occasionnellement, accidentellement et fortuitement sans entraîner des catastrophes hormis des pertes financières importantes ?

Pour s'en convaincre, il convient de mesurer les conséquences liées d'une part aux phénomènes météorologiques tels que les cyclones, les ouragans et autres tempêtes tropicales, d'autre part aux conflits sociaux et aux grèves dans certains secteurs d'activités sensibles dont la paralysie gêne parfois l'économie complète d'un pays pendant plusieurs jours.

En outre, un ancien chef des services techniques de la navigation aérienne à la Direction Générale de l'Aviation Civile (D.G.A.C.) confiait[19] : "*le radar, le contrôleur sait gérer l'avion, la sécurité est assurée. Il existe une vingtaine de radars actifs sur le territoire, tous branchés sur le système RENARD, un Transpac privé parfaitement étanche. Ce système est triplé et doté d'un moyen de secours*.". Les ordinateurs utilisés dans le contrôle du trafic aérien ne contrôlent rien. Ils procurent simplement une aide au contrôleur humain. De fait, la mise hors service accidentelle des communications d'un aéroport civil n'engendre pas de catastrophes. Pour Mark M. POLITT[20] "*l'ordinateur ne contrôle pas suffisamment le système pour poser un risque de terrorisme (dans le sens classique) significatif*".

2.2- Mais quid du "terrorisme informatique"?

2.2.1- Tentatives de définition.

Rares sont ceux qui se hasardent à tenter de définir le "cyberterrorisme". L'étude du "cyberterrorisme" pose pourtant le problème de sa définition.

Le terrorisme informatique serait-il le fait de détruire ou de corrompre des systèmes informatiques, dans le but de déstabiliser un pays ou de faire pression sur un gouvernement, ou bien serait-ce le fait de mener une action destinée à déstabiliser un pays ou à faire pression sur un gouvernement, en utilisant des méthodes classées dans la catégorie des crimes informatiques ?

Selon Mark M. POLITT: *"le cyberterrorisme est une attaque préméditée, politiquement motivée, contre l'information, les programmes informatiques et les données contre des cibles non combattantes (ou combattantes) par des groupes subnationaux ou des agents clandestins"*. Cette définition présente au moins l'avantage de distinguer le "cyberterrorisme" de la "cybercriminalité" par la discrimination intentionnelle : "politiquement motivée".

[19] Tiré de "L'ennemi à l'ère numérique" de F.B. HUYGUE.
[20] Expert du F.B.I. Laboratory et auteur de "Cyberterrorism fact or fancy".

2.2.2- Il existe trois types d'actions contre un système informatique : une attaque physique, syntaxique ou sémantique.

L'attaque physique consiste à endommager les équipements de manière "classique" par bombes, incendie, etc…

L'attaque syntaxique consiste à modifier la logique du système, afin d'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.

Les systèmes informatiques réputés sensibles appartiennent principalement aux huit secteurs d'activités suivants : les télécommunications, les systèmes d'alimentation électrique, la production et le stockage de gaz et pétrole, la banque et la finance, les transports, les systèmes d'alimentation en eau, les services d'urgence, les services du gouvernement. Enfin, selon certains, le "cyberterrorisme" serait promis à un bel avenir car il serait plus simple à manipuler que le terrorisme N.R.B.C. (nucléaire, radiologique, bactériologique et chimique).

2.2.3- Pourquoi le terrorisme néglige-t-il pour l'instant le cyberespace, en tant que zone d'affrontement violent ?

Pour certains, les groupes terroristes notamment islamistes, éprouveraient encore des réticences à user de moyens technologiques qui sont ceux de "l'Occident décadent et diabolique". D'autres ajoutent que ces groupes ne possèderaient pas les capacités et les aptitudes nécessaires. Cette hypothèse paraît douteuse au moins pour deux raisons majeures. En premier lieu, à défaut de détenir toutes les compétences requises, ils possèdent néanmoins d'importants moyens financiers leur permettant de louer les services de "hackers" ou d'ingénieurs informaticiens peu scrupuleux. En deuxième lieu, notons que *"la moitié des étudiants en cours de thèse dans nos universités sont étrangers. Depuis 1980, plus de 4000 informaticiens de niveau D.E.A. originaires des pays du Moyen-Orient ont été formés…l'espace informatique n'a pas de frontière et les attaques peuvent partir de n'importe quel point du globe".*[21] L'obstacle se situe donc ailleurs ! Les terroristes d'aujourd'hui n'auraient-ils pas pleinement mesuré les enjeux du "cyberterrorisme" ?

Bien au contraire, ils sont conscients que le rapport "coût-efficacité" reste, encore aujourd'hui, en faveur des méthodes "traditionnelles et classiques". En effet, un groupe terroriste est capable avec des moyens matériels rudimentaires et réduits de réaliser quelques

[21] Selon D. MARTIN, ex-commissaire de police D.S.T. cité dans "Menace sur Internet : des groupes subversifs et terroristes sur le Net." Grégory DESTOUCHE.

engins explosifs artisanaux et de semer ainsi la panique dans un pays entier : ce fut le cas lors de la vague des attentats du "groupe islamiste armé" (G.I.A.) en France de 1995 et lors de l'attentat d'Oklahoma City. Ces attentats illustrent comment la simple utilisation respectivement de bouteilles de gaz et d'engrais permet de confectionner de dangereuses bombes occasionnant plus de 100 morts dans le cas des Etats-Unis. Il est difficile de produire les mêmes effets dramatiques, traumatiques et psychologiques par des attaques informatiques.

Ajoutons enfin, que l'alerte à l'anthrax aux Etats-Unis à l'issue des "attentats du 11 septembre" s'est traduit par l'exportation fulgurante hors du continent américain de la terreur. Ainsi, de banales enveloppes contenant de la lessive peuvent d'une part créer la psychose, d'autre part ralentir le fonctionnement normal du courrier et enfin immobiliser indûment des moyens de sécurité à très peu de frais.

D'autres enfin, présentent les attentats du World Trade Center (celui de 1993 et celui de 2001) comme des attaques informatiques. Cette analyse semble sommaire. En effet, même si les conséquences informatiques des deux attentats ont été effectivement très importantes, il serait excessif d'interpréter celles-ci comme ayant eu pour objectif premier les réseaux informatiques. Le tragique épisode du 11 septembre constitue, en ce sens, un drame paroxystique. Car, les effets sont polymorphes et multiples tant par le nombre des victimes, par l'étendue des destructions, par les répercussions sur les économies américaine et mondiale (problème des bourses, des compagnies aériennes…), que par la recomposition engendrée dans les relations internationales.

Pour Grégory DESTOUCHE, *" le terroriste du futur sera (aussi) scientifique"*. Pourtant déjà, bon nombre de terroristes actuels ont suivi des formations supérieures de haut niveau (ingénieurs, informaticiens, mathématiciens, chimistes, pilotes de chasse...).[22] Alors pourquoi leurs compétences "high-tech" ne sont-elles pas exploitées dans l'action terroriste ?

