# Le cyberterrorisme : une nouvelle menace ?

***La manipulation d'Internet permettrait à une organisation terroriste de saboter la Bourse, le trafic aérien, de prendre le contrôle à distance d'un barrage ou d'une centrale nucléaire.***

Depuis la fin de la guerre froide, de nouvelles menaces fleurissent. Le cyberterrorisme, convergence du terrorisme et d'Internet, est l'une d'elles. Certains experts le définissent comme "l'usage calculé de cyberattaques ou la menace de celles-ci pour susciter la peur". Des spécialistes ont tenté d'alerter la population sur les dangers potentiels d'une attaque informatique menée par des terroristes. Ils n'ont pas été pris au sérieux, jusqu'aux attentats du 11 septembre 2001. Depuis, les discours ont changé et les risques sont bien réels.

## Un "Pearl Harbor informatique"

Une poignée d'informaticiens malintentionnés pourrait-elle provoquer le chaos dans nos sociétés si dépendantes de l'informatique ?

"*On ne peut que constater que la sécurité intérieure d'un pays est aujourd'hui confrontée à des menaces criminelles nouvelles, liées à l'existence des nouvelles technologies*", souligne Solange Ghernaouti, professeur à Georgetown University.

Les nombreux virus informatiques qui apparaissent régulièrement sur Internet rappellent à quel point les réseaux sont fragiles et faciles à percer.

Dans une interview au journal Ausaf, en novembre 2001, Oussama Ben Laden avait évoqué "les centaines d'islamistes ingénieurs en électronique" prêts à combattre à ses côtés.

En juin 2003, le Washington Post évoquait des infiltrations suspectes, via Internet, depuis des pays islamiques, sur des ordinateurs appartenant à des sociétés de distribution d'eau, d'électricité ou d'autres infrastructures vitales. On reparle aussi d'une "cyberacadémie de la Terreur" au Pakistan, où les partisans d'Al-Qaïda auraient été entraînés au sabotage cybernétique.

"*La prise de contrôle d'infrastructures critiques semble être l'un des objectifs du cyberterrorisme*", prévient Solange Ghernaouti. D'après le FBI, beaucoup de sociétés ou d'institutions gouvernementales sont insuffisamment protégées contre les pirates informatiques. Quelque 5 000 infrastructures vulnérables au cyberterrorisme et dont l'attaque pourrait déstabiliser l'économie d'un pays, ont été recensées. Divers scénarios existent et décrivent l'infiltration dans des réseaux informatiques pour saboter les transactions financières, le trafic aérien, pour bloquer les communications, effacer les archives, ou changer la composition chimique de produits alimentaires dosés par ordinateur.

## Quelques exemples de cyberattaques

• En 1994, un pirate informatique de 27 ans a pénétré les systèmes informatiques d'un barrage hydroélectrique, en Arizona, sans toutefois arriver à en prendre le contrôle.

• En 1999, un adolescent du Massachusetts a pénétré le réseau informatique de la société de téléphone NYNEX. Il a coupé durant six heures le service à 600 clients, dont la police et l'aéroport local.

• Des essais ont été menés par le gouvernement américain qui a recruté des pirates informatiques, désignés par le terme anglais "hackers", pour pénétrer des systèmes gouvernementaux ou privés. Ils sont arrivés à prendre le contrôle de la plupart des réseaux électriques américains.

• Les conflits régionaux au Sri Lanka, au Timor, la guerre du Kosovo ou le début des opérations militaires contre l'Irak ont systématiquement suscité des "cyberattaques", visant, suivant les cas, des ambassades, l'Otan, des médias, un fournisseur d'accès israélien ou le Hezbollah, mais aussi des sites commerciaux et des systèmes informatiques gouvernementaux.

Dans le cas des barrages ou des infrastructures électriques telles les centrales nucléaires, elles ne devraient pas être accessibles à partir d'Internet - ou si elles le sont, une grande vigilance s'impose pour prévenir toute intrusion.

Dans la plupart des cas, le scénario catastrophe des vannes du barrage ouvertes à distance pour laisser passer des trombes d'eau ne se réalisera pas. Il suffit cependant d'une infrastructure mal protégée quelque part...

