«La cybersécurité est l'affaire de tous»

ATTAQUES SUR INTERNET • *Consciente de ses faiblesses, la Suisse prépare une stratégie nationale de cyberdéfense. C'est que la menace est bien réelle. Les explications de l'experte Solange Ghernaouti-Hélie.*

PROPOS RECUEILLIS PAR
PASCAL FLEURY

Ce n'est pas un secret d'Etat: en cas de cyberattaques massives, la Suisse serait bien démunie. Pour parer à tout risque de paralysie du pays, le Conseil fédéral a donné la mission au Département de la défense d'élaborer, d'ici à la fin du premier trimestre 2012, une stratégie nationale de cyberdéfense. Un groupe d'experts civils et militaires planche depuis le début de l'année sur un système de milice qui permettrait d'anticiper les dangers et de limiter les dégâts.

Tout internaute peut utiliser des programmes malveillants

SOLANGE GHERNAOUTI-HÉLIE

L'armée suisse (ici lors de l'exercice Stabilo 08) a son rôle à jouer dans une stratégie nationale de cyberdéfense. Mais selon l'experte Solange Ghernaouti-Hélie, une efficacité ne sera possible que dans une collaboration étroite avec le monde civil. KEYSTONE

Experte internationale en cybersécurité et criminalité du numérique, la professeure de l'Université de Lausanne Solange Ghernaouti-Hélie explique les enjeux de ce grand défi de société. Conférencière très sollicitée, elle est l'auteure de plus de 25 ouvrages dont «La Cybercriminalité: le visible et l'invisible» (Ed. Le Savoir suisse). Entretien.

Notre armée doit élaborer une stratégie nationale de cyberdéfense. En fait, les cyberattaques sont-elles plutôt militaires ou civiles?

Solange Ghernaouti-Hélie: A ce jour, très peu de cyberattaques relèvent d'un acte de guerre impliquant des militaires. Elles sont au service de l'économie illicite, de la délinquance et de la criminalité organisée et contribuent à tous types de trafics (drogue, êtres humains, blanchiment d'argent...). Selon un des derniers rapports de la société informatique Symantec, le marché de la cybercriminalité serait équivalent à celui du trafic mondial de drogue, soit de l'ordre de 410 milliards de dollars. Même si son origine est à trouver du côté du Département de la défense américain, internet est avant tout un espace construit par les civils pour des applications civiles. Mais désormais, ce cyberespace est également exploité par le monde militaire, qui met à profit des moyens civils pour être opérationnel.

La défense nationale contre les cyberattaques doit-elle être alors du ressort de l'armée ou de la société civile?

Même si des cyberattaques ou des défauts de sécurité informatique peuvent fragiliser les infrastructures critiques du pays, et même si des actions terroristes tirent partie d'internet, ce n'est pas pour autant que le Net doit être contrôlé par les militaires. Internet doit rester au service du développement économique et social du pays. Il ne doit pas devenir une arme de guerre! Ni un champ de bataille ou seuls les militaires auraient un certain pouvoir de contrôle et de sécurité. La défense contre les cyberattaques ne sera efficace que si elle exploite rationnellement l'ensemble des ressources disponibles en Suisse et coordonne tous les acteurs, aux niveaux cantonal et national, avec une collaboration entre les secteurs privé et public et entre les mondes civil et militaire.

Les forces de justice et police possèdent des moyens et compétences dans le domaine de la lutte contre la criminalité. Les Hautes Ecoles et les entreprises ont un savoir-faire en matière de technologie de l'information et de sécurité informatique. Les militaires, pour leur part, possèdent des moyens et compétences dans le domaine du renseignement, de la sécurité nationale ou du terrorisme. Bien sûr, pareille coordination suppose une réelle volonté de collaborer et une confiance dans les acteurs de la sécurité.

Chacun a donc un rôle à jouer dans la cybersécurité. Aussi les simples citoyens?

Oui, dans la mesure où leur ordinateur, leur comportement en ligne, leurs données livrées de leur plein gré sur des réseaux sociaux ou suite à un leurre, tout peut profiter aux pirates. Les citoyens peuvent être abusés par des messages de «phishing» et livrer sans le vouloir leurs paramètres de connexion et leurs identifiants. Ils peuvent aussi se faire voler des données sensibles. Leurs ordinateurs peuvent être infectés par un virus et devenir des machines «zombies», télécommandées par des hackers pour réaliser des cyberattaques.

Aucun Livre blanc, aucune doctrine militaire ne peut pallier le manque de responsabilité individuelle et collective de la société civile, ni le manque de partenariat efficace entre le secteur privé et le secteur public.

Quels sont les types de cyberattaques les plus menaçants pour notre pays?

Les attaques visant les systèmes informatiques qui contrôlent les infrastructures critiques pour la société et la sécurité nationale. Cela peut concerner les centrales nucléaires, les systèmes de distribution électrique ou d'eau potable, les CFF, la signalisation du réseau routier... Le plus grave serait des attaques combinées sur plusieurs infrastructures vitales ou couplées avec des attaques physiques sur des sites. L'économie de la Suisse dépendant pour beaucoup de sa place financière, des cyberattaques portant atteinte à la disponibilité, à l'intégrité, à la confidentialité des données ou des transactions financières pourraient avoir aussi des conséquences catastrophiques. De même, des défigurations de sites web ou des attaques sur des sites institutionnels pourraient avoir des incidences en termes d'image pour les personnes ou les institutions ciblées, menant à une perte de confiance et de crédibilité.

Qui sont les auteurs de ces attaques: des hackers à la solde d'Etats malveillants? Des cyberguerriers?