Comment expliquer l'inexistence d'actions "cyberterroristes" alors qu'il semble acquis que de telles entreprises seraient techniquement très accessibles et qu'elles octroieraient de surcroît une parfaite impunité à leurs auteurs potentiels, sans préjuger en cela de leur redoutable efficacité? Certes, il est impossible d'écarter l'hypothèse de la dissimulation volontaire des attaques subies par des gouvernements ou des organes officiels, qui souhaiteraient ainsi éviter la mauvaise publicité liée à ce type d'événements pour d'évidentes raisons de sécurité. Un "calme apparent" semble toutefois régner sur le cyberespace. Ce constat suggère l'alternative suivante : soit les éventuelles agressions ne répondent pas aux critères communs du "terrorisme classique" tels que définies supra, soit les

[22] Exemples : Anouar HADDAM, porte parole du F.I.S. à Washington DC est physicien, Ramzi YOUSSEF impliqué dans le 1er attentat contre le W.T.C. est ingénieur en électronique…etc

terroristes ont bien compris les avantages de l'outil Internet et ils ne souhaitent pas remettre en cause cet instrument, cet espace de liberté dont ils usent en évitant "soigneusement" de l'utiliser comme cible ou comme arme.

La stratégie des terroristes est-elle en pleine mutation ? "*…Place à un terrorisme nouveau, déstructuré et low tech…*" Xavier RAUFER.

2.2.4- L'utilisation terroriste du cyberespace est cependant incontestable.

Soit à des fins de propagande, soit à des fins opérationnelles (sources d'information, préparation d'action, création d'une internationale terroriste sur le NET, de recrutement ou de formation initiale…), les groupes terroristes exploitent assurément le WEB.

En effet, les N.T.I.C. favorisent la coopération transnationale du terrorisme international. Elle peut revêtir les aspects suivants : la collaboration spontanée entre groupes permettant une coordination stratégique ; l'échange de services, de matériels de formations ou d'informations ; le parrainage et la coordination par un pays disposant d'appuis logistiques de par le monde ; la "multinationalisation" des actions terroristes, usage de sanctuaires dans des pays, limitrophes ou non, aux lieux de commissions des actions. L'utilisation du NET comme outil de communication est indéniable, il favorise l'échange de mails par procédé de cryptage ou par dissimulation dans des documents photographiques.[23] Par ailleurs, sur le réseau figurent en ligne des documents subversifs dont "le parfait manuel du terroriste" où l'on peut s'informer des méthodes pour commettre un attentat à la bombe, un assassinat ou confectionner des faux papiers. Il est très improbable que ces renseignements s'adressent à des terroristes chevronnés qui acquièrent les règles de "l'art terroriste" dans des camps d'entraînement et non sur le NET. En revanche, ce manuel représente un réel danger pour les esprits influençables, pour tout groupe ou tout individu marginal souhaitant connaître le ba-a-ba de l'action subversive. Ajoutons aux facilités autorisées par les N.T.I.C., le renseignement satellitaire. Il est désormais à la portée de toutes les bourses. Pour 275 à 730 €, il est aisé d'obtenir[24] par Internet des photographies de n'importe quel coin de la planète grâce au satellite "Earlybird I". Enfin, grâce au N.T.I.C. les réseaux terroristes peuvent également gérer en temps réel leurs avoirs et financer rapidement leurs actions.

Mais l'utilisation de l'outil informatique à des fins de communication entre terroristes signifie-t-elle pour autant l'apparition d'une nouvelle menace hâtivement baptisée : "cyberterrorisme" ?

[23] Ce procédé de dissimulation d'informations se nomme la stéganographie.
[24] D'après Laurent ZECCHINI, "Un satellite espion pour M. Tout-le-Monde", le Monde du 28-29 déc.1997.

2.3- La menace "cyberterroriste" est-elle réelle?

2.3.1- Oui, particulièrement dans le cadre d'un conflit informationnel.

Ainsi, "le terrorisme informatique" (ou terme plus approprié : le piratage informatique lorsqu'il a pour but de détruire des systèmes informatiques ou de mettre en danger des populations), doit être considéré comme un acte proche d'un acte de guerre, au point d'en constituer un prélude. Toutefois pour s'avérer totalement efficace, il doit peut-être s'inscrire dans la durée et dans une stratégie à long terme. Cette stratégie viserait au piratage des systèmes informatiques de manière synchronisée, ainsi qu'à l'infiltration d'agents dans différentes compagnies afin d'y insérer des "chevaux de Troie" ou des "backdoors". Ce serait donc un travail de longue haleine. En réalité, de telles actions s'inscriraient dans la phase préliminaire d'un conflit armé, une sorte de "Pearl Harbor informatique".

Le scénario pourrait être le suivant : un "rogue state"[25] désirant attaquer un état voisin aurait tout intérêt à conduire, préventivement ou non, une attaque informatique soit contre cet état, soit contre une nation qui pourrait contrecarrer son expansionnisme guerrier. Mais dans cette hypothèse, nous sommes alors confrontés non pas tant au "cyberterrorisme" mais davantage à la phase initiale d'un conflit informationnel.

2.3.2- Non. Les dix raisons pour ne pas sombrer dans la paranoïa.

Martin C. LIBICKI[26] du National Defence University apporte des éléments de réponse. Il déclare : "*les systèmes d'information sont–ils vulnérables ? Beaucoup trop. Une catastrophe est-elle possible ? Oui, car non impossible. Mais doit-on en perdre le sommeil et craindre que des pirates mettent les Etats-Unis à genoux ? Voici dix raisons qui nous font répondre non*". Ses arguments, classés du moins déterminant au plus pertinent, peuvent être résumés ainsi.

10- ça n'est jamais arrivé, les attaques signalées jusqu'à maintenant ne constituent que de "simples piqûres de guêpes";

9- si les incidents s'accumulent, les usagers prendront la sécurité plus au sérieux et dresseront des barrières;

8- les "firewalls"[27] et les détecteurs d'intrusion fonctionneront un jour;

7- la défense d'un système entier en surveillant son périmètre est une gageure. En revanche, il est possible de fixer efficacement son attention défensive sur les composants clés du système afin de s'assurer de leur intégrité, de leur confidentialité, et de leur accessibilité;

---

[25] "Etats voyous", qui ne respecteraient pas les règles du droit international.

[26] Auteur de "What is Information Warfare ?" INSS, Advanced Command Concepts and Technology Center, 1995.

[27] Protection "pare-feu" dont le principe repose à la fois sur le cloisonnement et la pratique des sas.

6- le recours privilégié aux signatures informatiques, au détriment des mots de passe, protégerait mieux les données;

5- le développement constant des cd-roms (de grandes capacités) permet d'éviter des pertes en mode de sauvegarde de données, surtout si elles sont très volumineuses. De plus, les systèmes d'exploitation sur cd-rom sont protégés contre les virus postérieurs à leur production;

4- l'inaccessibilité d'un système sensible est garantie en évitant sa mise en réseau;

3- la plupart des pannes délibérées des systèmes informatiques proviennent jusqu'ici de sabotages provoqués par des actions malveillantes et internes;

2- la nature peut faire pire pour paralyser un Etat. De plus, il ne suffit pas seulement de détériorer les systèmes, il faut aussi empêcher leur restauration. A supposer qu'il soit possible de démanteler pour deux jours les infrastructures américaines principales, la perte de P.N.B. s'élèverait à environ 20 milliards de dollars. Cette facture s'inscrit dans la même échelle d'importance que les conséquences financières de l'ouragan Andrew (25 MM$).

