L'EXPRESS .fr
TOUS LES JOURS, TOUTE L'INFO

La cyberguerre a commencé

Par De notre envoyé spécial, Guillaume Grallet, publié le 06/05/2008 - mis à jour le 06/05/2008 11:04

Attaques, contre-attaques, opérations de sabotage, espionnage qui ne dit pas son nom... Sur Internet, de nouvelles formes de conflits se développent. Une extension des champs de bataille dans le monde virtuel, que les Etats ne peuvent plus ignorer.

Le bâtiment de crépi ne paie pas de mine. Pourtant, ces deux étages ternes sont sans doute plus essentiels pour la souveraineté de l'Inde que le Taj Mahal. En haut d'un escalier en colimaçon, l'oeil est attiré par une photo jaunie, où des agents du Mossad, les services israéliens de renseignement, tout sourires, sortent d'un cours d'informatique. A l'intérieur, le ronflement des ventilateurs masque mal la chanson de Balasubramanyam, un crooner de Bollywood. Une trentaine d'ados, accrochés à leur clavier, usent de pseudonymes pour subtiliser, auprès de hackers du monde entier, les secrets d'une attaque à venir sur une compagnie aérienne locale, Kingfisher Airlines.

Bienvenue à e2Labs, la première école indienne de lutte contre la piraterie informatique, nichée à Hyderabad, dans le centre du pays. Sur deux étages d'un immeuble érigé dans les années 1950, des experts forment, depuis 2003, au rythme de 250 par an, les jamesbond.com, ceux qui devront répondre du tac au tac aux attaques en ligne. D'ores et déjà, Internet apparaît comme le nouveau champ de bataille planétaire.

DR
Dans les locaux de e2Labs, un centre de formation créé en 2003, près de 250 personnes apprennent, chaque année, à contrer les hackers. Situé à Hyderabad, e2Labs aide le gouvernement indien à se prémunir contre les attaques des pirates, de plus en plus nombreuses.

Voilà qui ne manque pas de sel. Alors que le réseau mondial a été conçu pour survivre à une attaque nucléaire, quelques malicieuses lignes de code suffiraient ainsi à transformer ce génial instrument de communication en machine à détruire? Révolue, en effet, l'ère du *script kiddie,* hacker boutonneux qui, hier, «pissait» des lignes de code, motivé uniquement par le défi intellectuel de l'exploit informatique. Aujourd'hui, le pirate, déjà doté d'un fort appétit financier, se découvre guerrier. Certes, Famas, kalachnikovs et mines antipersonnel ne sont pas près de finir au placard. Mais il faudra désormais compter avec ces fantassins des temps modernes qui, par le côté soudain, dévastateur et global de leurs attaques, obligent les gouvernants de tous les pays à revoir leur stratégie de défense.

Le Conseil de l'Europe n'a-t-il pas tenu, début avril, à Strasbourg, un colloque consacré au sujet? Dans la foulée, au sommet de Bucarest, l'Otan réclamait plus de coopération entre ses Etats membres et tirait la sonnette d'alarme. Tout comme la première puissance du monde, désemparée. «Vous n'avez besoin ni d'une armée, ni de marines, ni d'une aviation hors pair pour battre les Etats-Unis», explique le général américain William T. Lord, pour qui un ordinateur peut virtuellement être à l'origine de plusieurs 11 Septembre. Un «hacktivisme» qui, redonnant de la vigueur aux terrorismes de tout poil, secoue l'équilibre des forces en vigueur depuis la chute du mur de Berlin.

La menace était latente depuis une quinzaine d'années, mais c'est l'Estonie, modèle d'administration informatisée, qui a réveillé les états-majors.

A Berlin, un ministère reconnaît avoir été «hacké»

Fin avril 2007, alors que des employés municipaux de Tallinn déplaçaient le Soldat de bronze, monument cher au c?ur des Russes du pays, une demi-douzaine de sites estoniens ont été, à la surprise générale, mis hors d'état de marche. En quelques minutes, dans cette république où 97% des ordres bancaires sont passés en ligne, il était impossible d'accéder aux comptes de Hansabank et de SEB, les deux principaux établissements financiers du pays. Représailles des nostalgiques du communisme? Hors de lui, Urmas Paet, ministre estonien des Affaires étrangères, réclamait

sur-le-champ des excuses publiques à Moscou. Si une partie des ordinateurs incriminés semble bien avoir été envoyée par des pirates d'origine russe, le Kremlin, de son côté, a démenti toute implication.

Deux mois plus tard, au beau milieu de l'été, c'était au tour des Etats-Unis, de la France, de l'Allemagne et de la Grande-Bretagne de recevoir des «visites» inattendues, et surtout non désirées, sur leurs sites Internet. «De manière répétitive», insiste-t-on au ministère des Affaires étrangères de Berlin. Plusieurs centaines d'ordinateurs ont été mis hors d'usage. Pointé du doigt, Pékin a répliqué qu'il n'y était pour rien, rétorquant au passage que, la Chine abritant le plus grand nombre d'ordinateurs au monde, des pirates «étrangers» pouvaient en avoir pris le contrôle à son insu.

