Le Monde.fr http://www.lemonde.fr/web/imprimer_element/0,40-0@2-3238,50-924253,0.html

Entretien avec Athina Karatzogianni, spécialiste des conflits sur le Net

Le temps des cyberguerres

LE MONDE | 16.06.07 | 14h21 • Mis à jour le 17.06.07 | 08h49

Venons-nous d'assister, en Estonie, à la première cyberguerre ?

Des cyberconflits ont été observés dès le milieu des années 1990, mais c'est la première fois que les infrastructures d'un Etat dans leur globalité, en l'occurrence celles de l'Estonie, ont été visées durablement par une attaque Internet orchestrée. D'où l'évocation de "première cyberguerre" ciblant un pays pionnier du Net, surnommé "e-Stonia". Il est d'ailleurs intéressant de noter que ce pays doit accueillir, en 2008, le nouveau centre de l'OTAN pour contrer le cyberterrorisme !

Rentrons-nous dans le siècle des cyberconflits ?

Leur nombre va, en effet, être en constante augmentation, d'autant plus que les pays, de plus en plus connectés, vont accroître leur vulnérabilité sans en être forcément conscients.

Pour autant, il faut garder le sens de la mesure. Avec humour, une lettre spécialisée, la *Crypt Newsletter*, écrit que *"ce qui est magnifique avec la cyberguerre secrète, c'est qu'elle peut être ce que chacun veut qu'elle soit"*. Certains incidents rapportés par des médias n'ont pas été vérifiés. Des alertes suscitent le doute car elles sont lancées soit par des groupes qui peuvent bénéficier directement de dépenses publiques destinées à combattre cette menace, soit par des sociétés qui vendent des services de sécurité informatique.

Y a-t-il une typologie des cyberconflits ?

Empiriquement, on peut en distinguer de deux sortes, même si ce sont des affrontements complexes, dont les acteurs ont des contours et des revendications parfois assez flous. Jusqu'à présent, nous avons observé des cyberconflits dits "sociopolitiques", déclenchés par des groupes militants comme les mouvements antimondialistes ou antiguerre qui organisent bien plus rapidement leur lutte par Internet et piratent des sites institutionnels ou d'entreprises. Il existe aussi des cyberconflits dits "ethnoreligieux", souvent la prolongation dans le cyberespace de conflits réels comme au Kosovo, ou entre Israéliens et Palestiniens, Indiens et Pakistanais, Taïwanais et Chinois. Il s'agit alors de pirater les sites ennemis, de créer des sites de propagande... Ces groupes utilisent alors l'Internet, non pas pour recadrer le débat, mais comme une arme, dans une méthode analogue à la guerre des pierres. Internet, moyen peu onéreux et facile d'utilisation, permet à ces acteurs d'atteindre un niveau d'influence qui leur était jusqu'à présent refusé ou inaccessible.

Quelle leçon pour l'avenir pouvons-nous tirer de l'événement estonien ?

C'est un signal d'alarme. L'échelle du cyberconflit estonien souligne la déficience de la communauté internationale à savoir définir les cyberconflits et réagir rapidement lorsqu'un Etat est visé. Que ces attaques massives aient été menées par le gouvernement russe, par des communautés de la diaspora russe ou, plus probablement, par des Russes vivant en Estonie, force est de constater que l'OTAN ne définit pas encore les attaques électroniques comme des actions militaires. Malgré l'importance de cet assaut, l'OTAN n'a fait qu'envoyer des experts pour comprendre ce qui s'était passé. Il faudra peut-être un plus gros Pearl Harbor électronique pour que les cyberconflits et leurs futures implications soient pris en considération.

Les Américains semblent, eux, prendre très au sérieux la menace et redoutent une attaque qui paralyserait leur économie. Est-ce crédible ?

Une crise des réseaux d'information perturberait gravement les marchés financiers, les systèmes bancaires, le contrôle aérien ou les services d'urgence. Selon un représentant républicain, un réseau terroriste aurait déjà testé les infrastructures électroniques de sociétés dans l'eau, l'énergie et les télécommunications.

