




La Presse

Forum, samedi, 10 août 2002, p. A13

 Voir la page PDF

La cyberguerre

Les guerres ne sont plus que conventionnelles;elles ont trouvé un nouveau champ de bataille: Internet

Gagnon, Benoît

INTERNET est devenu un nouveau champ de bataille international. La guerre qui se déroule présentement entre Israël et l'Autorité palestinienne a provoqué une telle montée de la violence qu'elle s'est déplacée dans le cyberspace. Dorénavant, une **cyberguerre** virulente et surtout très coûteuse se déroule parallèlement aux luttes armées "traditionnelles". En fait, la situation est tellement dramatique que plusieurs discutent d'une "Netintifada" ou d'une "e-djihad".

"Hactivisme" et cyberattaques

Nous constatons deux pivots dans la **cyberguerre** se déroulant au Proche-Orient. Le premier pivot consiste surtout à déstabiliser les différentes communautés en utilisant le cyberspace. Cela se fait principalement avec l'"hactivisme", c'est-à-dire l'utilisation d'Internet pour véhiculer des messages activistes, dans ce cas-ci des messages propagandistes. Par exemple, le site pro-palestinien Electronic Intifada (<http://electronicintifada.net>) ou encore le site pro-israélien Israel Support Group (<http://www.israelsg.com>) sollicitent très explicitement un appui à leurs causes respectives.

Malheureusement, cet hactivisme se transforme souvent en cyberviolence. Des messages haineux sont propagés à travers le cyberspace pour rallier les masses vers des actions de cyberlutte, voire de lutte armée, contre l'ennemi. De nombreux sites de clavardage se sont ainsi transformés en véritables plates-formes servant à menacer l'adversaire. D'autres méthodes encore plus agressives d'hactivisme ont aussi été rapportées. Des virus informatiques activistes se sont propagés un peu partout dans la région israélo-palestinienne, comme le fameux virus Injustice. Lorsqu'il était activé, ce virus faisait apparaître à l'écran un message rappelant la mort d'un jeune Palestinien sous le feu des soldats israéliens. Certes, ce virus s'excusait auprès de l'utilisateur, signifiant que son créateur espérait simplement la paix pour la Palestine, mais il se dédoublait et s'envoyait aux 50 premiers contacts présents dans le logiciel de courriel Outlook. De plus, il dirigeait automatiquement l'utilisateur vers plusieurs sites pro-palestiniens.

Le second pivot utilisé dans la **cyberguerre** proche-orientale est la perpétration d'attaques et de ripostes contre des systèmes de données. Ces cyberattaques consistent surtout en des déformations ou des destructions de sites Internet qui représentent des intérêts dans un camp ou dans l'autre.

La première attaque informatique recensée dans la région israélo-palestinienne date d'octobre 2000 et fut perpétrée par des adolescents israéliens en réaction à l'enlèvement de trois soldats israéliens par des forces palestiniennes. Les sites du Hezbollah libanais et le portail arabe Albawaba (<http://www.albawaba.com>) ont été les victimes de cette cyberagression. Au cours de cette cyberattaque, une image du drapeau israélien fut implantée sur le site du Hezbollah et le portail Albawaba a vu sa page d'accueil bloquée pendant plusieurs heures, empêchant le transit d'informations sur le site.

Israël est particulièrement vulnérable

Depuis septembre 2000, 1295 cyberattaques perpétrées au Moyen-Orient ont été recensées, dont 548 furent dirigées contre les portails israéliens. Israël est particulièrement vulnérable aux attaques informati- ques, car elle a le plus grand nombre de connexions Internet dans la région du Proche-Orient. Elle possède 2,4 millions de connexions Internet, soit plus que n'importe quel des 22 pays arabes.

Plusieurs sites emblématiques d'Israël se sont faits attaquer par des groupes arabes. Soulignons par exemple des sites comme celui de la Bank of Israël, celui du Tel-Aviv Stock Exchange, ou encore le site d'Isranews, un site francophone d'informations israéliennes. Tous ces sites furent criblés par des cyberattaques les rendant inopérants pendant de longues heures.