1- enfin, "*les Etats-Unis peuvent faire pire, face à une attaque scélérate dont les auteurs seraient identifiés. Leur appareil militaire est en mesure de porter des coups bien plus rudes. Un argument que tout acteur rationnel peut garder à l'esprit*".

Pour un état aux dimensions et capacités plus modestes, tel que la France, le constat et les dix arguments de LIBICKI restent pertinents. La tempête de fin 1999 a provoqué des dégâts, des perturbations bien plus graves pour notre économie et la survie des populations que le "bogue" tant redouté de l'an 2000. Cette tempête a causé pour 13 milliards d'Euros de dégâts et elle a fait 90 victimes. Ces faits nous incite à relativiser la menace du "Pearl Harbor électronique" sans toutefois l'ignorer.

2.4- Alors pourquoi fait-on l'amalgame entre les mots cyber et terrorisme dans un néologisme : "cyberterrorisme"?

2.4.1- Ne peut-on imaginer des raisons politiques, économiques voire quasi "mystiques"?

En effet, le terrorisme est un terme et un thème mobilisateurs à la fois pour obtenir des moyens financiers afin de développer des technologies de plus en plus performantes, et à la fois pour justifier auprès des citoyens la restriction de certaines libertés.

L'exemple de la cryptologie est significatif, de la volonté de limiter la confidentialité du courrier électronique pour des raisons de sécurité. Ainsi, le cryptosystème

P.G.P.[28] offre-t-il une quasi certitude d'inviolabilité des courriers cryptés, aux grands dams des agences de renseignements.[29]

Les propos de l'attorney general, Janet RENO, en 1996 au sujet de l'exportation de matériel de cryptologie hors des Etats-Unis soulignent la réticence des services officiels à l'égard des moyens techniques qui amenuisent et limitent leur contrôle : *"la conséquence de la prolifération de cryptologie incassable aurait en fait un impact considérable, car nous perdrions notre capacité à chercher et à saisir des données informatiques et toute forme de preuve électronique. Même si nous disposions d'un mandat de perquisition en bonne et due forme, celui-ci serait inutile tant que nous disposerions pas de la clé".*

En France, la cryptographie est restée longtemps l'apanage des services de renseignements jusqu'à la parution des décrets n°99-199 et 99-200 du 17 mars 1999. Ces textes autorisent désormais l'utilisation de la cryptologie jusqu'à 128 bits : c'est à dire une cryptologie presque "incassable". Cette autorisation était rendue nécessaire notamment car nos entreprises ne disposaient d'aucun moyen sérieux de cryptage alors même que des moyens performants comme P.G.P. était librement disponible sur le WEB.[30]

Néanmoins, dans le cas d'espèce, les inquiétudes de Mme RENO paraissent non dénuées de fondement. En revanche, d'autres hautes personnalités de l'administration américaine n'hésitent pas à entretenir la paranoïa.

En effet en 1995, 500 attaques informatiques avaient été décelées aux Etats-Unis. Selon la D.I.S.A. (Defence Information Systems Agency) seulement 0,2% des attaques réelles sont identifiées, ce qui porterait le total des attaques supposées à 250 000. Bien que discutable dans son mode de calcul, cette information est relayée sans nuance par le Directeur de la C.I.A. devant le Sénat. Il cite même une pseudo étude du "Departement of Defence", ce qui confère plus de crédit à son propos visant à alerter sur les 250 000 attaques informatiques prétendument recensées en 1995. Or, Georges TENET est trop bien informé pour s'être ingénument trompé à la fois dans les chiffres et dans le service source. Toutes proportions gardées cela ne rappelle-t-il pas, par exemple, les efforts de communications du Pentagone pour présenter les forces armées irakiennes, avant "Desert Storm", comme la 4ème armée du monde ? Le jeu de certains services de sécurité et de renseignements n'est-il pas de grossir la menace ?

[28] P.G.P. (pretty good privacy) est une combinaison de trois systèmes RSA, IDEA, MD5, c'est grâce à IDEA(international data encryption algorithm) que chaque fois qu'un message est crypté avec P.G.P., y compris avec une clé identique, « le texte » obtenu est différent. IDEA agit sur l'ensemble du message, en utilisant une clé de 128 bits.

[29] Selon Jean GUISNEL dans "Guerres dans le cyberespace".

[30] Voir l'article du C.E. BARLOY dans le n°25 de "la Tribune du C.I.D.", décembre 2001.

Par ailleurs, les efforts technologiques consentis pour combattre le "cyberterrorisme" sont politiquement plus corrects que ceux accomplis pour acquérir "l'info-dominance" y compris dans le cadre de la guerre économique. Or, les moyens mis en œuvre pour lutter contre le terrorisme peuvent être indifféremment utilisés tant dans "l'infoguerre" que dans la guerre économique. Il en est ainsi du détournement du "système Echelon" à des fins de guerre économique.

Enfin, le terrorisme informatique contribue à développer le marché de la sécurité informatique, notamment par la création d'officines spécialisées et de protections diverses. L'explosion du marché des logiciels anti-virus avec leurs constantes mises à jour constitue une démonstration éclatante du dynamisme des activités liées à la sécurité informatique. Toute organisation disposant de systèmes informatiques possède aujourd'hui un directeur chargé de la sécurité des systèmes informatiques. De plus, tout un pan de l'économie mondiale dépend des nouvelles technologies, lesquelles possèdent même leur marché et leur indicateur boursier spécifique, le NASDAQ.

En outre, n'y aurait-il pas dans nos sociétés post-industrielles le fantasme du "high tech" ? Ce dernier serait à la fois la source du bien être de nos sociétés occidentales mais il pourrait également en causer la perte. Il s'agit ici de l'application moderne de l'adage "celui qui vit par l'épée périra par l'épée". Souvenons nous à ce sujet des craintes pour ne pas dire des angoisses entretenues par des "prédicateurs alarmistes" au moment du passage à l'An 2000. Peur augmentée par le bogue qui devait paralyser nos entreprises, nos ordinateurs et finalement toutes activités humaines s'il n'était pas correctement anticipé. Les investissements financiers consentis soit pour exécuter des audits préalables, soit pour développer des logiciels de protection n'ont pas toujours convaincu de leur utilité.

2.4.2- "Cyberterrorisme" : Mythe ou réalité ?... Le mythe du "doomsday".

"Nous distinguons mal les périls réels des virtuels ! Quelle est la part de l'inconnu, de l'hypothèse, de la légende, de la dissimulation ? … Comment appréhender exactement un phénomène d'après des cas mal documentés, des rapports censurés ou des vantardises non vérifiées ? La panique s'installe face à des dangers imaginaires ou largement surestimés (bogue de l'an 2000), mais que personne ne peut prendre le risque de traiter par le mépris".[31] La politique de l'impasse équivaudrait à la stratégie de l'échec cuisant. Face à un risque mal identifié aux contours incertains, aux modes d'actions divers et aux motivations complexes, les autorités et les organismes en charge notamment de la sécurité des systèmes informatiques ne peuvent ni écarter à priori ces risques, ni les minimiser tant ils sont lourds de

[31] Tiré de "L'ennemi à l'ère numérique" de F.B. HUYGHE.

vulnérabilités. D'autant moins que, ces risques plus ou moins exagérés justifient aussi leurs existences, leurs missions et leurs moyens.