Attention! Dorénavant, tout internaute peut potentiellement utiliser des programmes malveillants permettant de réaliser des cyberattaques. De tels logiciels sont accessibles sur internet. Certains sont gratuits, certains à configurer, à adapter au besoin. Sur le Net, on peut louer, acheter, recruter les compétences manquantes. Une mobilisation peut être extrêmement rapide et efficace. Les internautes peuvent devenir des cyberagents au service de causes particulières.

Tous les conflits peuvent être transposés dans le cyberespace. Ils peuvent même être attisés sur internet. C'est le cas ces jours avec les revendications de citoyens et du groupe de hackers Anonymous contre la Bourse de New York. La guerre de l'information sur internet n'est pas le pré carré d'une petite partie de la population, ni réservée aux militaires. Les actions portées par le groupe Anonymous en témoignent, comme leurs slogans d'ailleurs: «Nous sommes la voix du peuple. Nous déclarons la guerre!»

Mais alors, quels pays peuvent affirmer être prêts à faire face à des cyberattaques massives?

Ceux qui peuvent démontrer qu'ils possèdent une force de frappe offensive puissante et dissuasive, mais qui peuvent aussi s'appuyer sur des alliances stratégiques entre Etats. La cybersécurité passe aujourd'hui également par la diplomatie et la coopération internationale. Une approche nationale est nécessaire mais pas suffisante car les cyberattaques peuvent être transfrontalières, transnationales. Les pays qui devraient être les mieux préparés à faire face sont ceux qui sont les plus dépendants des technologies de l'information. I

LA SEMAINE PROCHAINE

LE DOSSIER BERLUSCONI

Silvio Berlusconi, après une longue carrière d'entrepreneur et de politicien, demeure un mystère. Son ascension fulgurante et son long maintien au pouvoir, malgré les scandales, ses ennuis judiciaires et ses liens suspects, continuent d'intriguer. Le témoignage de Licio Gelli, ex-chef de la loge P2, révèle en particulier comment cette organisation secrète d'extrême-droite a misé sur ce politicien pour s'assurer une emprise durable sur tous les rouages de la société italienne.

La guerre numérique a déjà commencé

Les risques de «cyberguerre» sont exagérés, affirme l'Organisation de coopération et de développement économiques[1]. L'OCDE juge faible la probabilité d'un cyberconflit à grande échelle entre deux pays. Elle note toutefois que les Etats doivent se tenir prêts à se protéger des attaques informatiques, qui pourraient être utilisées en tant qu'armes complémentaires lors d'une offensive classique.

C'est que de telles attaques ont déjà fait leurs preuves. Sur le plan international, on peut citer l'attaque en règle contre l'Estonie, menée en avril 2007 par des hackers, vraisemblablement à la solde du Kremlin. En mesure de rétorsion contre le déboulonnage d'une ancienne statue soviétique, à Tallin, de nombreux sites web gouvernementaux et bancaires ont été paralysés par des envois massifs de messages.

Un an plus tard, c'est en Géorgie que des sites internet de l'Etat ont été bloqués, juste au moment où l'armée russe lançait son offensive terrestre. Les pirates ont même remplacé la page d'accueil du Ministère des affaires étrangères par des photos mettant en parallèle le président géorgien et Hitler. Pareille désinformation a aussi été pratiquée lors de l'opération «Plomb durci» contre les Palestiniens, fin 2008. Les Israéliens ont piraté la chaîne TV Al Aqsa pour diffuser une vidéo ciblant les responsables palestiniens avec le message «Le temps vous est compté».

Les cyberattaques peuvent aussi avoir des objectifs militaires. En 2007, l'armée israélienne a réussi à s'introduire dans les ordinateurs contrôlant les radars syriens de surveillance aérienne pour les réorienter et dégager ainsi un corridor non protégé. Israël a alors pu lancer une attaque aérienne en Syrie et détruire une usine suspectée de produire des missiles nucléaires.

L'espionnage se trouve également au cœur de la guerre numérique. Souvent montrée du doigt, la Chine surveillait un millier d'ordinateurs d'organisations de défense du Tibet. Des PC gouvernementaux américains ont aussi été espionnés.

S'agissant de sabotage d'infrastuctures civiles, plusieurs cas ont été rencensés. Aux Etats-Unis, au moins deux centrales nucléaires ont dû être momentanément arrêtées à la suite de cyberattaques. Les Américains auraient même découvert des «bombes logiques» chinoises dans leur réseau électrique. Ces virus informatiques dormants auraient été capables de sabotage à distance. En Amérique du Sud, des réseaux électriques ont été coupés en échange de rançons.

La plus impressionnante attaque numérique réalisée à ce jour reste celle du ver informatique Stuxnet contre l'usine nucléaire iranienne de Natanz, en 2010. Le virus sophistiqué, vraisemblablement d'origine israélienne ou américaine, a d'abord contaminé des milliers d'ordinateurs autour de la centrale, en exploitant les failles de Microsoft. Il a suffi alors qu'un employé peu regardant insère une clé USB infectée dans le réseau sécurisé de l'usine pour que Stuxnet se glisse peu à peu jusqu'aux centrifugeuses destinées à la concentration de l'uranium. Les mettant en panne en série, il a retardé durablement le programme nucléaire iranien. PFY

Le président iranien Ahmadinejad lors d'une visite de l'usine d'enrichissement de l'uranium de Natanz, où des centrifugeuses ont été détruites par un virus. KEYSTONE

[1] «Reducing Systemic Cybersecurity Risk», OCDE, 2011. Voir aussi le documentaire «La guerre invisible», d'Antoine Vitkine, dimanche sur TSR2.