De surcroît, les attaques informatiques ne se limitent pas à la région immédiate du conflit. De nombreux sites de

lobbyistes présents aux États-Unis se sont fait dévisager et dévaliser par des cyberattaques arabes provenant d'un peu partout dans le monde. Notons, entre autres, la page d'accueil du site du American Israel Public Affairs Committee (AIPAC), qui a été modifiée par des pirates qui en ont fait un site d'accès à de la pornographie et à des informations sportives. Lors de cette attaque, les cybervandales se sont aussi emparés de près de 200 numéros de cartes de crédit, d'informations personnelles sur quelque 700 personnes et des adresses de courrier d'environ 35 000 des 55 000 membres.

Les mouvements pro-palestiniens de cyberlutte sont de plus en plus diversifiés et la diaspora arabe y participe fortement. Notons comme exemple le Pakistan Hackerz Club, considéré comme le fer de lance dans la cyberlutte palestinienne. D'autres groupes se joignent rapidement au mouvement comme le Unix Security Guard (USG), né en mai dernier, qui regroupe une alliance internationale de hackers anti-Israéliens. Plus de 87 cyberattaques contre des intérêts israéliens sont imputables à ce groupe depuis leur naissance.

Évidemment, Israël n'est pas en reste. De nombreux groupes très organisés se sont lancés dans la **cyberguerre**. Mentionnons le M0ssad, un groupe de hackers qui s'est surtout distingué lorsqu'il a réussi, en mai 2001, à détruire plus de 480 sites Internet en moins d'une minute. D'autres groupes influents comme les Israel Hackers (<http://www.israelhackers.cjb.net>) ou le Israel Internet Underground (IIU) émergent rapidement pour se livrer à la cyberbataille.

Ces divers groupes ont attaqué de nombreux sites liés de près ou de loin aux intérêts palestiniens. Par exemple, le site Al-Aqsa (<http://www.al-aqsa.org>), un site pro-islamique véhiculant des messages d'appel à la lutte contre Israël, s'est fait dévisager par le M0ssad. Le site d'information arabe Gulf News (<http://www.gulfnews.com>) a aussi goûté à la médecine des hackers. Cela est sans compter les différentes cyberattaques perpétrées sur des sites reliés de près ou de loin au Hamas.

Un phénomène grandissant

Les cyberagressions qui se déroulent au Proche-Orient ne sont pas des phénomènes isolés. En fait, on peut constater que les tensions régionales ont une fâcheuse tendance à déborder de plus en plus dans le cyberspace. À titre d'exemple, la région indou-pakistanaise est présentement le théâtre d'une **cyberguerre** qui prend de plus en plus d'ampleur. Une alliance de hackers pakistanais nommée Anti-India Crew (AIC) s'est lancée dans une croisade informatique contre les intérêts indiens, entraînant jusqu'à ce jour 77 cyberattaques sur des sites indiens gouvernementaux, universitaires et commerciaux. Un autre cas éloquent est celui du différend entre la Chine et Taiwan. La tension dans cette région a souvent enfanté des escarmouches virtuelles, et les deux adversaires ont ouvertement annoncé des plans de **cyberguerre**.

Le cyberconflit qui risque d'être le plus imposant dans les années à venir est celui qui oppose la Chine aux États-Unis. Une flambée de cyberviolence a démarré entre les deux adversaires à la suite de la collision d'un avion espion américain et d'un avion de combat chinois en avril 2001. D'avril 2001 à mai 2001, environ 360 cyberattaques lancées de part et d'autre ont été répertoriées. Depuis, la situation s'est calmée, mais des cyberagressions sont encore lancées sporadiquement, ayant pour conséquence de maintenir des tensions élevées dans le cyberspace.

À ce chapitre, l'avenir est sombre pour Internet. L'utilisation du cyberspace à des fins de violence deviendra probablement plus fréquente avec la croissance constante des utilisateurs du Web. De même, les tensions politiques régionales engendreront une croissance des cyberattaques. La dimension mondiale d'Internet fera en sorte que les conflits régionaux auront des impacts globaux, dépassant largement le cadre des frontières géographiques.

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

Illustration(s) :

AFP

Dans le camp de réfugiés Ain el-Helweh, près de la ville libanaise de Sidon, des membres du Front de libération de la Palestine se livrent à des cyberattaques contre Israël.

© 2002 La Presse. Tous droits réservés.

Numéro de document : news·20020810·LA·0028

PUBLI-C news·20020810·LA·0028

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.