Le contenu du cyberarsenal américain est un secret aussi bien gardé que les capacités nucléaires. Mais de nombreux comités ont été créés. Le plus important est le National Information and Protection Center, qui regroupe des agents du FBI, des militaires et des spécialistes de la sécurité nationale. D'autres comités regroupent des spécialistes du monde de l'entreprise et des affaires. L'un des dirigeants de la lutte contre la cybercriminalité, le major général James David Bryan, a décrit les trois missions principales à assumer : tester des cyberarmes pour mieux comprendre leur impact, ne pas les traiter comme une entité séparée, mais les inclure dans l'arsenal global de défense, former un cadre professionnel des cyberguerriers militaires.

Un tel zèle peut s'expliquer alors que la Corée du Nord, par exemple, "produit" chaque année 100 cybercriminels et que, selon le FBI, près de 90 % des entreprises et des agences gouvernementales ont été la cible d'attaques en 2002. Les autorités craignent que des cyberterroristes soient, demain, soutenus par des Etats voyous. Ou qu'ils lancent, à partir d'origines multiples, une attaque convergente sur une cible, remplaçant le mode classique : en une vague, à partir d'un point unique.

On voit que, depuis le 11-Septembre, les Etats-Unis sont rentrés dans un mode répressif très binaire, qui divise le monde entre "eux" et "nous" et dont une des conséquences est une érosion des droits civils. Il reste encore à convaincre l'opinion de la nécessité d'actions intrusives des autorités pour assurer la sécurité nationale face aux cyberconflits. Peut-être si le pays est victime d'un événement à l'estonienne.

L'Europe est-elle préparée ?

L'Europe s'est jusqu'ici plus intéressée aux contenus Internet relatifs à la propagande néonazie, à la pédophilie, à la fraude électronique... Les choses pourraient changer après ce qui vient de se dérouler.

Peut-on évaluer la menace que représente Al-Qaida ?

Le réseau terroriste s'accommode évidemment bien d'un réseau de communication sans frontière. Il l'a utilisé comme outil de mobilisation avant le 11-Septembre, et encore plus après la destruction de ses cellules en Afghanistan, au Pakistan et en Arabie saoudite. Internet est, pour Al-Qaida, un moyen de recrutement et d'entraînement, un outil de propagande ainsi qu'une arme pour perturber les opérations financières ou pour voler des données. Al-Qaida, acteur à caractère ethnoreligieux, dont l'idéologie ne repose pas sur une identité nationale, est un cas unique pour ce qui est de l'utilisation des ressources offertes par le Web. Selon le récent avertissement lancé par un élu républicain américain, il y a 50 % de chances que le prochain attentat d'Al-Qaida sur les Etats-Unis inclue une cyberattaque.

Propos recueillis par Laure Belot et Jean-Pierre Stroobants

LE CAS ESTONIEN

26 AVRIL.

Le déplacement de la statue d'un héros de l'armée soviétique symbolisant la libération de l'Estonie en 1944 provoque des émeutes.

29 AVRIL.

Début des cyberattaques vers les serveurs d'institutions publiques et privées estoniennes - ministères, banques... - en les bloquant par "saturation" : des millions de faux messages sont envoyés sur des serveurs mails, des millions de requêtes sur des serveurs Web.

Pour réussir cette manoeuvre, les pirates ont, aux Etats-Unis, au Pérou, en Chine ou encore Vietnam, pris le contrôle d'ordinateurs à l'insu de leurs propriétaires ou ont loué des serveurs à des prestataires peu scrupuleux. Ils ont ainsi constitué un réseau clandestin et éphémère de 1 million d'ordinateurs qui a permis des attaques simultanées de sources multiples. Une technique désormais classique.

8 ET 9 MAI

. Attaques les plus massives, (certaines ont duré plus de dix heures), le jour de "la grande fête patriotique" où la Russie célèbre la victoire de 1945.

SUR INTERNET

Think tank américain sur les cyberconflits. WWW.CYBERCONFLICT.ORG/

À LIRE

The Politics of Cyberconflict d'Athina Karatzogianni (Routledge 2006).

Article paru dans l'édition du 17.06.07