Le mythe est soigneusement entretenu à la fois par les autorités politiques, les militaires, les services de renseignements, les officines de sécurité informatiques, les sociétés informatiques, les auteurs…etc… pour des raisons très différentes selon les cas. Mais, à force de crier "aux loups !", le risque est de ne plus suffisamment mobiliser les énergies et les volontés le moment venu. Autour des "cyber-vulnérabilités" montées en épingle, l'enjeu est de donner corps à la peur soit des attaques, soit d'un véritable conflit, usant de l'Internet, mené non pas par des "bidouilleurs" excités contre quelques pages d'un site WEB, mais par des gouvernements ou des groupes terroristes. Bref une guerre cybernétique ayant les réseaux pour champ de bataille sur lequel des virus et des "bombes logiques" sont capables de bloquer les communications, les transports, et de détourner des fonds.

Comment mesurer les dangers d'intrusion sur et par le NET ? Les chiffres les plus effrayants circulent, sans distinguer toujours les tests d'intrusion conduits par des services officiels, les histoires de "hackers", l'alarmisme des services de renseignement, les réticences de certaines firmes et organismes à signaler ou à reconnaître les attaques dont ils ont été victimes.

Ainsi en 1997, 35 "pirates" mandatés par l'Armée américaine aurait pu saboter les systèmes de commande des réseaux d'électricité de toutes les grandes villes américaines dont Los-Angeles, Washington, New-York, Chicago les réseaux téléphoniques de la police et les réseaux de communication du Pentagone. Selon les autorités américaines, le taux de réussite des attaques serait de l'ordre de 80%, pour seulement 5 à 10 % des attaques réellement détectées. Des sociétés privées, américaines comme françaises, établissent un constat identique, mais il est vrai que celles ci ont un intérêt mercantile qui consiste à vendre de la sécurité informatique.

◆

En résumé, le "cybermonde" est un espace où il est très difficile de dégager la vérité du mensonge, la réalité du mythe, l'attaque de la non attaque, la menace de la paix. Nombreux sont les observateurs qui affirment voir dans le "cyberterrorisme" la menace majeure du nouveau siècle. Après en avoir défini les contours et les formes, la réalité paraît à la fois plus complexe et plus nuancée. Il semblerait en effet que les manifestations terroristes sur le cyberespace demeurent soit secrètes, soit peu spectaculaires, soit les deux à la fois. De ce fait, elles ne présentent pas les critères communs d'identification des actions terroristes telles que je les ai définies au §214.

Le caractère terrifiant du terrorisme semble difficilement s'accommoder de la virtualité du cyberespace. En effet, bien que les attaques puissent se solder par des pertes financières ou matérielles importantes, ces agressions n'ont pas un impact psychologique sur les médias et les opinions publiques comparable à celui provoqué par des destructions massives ou des pertes humaines nombreuses. Sauf à considérer qu'un jour viendra où un réseau terroriste pourra à distance commander l'explosion de n'importe quel ordinateur dans n'importe quelle société ou chez n'importe quel particulier. La propagation de la terreur n'existe pas encore sur les réseaux.

En revanche, l'utilisation du cyberespace par des terroristes, soit aux fins de propagande, soit comme vecteurs de communication et d'échange d'informations cryptées ou non, semble démontrée. De surcroît, l'exploitation des N.T.I.C. afin de transférer des fonds occultes au profit d'actions criminelles est évidente. Faut-il pour autant amalgamer les "cyberattaques" et la "cybercriminalité" au terrorisme cybernétique ? Jusqu'à présent les affaires connues renvoient davantage à des actions de pirates ("hackers", "crackers") qui par bravades ou par malhonnêteté percent des systèmes informatiques bien défendus. D'autres attaques constituent les prémices de la guerre de l'information.

Que peuvent faire les Forces Armées en réplique à ces vulnérabilités ?

◆ ◆

III) Rôle des Forces Armées dans la lutte contre les cyber-vulnérabilités.

A défaut d'un véritable "cyberterrorisme", l'information n'en demeure pas moins un enjeu. Facteur de puissance, l'information et son support de traitement privilégié qu'est l'informatique, sont plus que jamais l'objet de luttes informatiques.

La doctrine en matière de lutte informatique au sein du MINDEF (Ministère de la Défense) connaît aujourd'hui des évolutions sensibles. Bien que les Armées aient déjà pris des mesures de renforcement et de protection de leurs réseaux,[32] il leur manquait un schéma directeur global et rationnel de lutte contre les vulnérabilités informatiques.

[32] Par exemple, SOCRATE(support opérationnel constitué des réseaux des armées pour les télécommunications) est un réseau d'infrastructure qui satisfait aux normes les plus élevées en matière de débit et de protection contre les intrusions ou les agressions. Bâti autour de réseaux hertziens spécifiquement militaires, Socrate utilise aussi les réseaux fibre optique d'Orange. Les communications sur ces artères sont systématiquement chiffrées. Ces protections se doublent d'une résistance aux impulsions électromagnétiques (IEM).

3.1- Le nouveau concept doctrinal au sein des Armées définit la lutte informatique.

La sécurité de l'information y est appréciée selon trois critères : la confidentialité, l'intégrité et la disponibilité des informations.

3.1.1- Données générales.

3.1.1-1 Champ d'application de la lutte informatique au MINDEF.

Elle a pour champ d'action :

- dans le monde civil : les réseaux et les systèmes d'information ressortissant aux infrastructures critiques ou nécessaires à la continuité de l'action militaire ou de l'exercice des missions de services publics ;
- dans le monde militaire : les systèmes d'information, de commandement et de communication ainsi que ceux des systèmes d'armes.

3.1.1-2 La lutte informatique est une composante de la guerre de l'information.

Elle inclut les luttes informatiques défensive et offensive.

- La lutte informatique offensive :

Celle-ci est citée pour mémoire, elle ne sera pas développée ici, par souci de confidentialité.[33] Précisons simplement que les prouesses et les possibilités techniques reconnues aux "hackers", "hacktivistes" et autres terroristes sont pour le moins égalées par les services de renseignements, lesquels savent également user à leur avantage des vulnérabilités de l'informatique. Selon Jean GUISNEL dans "Guerres dans le Cyberespace : services secrets et Internet", ils "recrutent" parfois même des génies informatiques parmi les "hackers".

- La lutte informatique défensive (L.I.D.):

L'aspect défensif concerne les mesures de protection, de mise en alerte et les mesures prises en réaction face à une agression possible, probable ou réelle. La L.I.D. sera développée dans les lignes qui suivent.

3.1.2- Evaluation de la menace en lutte informatique.

Le MINDEF définit une menace comportant cinq niveaux : la menace stratégique, la menace idéologique, la menace terroriste, la menace cupide et la menace vengeresse.

La menace stratégique est constituée par l'espionnage entre Etats, l'atteinte contre les "infrastructures critiques", les atteintes à la sécurité de l'Etat ou au secret de défense, l'atteinte à l'efficacité de l'organisme dans l'exécution de sa mission. Elle inclut l'action militaire adverse, y compris au niveau tactique.

[33] Cette lutte informatique offensive regroupe l'ensemble des actions conduites contre des cibles informatiques adverses déterminées dans le but : de s'y introduire, de récupérer de l'information, d'en altérer le fonctionnement, voire de les détruire.

La menace idéologique vise généralement en discrétion à la diffusion, à la destruction ou à l'appropriation illégale de données relatives à des personnes ou à l'institution même.