De fait, devenir cybercombattant est à la portée de tout le monde, ou presque. Avec un peu d'ingéniosité et moins de 500 euros en poche, il est possible de bloquer l'accès à un site gouvernemental durant plusieurs heures! Il suffit d'acheter des listes d'adresses e-mails, disponibles sur des forums Internet grand public, que ces derniers parlent de la mode ou de la dernière tendance gastronomique... Ces portes d'entrée offrent la possibilité à l'apprenti pirate de repérer les ordinateurs les plus fragiles, de les infecter et d'en prendre le contrôle à distance. Réitérée à l'envi, l'opération permet de disposer d'une petite armée de machines esclaves (un «botnet»). L'opération est efficace et quasiment anonyme. «C'est du billard à deux bandes: ce n'est pas vous qui attaquez, mais des ordinateurs à vos ordres», met en garde Nicolas Sadirac, directeur de l'école informatique Epitech. Mieux, les disparités légales à l'échelle de la planète protègent les malfrats. «Les Pays-Bas, qui respectent la vie privée, interdisent d'établir un lien entre une connexion et l'identité de la personne qui se connecte», explique-t-on chez Kaspersky, éditeur d'antivirus, qui distingue d'autres «cyberparadis» en Amérique latine et en Afrique. «Devenir cyberdélinquant est un jeu d'enfant, s'inquiète un expert de l'Otan. Mais peut provoquer des dégâts aussi importants que les armes conventionnelles.»

Comment s'y prennent les cybercombattants

1. Espionnage
En envoyant un virus à l'ordinateur qu'ils veulent espionner, les pirates ouvrent une porte dérobée, sorte de miroir qui va leur permettre de suivre en temps réel tout ce qui s'écrit sur l'ordinateur, y compris les mots de passe.
2. Frappe chirurgicale
Même un pacemaker peut être déréglé à distance ! Les hackers se servent de l'accès Internet pour infiltrer tous les endroits où ils veulent agir : aéroports, centrales nucléaires, banques...
3. Blocage des systèmes
Des hackers infectent des milliers d'ordinateurs avec des mails contenant un virus qui les oblige à exécuter un ordre prévu à l'avance. Tous ces ordinateurs « zombies » agissant de concert provoquent un énorme embouteillage.

Un jeu d'autant plus dangereux qu'Internet est omniprésent: c'est l'espéranto qui permet à un nombre croissant de machines de communiquer ensemble. Le moindre dysfonctionnement a des effets immédiats sur la vie réelle... Le 3 février, plusieurs dizaines de milliers de Qatariens, de Malaisiens et d'Egyptiens en ont fait l'amère découverte, eux qui, face à un écran noir, se sont tout à coup retrouvés privés d'accès à leur compte bancaire, au téléphone ou à la télévision en ligne. Un câble enfoui sous la mer avait tout simplement été sectionné. Après avoir envisagé un accident, les enquêteurs n'excluent pas aujourd'hui une piste criminelle.

Les cyberguerriers pourraient facilement paralyser un pays

Les réseaux de transport ou l'alimentation en énergie pourraient être menacés à terme», redoute Guillaume Tissier, un des responsables de la Compagnie européenne d'intelligence stratégique (CEIS), une société privée d'intelligence économique. Le 24 avril, le GovSec, une émanation du département américain de la Défense, a listé les secteurs qui seraient touchés les premiers en cas d'une attaque organisée sur Internet. Les circuits électriques, tout comme les télécoms, seraient déréglés, suivis du système bancaire et de l'approvisionnement en pétrole. Avant de parvenir à une paralysie du pays, avec des pompiers ou des chirurgiens hors d'état de travailler. Le pire devient possible. «Pourquoi ne pas envisager la perte de la mainmise sur les équipements nucléaires?» s'interroge-t-on chez l'éditeur israélien Check Point.

Nous n'en sommes - heureusement - pas là. Le quotidien de la cyberguerre consiste plutôt en une guérilla menée par des mercenaires qui jouent d'autant plus les gros bras qu'ils opèrent cachés. Un reportage de CNN sur les émeutes de Lhassa ne plaît pas? Aussitôt le site de la chaîne est brouillé, avant que des sites pro-chinois ne soient, à leur tour, pris pour cible. Radio Free Europe/Radio Liberty (RFE/KL) envisage de couvrir le 22e anniversaire de l'explosion de Tchernobyl? Son site est attaqué, rendant difficile toute écoute sur Internet durant plusieurs jours. Le président de la radio, Jeff Gedmin, compare cette cyberattaque au brouillage des fréquences à l'époque soviétique.