"Les systèmes sont tellement complexes qu'il est impossible d'éliminer toutes leurs faiblesses", rappelle Dorothy Denning. Quand on lui dit qu'il semble difficilement imaginable de voir des terroristes s'emparer à distance d'une centrale nucléaire, sa réponse reste prudente : "*J'espère bien que vous avez raison.*"

## "Hacktivisme" et Internet

Le cyberterrorisme n'est pas aussi facile à mettre en œuvre que certains l'imaginent. Les cyberattaques répertoriées jusqu'à présent n'étaient pas le fait de groupes terroristes. Elles sont attribuées à des internautes, idéologiquement motivés, qui veulent faire passer leur message, ou à des groupes de hackers. L'impact économique de ces actes est parfois énorme, mais ils ne peuvent pas être qualifiés de "vrai terrorisme". On parle plutôt de "hacktivisme". Ce mot est formé par le mélange d'activisme et de hacker. Il définit l'usage de moyens électroniques contre des sites ennemis : prélever ou changer des données, passer de fausses rumeurs, infecter par des virus informatiques, rendre inopérant un site Internet, ...

Kevin Mitnick est sans aucun doute le hacker le plus connu. La justice américaine l'accuse d'avoir provoqué quelque 80 millions de dollars de dégâts au cours de ses intrusions au sein des entreprises Motorola, Nokia ou Sun Microsystems. En juin 1999, il a été condamné à 22 mois de prison.

## Terrorisme et Internet

Un cyberterrorisme tuant ou provoquant des dommages matériels graves est encore hypothétique. Bien des arguments militent pourtant en sa faveur, comme son faible coût ou l'impunité qu'il procure, puisqu'on agit à distance. Aucun État n'a encore subi d'attaque concertée portant simultanément sur les circuits financiers, les transports et les réseaux publics et personne ne connaît l'étendue du chaos qui en résulterait. Reste à savoir si une panique boursière basée sur des fausses rumeurs, ou la perte d'archives importantes apporteraient à un groupe terroriste les mêmes satisfactions spectaculaires ou symboliques qu'un attentat dont les seules images répandent la panique. Un kamikaze est encore aujourd'hui plus "rentable" et moins cher qu'une offensive électronique.

Que sait-on au juste des cyberterroristes ?

Ils ont su mettre en échec des agences de renseignements comme la NSA, le FBI et la CIA, par l'utilisation des technologies numériques les plus récentes : messages électroniques codés, technique de la stéganographie - art de dissimuler des messages sous forme de pixels invisibles, noyés dans des images ou sur des sites Internet. On a découvert, par exemple, que Richard Reid, le terroriste aux chaussures piégées du vol Paris-Miami, passait ses journées dans un cybercafé parisien.

## Sauver Internet du cyberterrorisme

Dès 1947, les États-Unis ont créé un réseau d'écoute, baptisé "Échelon", pour intercepter les télécommunications du Bloc de l'Est. D'autres systèmes, comme *Etherpeek*, *Omnivore* (1997), puis *Carnivore* (1999) ont été mis en place afin de surveiller à la volée les communications électroniques.

*Carnivore* est un logiciel installé sur un ordinateur dans les locaux d'un fournisseur d'accès (FAI). Il fonctionne comme un "sniffer" très spécialisé, capable de filtrer les paquets de données qui transitent entre l'utilisateur et le FAI et de reconstituer les messages échangés : courriers électroniques mais aussi pages web visitées, conversations en direct (chats).

Ces méthodes d'investigation sont cependant improductives et inadaptées. Elles ne sont efficaces que dans des cas précis, lorsqu'on dispose d'indices permettant de savoir que tel ordinateur ou tel fournisseur d'accès sont utilisés. Mais même quand ces éléments sont disponibles, les messages interceptés sont souvent cryptés (PGP est un très bon logiciel de cryptographie, disponible gratuitement sur Internet) et donc presque impossibles à déchiffrer. Aucun logiciel, aucun expert ne peut proclamer pouvoir surveiller tous les sites web ou tous les forums de discussion sur Internet. Une veille totalement exhaustive du réseau des réseaux est impossible à ce jour.