S'agissant de la menace terroriste, elle consiste au travers **d'une action hautement médiatisée**, soit à frapper l'opinion publique afin de créer un climat national de peur, soit à interférer avec la conduite d'opérations sur un théâtre.

Enfin la menace cupide défie principalement les systèmes de sécurité d'organismes réputés inviolables.

La menace vengeresse est citée ici pour mémoire.

3.1.3- La prévention en L.I.D. - comment se prémunir ?

3.1.3-1 La prévention.

Pour prévenir la concrétisation d'une menace, selon le MINDEF il convient principalement : de surveiller les biens les plus sensibles ; de recenser, d'identifier, de suivre les personnes susceptibles d'être la cible d'une menace et celles aptes à déclencher de telles attaques ; de coopérer entre services nationaux et internationaux ; de former et d'entretenir les connaissances des exploitants et des administrateurs-réseaux ; de vérifier périodiquement l'efficacité des mesures de protection ; d'assurer la veille technologique ; d'analyser et d'exploiter les retours d'expérience.

3.1.3-2 La protection - les modes d'attaques et leurs parades.

Cinq modes d'attaques sont identifiés: l'intrusion, l'exploration, l'altération, la destruction et la saturation. Ils peuvent se combiner ou se succéder selon les effets recherchés par l'adversaire. En principe, ces agressions sont précédées d'une période d'observation des réseaux.

Face à ces attaques, des parades existent. D'abord, la cryptologie s'avère efficace contre l'intrusion et l'exploration. Ensuite, le contrôle d'accès, les sauvegardes et leurs procédures de restauration, ainsi que les mécanismes de signature, préviennent des altérations. Enfin, la redondance des équipements limite les effets de la destruction.

En revanche, il est plus difficile de se prémunir contre la saturation avant la connexion au système. Après connexion, des contrôles de flux ou de temps de connexion peuvent réduire l'incidence des attaques.

3.1.4- L'O.P.V.A.R. : organisation permanente veille alerte réponse.

Les structures mises en place par le MINDEF en matière de L.I., s'insèrent naturellement dans le schéma global de la Sécurité des Systèmes Informatiques (S.S.I.) des "infrastructures critiques" piloté par le S.G.D.N., (Secrétariat Général pour la Défense Nationale).

Pour limiter, voire éviter les conséquences des attaques, il est nécessaire de protéger en priorité les systèmes de communications et les systèmes d'informations de nos "infrastructures critiques".

Prochainement, une organisation spécifique sera chargée d'exercer, au sein du MINDEF en liaison étroite avec le S.G.D.N./D.C.S.S.I.,[34] d'abord des fonctions de veille sur et à l'extérieur des réseaux, puis des fonctions d'alerte des usagers, d'analyse de l'incident et enfin des fonctions de réponse défensive ou de contre-attaque si nécessaire.

La permanence de l'action en matière d'alerte et de réponse sera assurée par l'intermédiaire d'un centre opérationnel, disposant d'une cellule d'analyse dotée de compétences tant en informatique, en télécommunication, en bureautique, en sécurité de défense et en S.S.I. .

3.1.4-1 Les différentes fonctions : la veille, l'alerte et la réponse.

- L'organisation de la veille reposera d'abord sur "le système de confiance", véritable chaîne de vigilance au sein du ministère. Déjà active, elle est formée par des maillons suivants : le fonctionnaire S.S.I., les administrateurs systèmes et réseaux, les équipes audit, les cellules de vigilance informatique, le Centre Opérationnel Interarmées (C.O.I.A.), le Centre Opérationnel de la Gendarmerie (C.O.GEND.), et les officiers de permanence du Cabinet. Elle coopère déjà étroitement avec des organismes extérieurs comme les C.E.R.T.s.[35]

- S'agissant de la fonction alerte, elle s'articulera autour de quatre niveaux : normal, pré-crise, crise, conflit/guerre.

- Enfin, la fonction réponse garantira la réactivité dans la protection des informations. Les réponses seront soit pré-planifiées, soit commandées. En cas de menaces avérées (informatiques ou non), au titre soit du principe de précaution, soit d'une stratégie indirecte ayant recours à des moyens asymétriques, la fonction réponse s'exprimera par des actions préventives, défensives ou offensives relevant de la lutte informatique opérationnelle.

3.1.4-2 Répartition des responsabilités.

En période normale et de pré-crise, la voie fonctionnelle de la sécurité des systèmes informatiques (S.S.I.), pilotée par un haut fonctionnaire (F.S.S.I.), est responsable de la mise en œuvre d'une part des mesures de protection, d'autre part des procédures de veille, de tests, de détection d'intrusion, et enfin de la pré-planification des mesures d'identification. Elle procède à la coordination des différentes actions.

[34] Direction Centrale de la Sécurité des Systèmes Informatiques.

[35] Computer Emergency Response Team, dont les missions sont : centralisation des incidents informatiques, traitement des alertes, élaboration des bases de données des vulnérabilités, prévention par des actions de sensibilisation, coordination avec les autres acteurs de la sécurité informatique.

L'identification de l'origine d'une attaque est confiée à la D.G.G.N.,[36] à la D.P.S.D.[37] et à la D.G.S.E.

L'application des procédures pré-planifiées est du ressort de l'autorité hiérarchique concernée.

Enfin, la D.S.T. effectue l'éventuelle contre-attaque en direction de l'agresseur, alors que la D.P.S.D. analyse les risques de compromission, sauf en périodes de crise et de conflit où ces dernières missions reviennent à la D.G.S.E. et aux Armées.

3.1.4-3 La définition des niveaux de gravité et la description des réactions planifiées.

Cinq degrés de gravité sont définis pour étalonner les attaques informatiques:

- A la gravité "inacceptable" correspond une dégradation majeure du système pouvant mettre en danger des vies humaines ou avoir des conséquences stratégiques ;
- A la "très forte" gravité équivaut une dégradation majeure du système mais sans risque pour des vies humaines ;
- La "forte" gravité provoque une sévère altération de la mission ;
- La gravité "moyenne" entraîne une altération maîtrisable de la mission ;
- Enfin, la "faible" gravité génère une faible diminution du service.

Quatre types de réactions planifiées permettent de contrer une attaque caractérisée : le repérage, l'isolation, le leurre et le confinement.

- Le repérage consiste par exemple à ne pas réagir pour permettre : d'abord le recueil des éléments sur l'origine de l'attaque, ensuite l'enregistrement des traces, enfin l'identification des centres d'intérêts de l'attaquant.
- Pour sa part, l'isolation du système s'avère efficace en terme de protection mais néfaste pour la recherche de l'attaquant.
- S'agissant du leurre de l'attaquant, soit en l'orientant vers des machines leurres soit en détournant le trafic, il implique cependant un suivi en temps réel.
- Enfin, le confinement de l'attaquant à l'intérieur de son propre système, en provoquant la saturation de son terminal ou en le déconnectant, peut s'avérer nécessaire.

Simultanément à la mise en œuvre de ces réponses planifiées, la recherche en identification de l'attaquant doit systématiquement être conduite. Toutefois, en l'état actuel de la législation, la pénétration sur un réseau informatique sans autorisation formelle d'accès

[36] Direction Générale de la Gendarmerie Nationale.
[37] Direction de la Protection et de la Sûreté de la Défense.