La cyberguerre sera nationaliste ou ne sera pas. En décembre 2001, les bureaux de comptabilité d'une grande administration indienne sont attaqués. Le groupe bien nommé Anti-India Crew poste un message sur tous les écrans d'ordinateurs: «Nous allons viser les gouvernements américain, indien et israélien, jusqu'à la paix finale!» Tout de suite, les Indiens soupçonnent un mauvais coup des Pakistanais, leurs frères ennemis. Et les Indian Snakes, hackers originaires de New Delhi, de bombarder à leur tour ces «Pakistanais trop nuls en informatique!». En plus du sens de la dérision, les pirates informatiques ont le sens de l'Histoire... Le 20 mars 2005, le site du ministère coréen des Affaires étrangères doit fermer à cause d'une attaque provenant du Japon. Les deux pays se disputent la souveraineté d'îlots situés en pleine mer. Quatre ans plus tôt, des hackers prochinois s'en étaient pris à des sites Web japonais après que le Premier ministre nippon eut rendu visite au sanctuaire nationaliste Yasukuni.

Internet ou le moyen idéal de s'inviter chez l'ennemi? Tout ce que vous dites, à l'autre bout du monde, est susceptible d'être entendu. La société Espion-on-line.com commercialise ainsi un programme ultradiscret qui, installé à distance, peut enregistrer exactement l'activité du clavier et de la souris. Les mots de passe, le nom d'utilisateur, les textes frappés... Contacté par L'Express, le dirigeant de cette firme basée à Londres explique avoir vendu l'an dernier pour plus d'un demi-million d'euros d'un tel attirail aux dirigeants d'un pays d'Asie du Sud-Est. Car le Web a des oreilles: un soldat trop disert sur le réseau d'échanges Facebook a ainsi pu être identifié, grâce à sa participation à un groupe sur le site. Des cartes ainsi que des plans d'action ont été mis à nu. Le camouflage est indispensable en ligne également.

Il existe un marché mondial des hackers

Remarquable indic autant qu'outil de propagande, Internet joue aussi les aides de camp. L'armée israélienne aurait ainsi neutralisé, l'an dernier, un radar syrien à Tall al-Abyad, juste avant de lancer une offensive sur cette zone. Durant la guerre du Kosovo, selon le CEIS, des attaques groupées avaient permis aux Serbes de causer des ralentissements dans les systèmes de l'Otan. Le virtuel ou le meilleur moyen d'influencer le réel! Et que dire de cette capacité de détraquer à distance un pacemaker, comme l'a démontré le chercheur Tadayoshi Kohno, de l'université de Washington? Les meilleurs bidouilleurs auront ainsi le droit de mort sur des dizaines de milliers de personnes.

A la différence de la guerre froide, cette nouvelle bataille des nerfs n'est pas bipolaire, offrant au contraire un porte-voix inespéré aux revendications les plus minoritaires. En Iran, plusieurs universités auraient développé un cursus afin de former des hackers de haut vol. La Corée du Nord, elle aussi, possède sa propre école de pirates: le Mirim College, dans la région de Hyungsan, d'où sortent une centaine de soldats chaque année. La Légion étrangère bientôt en ligne? «Il existe un marché mondial des hackers, recrutés au coup par coup, et qui, pour une grosse opération, peuvent toucher jusqu'à 1 million de dollars», souligne Zaki Quereshy, directeur de l'école indienne e2Labs, par ailleurs consultant pour le gouvernement indien.

DR

Situé à Tallinn, en Estonie, cible de nombreuses attaques en 2007, le centre de formation à la cyberdéfense de l'Otan ouvrira ses portes le 1er janvier 2009.

Quelle stratégie de défense adopter? «Le pire serait d'ignorer le problème parce qu'il est difficile à concevoir», reprend Guillaume Tissier du CEIS. Dans ce nouveau désordre du monde, les Etats-Unis, peut-être les plus conscients de leur retard, ont été les premiers à dégainer en créant, il y a dix-huit mois, le Cyber Command, une unité spécialisée dans les attaques Internet. Le cinquième terrain de bataille après l'air, la terre, la mer et l'espace... Et ses soldats se sont livrés, du 4 au 12 avril dernier, à des man?uvres bien spéciales. Jugez plutôt: point de nettoyage chronométré de fusil ou de lever au son du clairon, mais la recherche, et l'identification, en un temps record, de menaces issues du monde entier. Des experts de Nouvelle-Zélande, du Royaume-Uni ou encore du Canada ont participé à cette opération. De son côté, la France devrait organiser une simulation comparable, Piranet, à la fin du mois de mai, sous l'égide du Secrétariat général de la Défense nationale (SGDN).

Pendant ce temps-là, à Tallinn, la capitale de l'Estonie, c'est un blockhaus que l'on réhabilite. Une ancienne caserne, construite à l'époque de la Russie tsariste, a été transformée en centre de formation à la cyberdéfense. L'Otan a pris possession de ce bâtiment imposant, bordé de roseraies blanches et rouges taillées au millimètre, aux allures de pensionnat. Sur cette terre qui, tour à tour, a dû affronter le siège des troupes danoises, allemandes, suédoises et soviétiques, on se prépare, dès 1er janvier 2009, à répondre aux attaques de toutes sortes. De manière défensive. Enfin, pour l'instant.