

Le cyberterrorisme à nos portes ?

L'objectif pour les pirates informatiques est de déstabiliser les sociétés visées en bloquant les opérations effectuées par les systèmes informatisés névralgiques

Gagnon, Benoît

DEPUIS les événements du 11 septembre dernier, les gouvernements, par souci de sécurité, tentent de déterminer les types d'agressions qui sont susceptibles de toucher leurs infrastructures. Les menaces asymétriques- des menaces employées par un acteur incapable d'affronter de manière conventionnelle un adversaire trop fort pour lui, mais capable de lui infliger des chocs déstabilisateurs par des moyens non orthodoxes- se retrouvent projetées au premier plan. Avec la multiplication des réseaux informatiques et l'accessibilité toujours croissante d'Internet et des ordinateurs, certains spécialistes voient désormais le **cyberterrorisme** comme une forme de menace qui pourrait émerger dans les années à venir.

Avec comme but ultime de voir leurs desseins politiques s'accomplir, les terroristes sont constamment à la recherche de nouveaux moyens pour arriver à leurs fins. Selon plusieurs spécialistes du terrorisme, le **cyberterrorisme** va vraisemblablement devenir l'un des moyens de prédilection des terroristes dans les années à venir. En effet, ses moyens d'action sont accessibles et peu coûteux. Or nos sociétés, de plus en plus "branchées" aux réseaux informatiques, sont plutôt fragiles face à ce type d'attaques.

Une fragilité causée surtout jusqu'à maintenant par le manque d'attention que les responsables sécuritaires accordent à cette menace. Cette situation est probablement liée à une méconnaissance du phénomène et de ses possibilités, aux coûts astronomiques de mise en place d'une cyberdéfense efficace et au fait que le **cyberterrorisme** ne s'attaque pas directement aux vies humaines.

Qu'est-ce que le **cyberterrorisme**?

Qu'entendons-nous par **cyberterrorisme**? Le **cyberterrorisme** rejoint le terrorisme classique. C'est une action violente et symbolique ayant pour mandat de faire changer des comportements sociopolitiques en dérangeant les opérations normales de la société. Évidemment, en ce qui a trait à la violence, il faut ici considérer qu'une attaque informatique constitue une action violente, notamment parce qu'elle perturbe les activités quotidiennes des sociétés.

Avec le **cyberterrorisme**, les attaques perpétrées visent les réseaux informatiques importants qui constituent un des piliers des sociétés technologiquement évoluées. L'objectif est de déstabiliser les sociétés visées en bloquant les opérations effectuées par les systèmes informatisés névralgiques. Ainsi, des tests effectués par le département de la Défense des États-Unis ont démontré l'ampleur que pourrait prendre une telle attaque. L'exercice *Eligible Receiver*, mené aux États-Unis à la fin des années 1990, a démontré que des cyberterroristes pourraient aisément attaquer des structures informatiques névralgiques. En effet, 35 agents de la National Security Agency avaient réussi, en moins de deux semaines, à pirater le système d'alarme (911) de bon nombre d'États, le submergeant de faux appels, et à s'attaquer à 41 000 des 100 000 ordinateurs du Pentagone. Le tout avait été fait à l'aide de plates-formes informatiques commerciales, camouflant ainsi le passage dans le cyberspace.

Effets déstabilisants

Imaginons simplement les effets déstabilisants sur l'économie occidentale d'une cyberattaque organisée. Entre autres, les terroristes pourraient utiliser les infrastructures informatiques pour bloquer les réseaux de communication, perturber les opérations informatiques et, finalement, porter atteinte aux entreprises et aux particuliers.

Tout porte à croire que le **cyberterrorisme** deviendra un phénomène de plus en plus important dans les prochaines années. En effet, il offre des avantages considérables aux terroristes: il requiert des moyens réduits et accessibles. Les ordinateurs et les logiciels suffisamment puissants pour commettre ce type d'agression sont disponibles à grande

échelle et sur le marché légal. Il est évident qu'il est plus risqué pour un individu mal intentionné de se procurer du matériel explosif acheté au noir que d'obtenir le tout dernier processeur d'Intel...

De plus, les cyberattaques peuvent être diffusées partout dans le monde et se faire de façon retardée, permettant aux terroristes de changer d'endroit avant que l'attaque ne se concrétise. De même, les cyberattaques peuvent provenir de différents endroits en même temps et ne pas dévoiler leur provenance. Autre avantage: le **cyberterrorisme** n'a pas besoin d'actions éclatantes pour être efficace, les cyberterroristes peuvent rester dans l'ombre et mettre sur pied des cyberattaques répétitives. Et cela, sans compter sur le fait que les cyberattaques n'exigent pas d'action suicide; un terroriste peut donc effectuer de nombreuses attaques.

Mais un des plus grands avantages du **cyberterrorisme** est la formation. Autrefois, les terroristes devaient suivre une formation appropriée avant de perpétrer leurs actions. Ils se rendaient dans des endroits spécifiques pour y apprendre comment effectuer leurs opérations. Ces mouvements rendaient donc leurs points de rencontre plus faciles à détecter. Or, avec le **cyberterrorisme**, la situation n'est plus du tout la même. Grâce à Internet, qui est une source inépuisable d'informations sur le piratage informatique, les cyberterroristes peuvent apprendre par eux-mêmes comment faire des cyberattaques et demeurer dans le confort de leur foyer.

Dangers et réalités

Il est à noter que le **cyberterrorisme** est d'autant plus inquiétant qu'il représente une menace flagrante pour les services de sécurité. Ces services, menant de plus en plus leurs activités à l'aide de moyens basés sur des hautes technologies, sont vulnérables à des attaques cyberterroristes, car ils multiplient les failles possibles au sein des systèmes informatiques.

Il faut toutefois mettre un bémol à ces cris d'alarme. À ce jour, il n'y a pas encore eu d'attaque cyberterroriste qui ait eu des répercussions importantes. Jusqu'ici, ce phénomène n'a entraîné principalement que des dégâts financiers. Cela s'explique par le fait que les cyberattaques ne sont pas très éclatantes: le piratage de systèmes informatiques n'a pas la même portée psychologique sur la population qu'une bombe qui éclate dans un centre-ville ou un avion qui s'écrase sur un gratte-ciel... Pourtant, le potentiel perturbateur d'une cyberattaque organisée est réel. L'importance qu'accordent de plus en plus les États à cette menace au sein de leur échelle des priorités de sécurité semble donc justifiée.

L'auteur est collaborateur à la chaire Raoul- Dandurand en études stratégiques et diplomatiques (www.dandurand.uqam.ca).

Illustration(s) :

La commotion causée par le virus Code Red en juillet dernier montre combien il est relativement facile pour un internaute malintentionné de perturber sérieusement le cyberspace.

Le numéro du 21 février du Newsweek comprenait un dossier sur le **cyberterrorisme**.

© **2002 La Presse. Tous droits réservés.**

Numéro de document : news·20020512·LA·0046

PUBLI-C news·20020512·LA·0046

Ce certificat est émis à **Université-de-Montréal** à des fins de visualisation personnelle et temporaire.

Date d'émission : **2007-11-22**

Le présent document est protégé par les lois et conventions internationales sur le droit d'auteur et son utilisation est régie par ces lois et conventions.