étant interdite, la remontée d'un réseau attaqué et des systèmes interconnectés pour identifier l'auteur d'une attaque est illégale, si elle s'opère en dehors d'une enquête judiciaire.

3.1.4-4 La traçabilité permet dans certains cas d'identifier les auteurs d'une attaque.

Cette traçabilité pour des attaques d'origine externe effectuées par Internet repose sur l'adresse "e-mail", sur l'adresse I.P.[38], sur les "cookies",[39] ou sur les habitudes de travail de l'attaquant.

En effet, l'adresse "e-mail" permet de remonter au fournisseur d'accès, qui possède normalement l'identité de l'utilisateur.

S'agissant de l'adresse I.P., elle est à la base de toute communication sur Internet utilisant le protocole T.C.P./I.P.[40] Elle est attribuée par les fournisseurs d'accès Internet (F.A.I.), qui en délivrent une nouvelle à chaque connexion. Néanmoins, les F.A.I. gardent des traces de toutes les connexions, avec les adresses I.P. associées, dans des fichiers appelés "logs", qui doivent être fournis sur réquisitions judiciaires.

Ainsi, même s'il existe quelques parades, au demeurant assez complexes, les adresses "e-mail" et I.P. restent de très bons moyens pour identifier une personne. L'adresse I.P. seule suffit à assurer le profilage pour une session particulière d'un internaute résidentiel, à fortiori elle est suffisante pour assurer le profilage d'un internaute possédant une adresse I.P. fixe.

Les "cookies" sont, quant à eux, des informations permanentes enregistrées sur la machine du client Internet afin qu'il soit reconnu plus rapidement par le serveur. Ils constituent donc autant d'éléments spécifiques propres à l'identité économique, culturelle et sociale de l'internaute.

D'autres traces existent, notamment grâce aux logiciels de stockage des informations de connexions, à la fois sur les machines et au niveau des serveurs eux-mêmes.

Par ailleurs, la traçabilité des attaques d'origine interne au sein d'un système présente globalement moins de difficulté. Les analyses des traces de routages, la "journalisation" des actions permettent en effet d'identifier plus rapidement le chemin de l'agression.

En définitive, chaque connexion d'un internaute génère un ensemble de données, qui peuvent être archivées chez le fournisseur d'accès ou sur les serveurs des sites visités. Ces données de connexions sont non seulement utilisées pour facturer les connexions mais aussi pour suivre le profil de l'utilisateur à des fins de démarchage commercial. Néanmoins pour les services de police, elles constituent des informations capitales et nécessaires à l'identification

[38] Internet Protocol.
[39] Témoins et "mouchards" de connexions.

des auteurs d'infractions. En effet, elles comportent le "login" utilisé, les heures de début et de fin de la connexion, les numéros I.P. de l'appelant et des sites visités. Ces données sont conservées pour des périodes variables selon les fournisseurs d'accès.

3.2- La Gendarmerie Nationale face au défi de la "cybercriminalité".

3.2.1- La cellule de lutte contre la délinquance et la criminalité liées aux hautes technologies.

La Gendarmerie nationale a créée en 1998 une "cellule de lutte contre la délinquance et la criminalité liées aux hautes technologies", au sein du S.T.R.J.D.[41] implanté à Rosny-sous-Bois. Cette cellule compte actuellement huit personnels officiers et sous-officiers organisés en trois entités : un groupe de veille du réseau Internet, un groupe "PLANET" et un groupe de diffusion du renseignement judiciaire. Ce dispositif est complété par l'affectation au sein de chaque Section de Recherches d'un enquêteur officier de police judiciaire ayant reçu une formation spécialisée dans le domaine de la lutte contre la délinquance de haute technologie.

3.2.1-1 La mission du groupe "veille".

La mission du groupe de veille est triple. Elle consiste d'abord à surveiller le réseau aux fins de rechercher d'initiative des infractions, puis à assister les unités de la Gendarmerie dans leurs investigations liées à toutes les infractions commises par le biais d'Internet et enfin à constituer des bases de renseignements documentaires au profit des unités. Soit le groupe informe des suites de son observation l'unité territorialement compétente afin que celle-ci puisse se saisir des infractions décelées ; soit les demandes de recherche proviennent des unités afin d'orienter la surveillance du groupe ou afin d'obtenir son assistance, notamment pour "profiler" les individus suspectés.

Toutefois, les personnels formant ce groupe ne possèdent ni compétence territoriale, ni habilitation judiciaire. Ils ne sont finalement que des "témoins éclairés".

Cette veille s'effectue de manière entièrement automatique sur un ou plusieurs sites en programmant la recherche de mots clés. Des logiciels performants effectuent ces tâches de fond selon une périodicité fixée par l'opérateur. Ce dernier consulte les résultats lorsqu'il le désire. Mais la veille s'opère aussi en temps réel. En effet, chaque nuit des opérateurs surveillent les conversations sur les "chats" afin de traquer les infractions pénales.

3.2.1-2 Le rôle du groupe "Planet".

Le groupe "Planet", abrégé de "plate-forme Internet", a débuté ses activités depuis mars dernier. A terme, son objectif serait de fournir des analyses fondées sur les

---

[40] Transmission Control Protocol / Internet Protocol, jeu de procédures que les applications utilisent pour communiquer au travers des réseaux ou d'Internet.

[41] Service Technique du Renseignement Judiciaire et de Documentation.

renseignements judiciaires liés aux infractions sur Internet. Par exemple, il établirait des bases de données interrogeables en mode multicritères qui permettraient le rapprochement et le tri de nombreux "login", I.P., adresses "E-mail" et serveurs. Dans des dossiers complexes où une multitude de suspects et de sites est impliquée, il est fondamental pour progresser dans les investigations d'établir les connexions entre les uns et les autres en s'appuyant sur l'outil informatique.

Par ailleurs, ce groupe pourrait également créer des bases documentaires élaborées sur des sujets sensibles, bien que parfois en marge de la police judiciaire (terrorisme, trafic d'armes, prolifération des armes N.R.B.C.) à partir de la documentation ouverte disponible en ligne.

Les matériels et logiciels mis à disposition sont les mêmes que ceux détenus par les différents services civils et militaires en charge du renseignement : D.G.S.E., D.R.M., D.S.T.[42] Ce groupe trouvera à terme son positionnement dans le traitement de toutes les informations à caractère ou à vocation judiciaire exploitables à partir d'Internet.

3.2.1-3 Le groupe "diffusion Police Judiciaire".

Enfin, le groupe "diffusion Police Judiciaire" est en charge de la diffusion de l'information judiciaire à destination des unités ou des services extérieurs à la Gendarmerie. Il en est ainsi des portraits robots, des appels à témoins, des avis de recherches…

3.2.1-4 Les activités du groupe "veille".

Pour 2001, le groupe "veille" est à l'origine de 155 signalements d'initiative au profit des unités de Gendarmerie qui ont abouti à la saisie de plus de 2500 contrefaçons diverses.