Le vrai danger réside aussi dans de nombreux sites web ou forums de discussion qui incitent à la haine. Même un enfant de 10 ans peut trouver, en utilisant un moteur de recherche, des informations sur la fabrication d'une bombe artisanale ou d'une arme chimique.

La seule technique efficace consiste à adopter une "offensive en réseau" et apprendre à exploiter l'intelligence collective. De la même manière que les fanatiques, islamistes ou occidentaux, utilisent Internet pour déployer leur stratégie de mort, chaque internaute peut devenir un "capteur", capable d'identifier un site web qui pousse à la haine ou à l'attentat. À titre d'exemple, les autorités britanniques viennent de faire fermer plusieurs sites qui réclamaient des fonds pour financer la guerre sainte ou qui proposaient des formations à l'usage des armes à feu. Le problème actuel de cette démarche est le manque d'un organisme international habilité à recueillir et analyser de telles plaintes.

## Les robots intelligents : parade contre le cyberterrorisme ?

Une société américaine basée en Géorgie est en train de développer un nouveau type de logiciel d'intelligence artificielle, censé prédire les attaques terroristes. KARNAC sera en mesure d'examiner et d'analyser des bases de données, publiques et privées, pour repérer des activités suspectes. La société Applied System Intelligence à l'origine du projet, soutient que si un tel système avait existé il y a quelques années, il aurait été capable de prédire les attentats d'Oklahoma City, et probablement aussi le désastre du World Trade Center.

## Internet sous haute surveillance

Le cyberterrorisme est prit très au sérieux outre-Atlantique. Moins d'un mois après les événements du 11 septembre 2001, Richard Clarke a été nommé conseiller spécial du président des États-Unis pour la sécurité dans le cyberespace. Il croit dur comme fer à ce danger et le place au même plan que l'utilisation des armes de destruction massive (biologique, nucléaire ou chimique). Le 18 septembre 2002, la Maison Blanche a rendu public un premier projet de document définissant les priorités, sous le titre *The National Strategy to Secure Cyberspace*. Les mesures sont suggérées à cinq niveaux, qui vont des ordinateurs personnels et de l'équipement informatique des petites entreprises au niveau global. Il s'agit de renforcer aussi la prise de conscience des dangers potentiels.

La France place, elle aussi, Internet sous surveillance, avec la création d'un Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLTIC). Cette structure est appelée à combattre toutes les formes de criminalité liées à Internet (délinquance financière, réseaux pédophiles, cyberterrorisme...). Elle travaillera de concert avec les services de police, la gendarmerie, la douane et la Direction générale de la concurrence de la consommation et de la répression des fraudes (DGCCRF).

## Le développement des sociétés modernes s'accompagne inévitablement de nouvelles vulnérabilités

Le paradoxe du cyberterrorisme est qu'il préoccupe, mais qu'il ne s'est - heureusement - pas encore réalisé. Les réactions qu'il suscite sont partagées : "*Une souris d'ordinateur peut être aussi dangereuse qu'une balle ou une bombe*", s'inquiète un parlementaire américain. À l'inverse, d'autres observateurs se montrent sceptiques et se demandent si la flambée des préoccupations autour de la cybersécurité ne représente pas une "*nouvelle corne d'abondance*" pour les entreprises de sécurité. Le marché promet en effet d'être en forte croissance dans les années à venir.

Un élément à ne pas perdre de vue est que l'IP v6, le protocole du futur Internet 2, ne disposera pas des mêmes facilités techniques pour la surveillance des communications que l'IP v4 actuel. L'IETF (Internet Engineering Task Force), l'organisme de standardisation d'Internet, a rejeté les propositions des services secrets américains visant à inclure des spécifications techniques autorisant les écoutes légales.

Attention donc à ce que pourrait réserver l'avenir : la prochaine génération de terroristes grandira dans un monde digital et sera plus apte à en utiliser les possibilités. Le risque du cyberterrorisme ne peut que croître dans notre société, en proportion de la place toujours plus grande de l'Internet dans notre vie quotidienne.

***Références***

***http://www.nsa.gov***
***http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html***
***http://www.nautilus.org/info-policy/workshop/papers/denning.html***

**Philippe BABELON**

***jhmbabelon@graphycom.com***