En assistance, la cellule a participé au succès exemplaire de l'enquête baptisée "forum 44". Cette enquête a débuté dès 2000 grâce à des renseignements initiaux fournis par le F.B.I. après les interpellations aux Etats-Unis de deux individus liés à la pornographie infantile sur le WEB. Pendant deux années les investigations menées par les gendarmes de la B.R.D.[43] Nantes en liaison avec le groupe "veille" du S.T.R.J.D. ont permis de confondre un réseau de pédophilie et d'échange de photo et vidéo à caractère pédophile. Une trentaine de personnes sur toute la France ont été interpellées le 29/01/02. Le chef du réseau a été confondu d'une douzaine de viols et d'agressions sexuelles sur mineurs de moins de quinze ans car il se mettait lui-même en scènes avec ses jeunes victimes. Les analyses des connexions (S.T.R.J.D.) et des matériels informatiques (I.R.C.G.N.) ont permis de dresser les ramifications et les contours de ce réseau pédopornographique.

[42] Services de renseignements français : respectivement, Direction Générale pour la Sécurité Extérieure ; Direction du Renseignement Militaire ; Direction de la Surveillance du Territoire.
[43] Brigade de Recherches Départementale.

Toutefois, il serait erroné de croire que la "cybercriminalité" repose essentiellement sur la pornographie infantile ou la pédophilie. Bien que constituant probablement les facettes les plus abjectes, les plus tapageuses et les plus médiatisées de la "cybercriminalité", la production, la commercialisation, l'échange de photographies et de vidéo impliquant des enfants ne sont pas parmi les crimes les plus répandus sur l'Internet français. De plus, bien qu'aucune statistique officielle ne soit disponible sur le sujet, il semblerait toutefois qu'environ les trois quarts des infractions identifiées par le "groupe veille" sur le NET français soient directement liées à la contrefaçon sous toutes ses formes : musiques, vidéos, D.V.D., livres, logiciels…au profit d'un marché manifestement très juteux. De surcroît, ce marché peut servir également au blanchiment d'argent pour des organisations criminelles. La pédophilie, la pédopornographie et les escroqueries représenteraient moins du quart restant. Depuis sa création, la cellule a relevé une trentaine d'infractions distinctes, ce qui traduit une concentration de la "cybercriminalité" sur quelques activités délictueuses seulement.

3.2.2- Le "département informatique-électronique" de l'I.R.C.G.N.[44]

L'Institut de Recherches Criminelles de la Gendarmerie Nationale est chargé d'établir la preuve scientifique lors de l'enquête criminelle. Doté de matériels de pointe et de spécialistes dans différents domaines, l'institut apporte quotidiennement son concours aux unités de Gendarmerie.

Au sein de la "division criminalistique B", le "département informatique-électronique" oriente ses activités vers les fraudes informatiques et télématiques. Ces centres d'intérêts s'étendent de la lutte contre le piratage de logiciels à la contrefaçon de cartes de paiement, en passant par la téléphonie cellulaire et l'électronique appliquée. Il est régulièrement sollicité pour assister les enquêteurs lors de perquisitions. Enfin, le département travaille en relation permanente avec différents organismes nationaux et internationaux liés au monde de l'informatique.

3.2.2-1 Modalités d'exécution des missions.

L'I.R.C.G.N. exploite scientifiquement des moyens de haute technologie aux fins de révélations des preuves judiciaires. Les techniciens de l'institut savent par exemple extraire des disques durs et autres supports informatiques des informations dissimulées. Cet organisme a vocation à compléter les investigations des unités de terrain par des constatations techniques ayant valeur d'expertise en matière judiciaire.

L'institut et son "département informatique électronique" interviennent dans l'enquête judiciaire soit sur "réquisition à personne qualifiée", soit sur "ordonnance de commission à expert". Les personnels de l'I.R.C.G.N., à l'instar de ceux du S.T.R.J.D., ne

[44] Institut de Recherches Criminelles de la Gendarmerie Nationale.

possèdent pas d'habilitation en police judiciaire. Ils ont pour vocation d'apporter un concours aux enquêteurs essentiellement de la Gendarmerie Nationale mais occasionnellement au bénéfice de la Police Nationale[45]. Ce département de l'institut participe également à des enquêtes administratives, à l'assistance technique au profit d'administrations de l'Etat, à la formation d'enquêteurs et à la veille technologique.

3.2.2-2 Composition du "département informatique-électronique".

Il est constitué de trois cellules : d'une part une "unité de traitement de l'information" dont la principale mission consiste à la récupération de données sur tout types de support ; d'autre part une "unité réseaux et télécommunications" qui sert aux identifications, localisations G.S.M. et à la mise en évidence de tout acte de piratage sur des réseaux ; enfin une "unité d'expertise électronique" qui s'attache à toutes les infractions liées aux cartes à mémoire en particulier les cartes bancaires. Les piratages de décodeurs TV-satellites, l'analyse de l'électronique embarquée dans les véhicules, et celle des dispositifs de mise à feu de bombes font également l'objet d'investigations approfondies.

3.2.2-3 L'engagement de l'I.R.C.G.N. dans des groupes de travail internationaux et nationaux contre la "cybercriminalité".

Ainsi, l'institut participe activement au sein d'instances internationales résolues à combattre la "cybercriminalité".

Au sein de l'E.N.F.S.I.,[46] réseau européen des laboratoires de criminalistique, sont constitués plusieurs groupes de travail représentant différentes spécialités. L'I.R.C.G.N. y compte des participations multiples dont une présidence dans le groupe de travail sur les "technologies de l'information".

La participation, au sein d'INTERPOL, est identique. Toutefois, un officier de l'I.R.C.G.N. y assure la vice-présidence du groupe en charge de "la criminalité liée aux technologies de l'information". Cette équipe agit pour développer la formation des enquêteurs, élaborer un guide de bonnes pratiques et d'investigations sur Internet, réaliser le projet "Fidotec" (projet de base documentaire sur la contrefaçon d'objets électroniques et de cartes à mémoire), conduire des études prospectives sur les nouvelles formes de criminalité.

A EUROPOL, un groupe sur la "cybercriminalité" travaille sur plusieurs projets. L'un d'eux porte sur la création d'un réseau européen de communications électroniques entre enquêteurs et d'un centre européen d'alerte, d'analyse stratégique et de veille sur Internet.

Le "G8" réunit plusieurs équipes de travail multidisciplinaires. Le MINDEF y est représenté par l'I.R.C.G.N. dans différents groupes d'experts. C'est le cas dans le "groupe de Lyon" qui traite de "la criminalité transnationale organisée" et qui comporte un sous-groupe

[45] La Police Nationale dispose au niveau interrégional de L.P.S., Laboratoire de Police Scientifique.

sur "la criminalité de haute-technologie". A noter qu'un autre groupe, le "groupe de Rome", a la charge de la lutte anti-terroriste. Ce dernier groupe se préoccupe actuellement de la conservation des données, de la traçabilité des connexions et des communications, de la définition des procédures de contact 24H/24H et 7 jours sur 7, de l'accès transfrontalier aux bases de données.

Mais l'I.R.C.G.N. participe également à des cercles de réflexion sur la sécurité informatique tels que : le C.L.U.S.I.F.,[47] qui regroupe principalement les grandes entreprises privées françaises.

Par ailleurs, l'institut entretient des contacts fréquents avec la communauté du renseignement : D.S.T., D.G.S.E., et les services liés à la S.S.I. : D.C.S.S.I., CELAR,[48] CASSI.[49]

Enfin, l'I.O.C.E. (International Organization on Computer Evidence) regroupe la plupart des agences gouvernementales en charge de la sécurité (douanes, police, gendarmerie), afin de développer les échanges et de proposer des standards de traitement de la preuve numérique.

◆

En somme, les Forces Armées prennent une part active dans la prévention, la protection, l'alerte et le traitement des menaces liées à "l'infoguerre" et à la "cybercriminalité" tant par le développement d'organismes en charge spécifiquement de sécurité informatique ou de criminalité liée à la haute-technologie, tant par la définition d'une doctrine rationnelle de lutte informatique, tant par la coopération renforcée et l'entretien des synergies avec d'autres acteurs extérieurs au MINDEF qu'ils soient nationaux ou internationaux. En effet, les réseaux informatiques ne connaissent pas les frontières. Dans le domaine de la "cybercriminalité", par exemple, la réponse ne peut pas être uniquement nationale. Aussi devrions nous à l'avenir observer des progrès marquants dans l'harmonisation des législations et dans les échanges d'informations entre les états, à l'instar des progrès apparus dans la "Convention européenne sur la cybercriminalité", élaborée par le Conseil de l'Europe à Budapest le 23 novembre 2001.

Les vulnérabilités informatiques sont bien réelles :"infodominance" , "guerre économique", "infoguerre", "cybercriminalité" mais le "cyberterrorisme" en tant que manifestations de violences terrifiantes par des moyens informatiques me paraît relever de l'anticipation. Il existe donc le danger de ne pas discerner derrière les risques "high-tech" des menaces "low-tech" pourtant très actuelles.

---

[46] European Network of Forensic Science Institutes.
[47] Club de la Sécurité Informatique Français.
[48] Centre d'Electronique de l'Armement.
[49] Centre de l'Armement pour la Sécurité des Systèmes Informatiques.

En effet, en matière de terrorisme, les "événements du 11 septembre" démontrent que les méthodes brutales ont encore la préférence des terroristes. Ces attentats d'une extrême violence, qualifiés "d'hyperterrorisme",[50] confirment que les ressorts de l'action demeurent encore "low tech" : détournement d'aéronef, cutter…Avec une efficacité létale jamais atteinte auparavant, ce terrorisme est loin du cyberespace mais malheureusement terriblement "efficace". Les groupes terroristes les plus connus sur la planète : E.T.A., G.I.A., Hamas,…pratiquent toujours aussi largement des attentats meurtriers en usant soit de l'explosif soit de l'assassinat pur et simple.

◆ ◆

Conclusions :

Si nul ne peut nier l'utilisation du cyberespace par des criminels de droit commun voire même par des terroristes pour leur propagande et la préparation de leurs actions, le "cyberterrorisme" m'apparaît néanmoins plus comme un risque pour le futur que comme une "menace actuelle".

L'association du mot terrorisme à celui du cyberespace a pour effet de mobiliser davantage les décideurs politiques, les agents économiques, l'opinion publique et de les sensibiliser à la nécessité de prendre des mesures contraignantes y compris à l'égard des libertés publiques. L'absence de définition officielle et universelle du terrorisme, notion contingente, d'un état à l'autre mais aussi d'une époque à l'autre, contribue à entretenir un flou très commode à la fois pour les gouvernants, les services de renseignements, les officines de sécurité informatique et les auteurs d'ouvrages dont les "cybermenaces" deviennent un fond de commerce lucratif.

Le "cyberterrorisme" n'est pas une menace actuelle. En effet, soit des attentats terroristes sur les systèmes informatiques se sont déjà produits et leurs dissimulations par les autorités ou leurs faibles retentissements ne renvoient pas l'image de terreur ; soit il n'y a pas eu encore d'actes "cyberterroristes" ce qui accréditerait la thèse selon laquelle les terroristes n'ont pas d'intérêt prononcé pour le déferlement de violence sur les réseaux.

En revanche, le cyberespace est un terrain largement exploité par la criminalité organisée : celle des cartels de la drogue, des milices paramilitaires et des "guérillas dégénérées" mais aussi celle de réseaux adeptes de contrefaçon ou de pédopornographie. Ces entités utilisent déjà amplement les N.T.I.C. et elles sont totalement immergées dans la société de l'information. Elles possèdent, de surcroît, des capacités technologiques importantes ou

[50] Selon l'expression de F. HEISBOURG, directeur de la Fondation pour la Réflexion Stratégique.

elles sont susceptibles de se les procurer aisément afin de porter leurs coups sur le cyberespace.

Du point de vue militaire, une multitude de "cyberattaques" en préalable d'un conflit armé ou l'accompagnant est en revanche très plausible. Le but de ces attaques serait de profiter des vulnérabilités des systèmes informatiques, véritable "talon d'Achille" des sociétés occidentales. Cette perspective s'inscrit dans un contexte de guerre de, pour et contre l'information.

En fait, à mon sens, la menace la plus actuelle (la plus prégnante) se développe dans le domaine de la guerre économique. Le cyberespace constitue un terrain propice à l'espionnage, à la collecte du renseignement économique, industriel et commercial soit à partir de "l'information ouverte", soit grâce aux services de renseignements officiels, soit par le biais d'officines "d'intelligence économique".

Néanmoins, il a souvent été reproché à l'outil de défense d'être calibré pour la dernière guerre. Il ne faut donc pas lui reprocher, aujourd'hui, l'anticipation ; d'autant qu'il serait présomptueux d'écarter irrémédiablement le "cyberterrorisme" des menaces pour l'avenir.

Les systèmes informatiques sont incontestablement vulnérables, surtout dans le cadre d'un conflit informationnel, mais faut-il pour autant craindre le pire, une catastrophe qui débuterait par des attaques informatiques généralisées sur les réseaux sensibles ? Il peut être répondu : oui, pour la phase préalable d'une guerre de l'information entre états ; non dans le cadre du terrorisme qui pour l'instant encore semble privilégier des options plus radicales.

•-•-•

SOURCES :

Ouvrages :

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

LIBICKI Martin, "What is Information Warfare ?", Août 1995.

SCHWARTAU Winn, "Terminal Compromise", 1993.

DESTOUCHE Grégory, "Menace sur Internet : Des groupes subversifs et terroristes sur le Net", Editions Michalon, 1999.

HUYGHE François-Bernard, "L'ennemi à l'ère numérique", Presses Universitaires de France, 2001.

Textes :

Loi : 86-1067 du 30/09/1986 : liberté de communication.
Loi : 88-19 du 5/01/1988 : Atteintes aux systèmes de traitement automatisé de données.
Décrets 99-199 et 99-200 du 17 mars 1999 : Cryptologie.
Loi : 2000-719 du 1/08/2000 : Identification des "contributeurs" illicites et obligation limitée des "hébergeurs".
Loi : 2001-1062 du 15/11/2001 : loi sur la sécurité quotidienne (art. 29 et 31).
Convention européenne sur la "cybercriminalité", Conseil de l'Europe, Budapest 23/11/2001.

Sites WEB :

Légifrance
http://légifrance.gouv.fr/

Patrick GALLEY, Terrorisme informatique, quels sont les risques ?
http://homer.spaw.ch/~spaw-1165/infosec/sts/iw.html

Mark POLITT, Cyberterrorism fact or fancy
http://guru.cosc.georgetown.edu/~denning/infosec/pollitt.html

The Terrorism Research Center
http://www.terrorism.com/

D.S.C.C.I. documentation
http://www.scssi.gouv.fr/fr/reglementation/901/index.html

SOMMAIRE :