

La cyber-sécurité

C'était le thème du 7^e Forum Sécurité Chablais 2013 organisé par l'Académie du Chablais et le Centre de formation du Chablais

TEXTE: JEAN-DANIEL FAVRE; PHOTOS: POLICE CANTONALE VS

Beaucoup de monde avait fait le déplacement de Champéry le 6 septembre dernier, dont une délégation de la gendarmerie nationale française de la région Franche-Comté. Grande première pour cette conférence: une diffusion en direct sur le réseau internet.

Cyber?

Mais que veut dire «cyber»? On a appris que ce mot provient de «cybernétique», formé en français à partir du grec *Kubernètikè* en 1834 déjà. A cette époque, il désignait la science du gouvernement. En 1948, un Américain a repris ce terme pour parler de la science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication entre l'être vivant et la machine, la *cybernétique* précisément. Par extension, on a le cyber-espace, soit l'ensemble des données réalisables par des logiciels informatiques. Par extension aussi, ont découlé la cyber-attaque, la cyber-criminalité la cyber-menace, etc. et la cyber-sécurité.

Comme l'a précisé M^{me} Solange Ghernaouti-Hélie, de l'Université de Lausanne, une des conférencières du jour, «certains acteurs à la recherche de profit et/ou de pouvoir ont accaparé Internet et le cyber-espace pour atteindre leurs objectifs, induisant des conséquences préjudiciables tant pour les individus, les organisations que pour les Etats».

Que fait la police?

Le moins que l'on puisse dire après avoir entendu les conférenciers est que la société en général n'est pas prête à faire face à la cyber-criminalité. L'informatique est devenue indispensable mais elle véhicule aussi des risques encore trop méconnus. Le secret numérique n'existe pas et il faut prendre des mesures sans tarder car il serait naïf d'attendre. Les premières menaces viennent de l'environnement proche, pas des Etats-Unis ou de Chine.

La police n'est pas prête à faire face à ce genre de délits car elle est non seulement mal outillée, mais en plus elle est bridée par les textes légaux et par la hauteur des coûts de la procédure facturés par les grands opérateurs comme SWISSCOM par exemple. En revanche, il est facile de faire l'espion pour un simple pékin. Les appareils ne coûtent pas cher et peuvent être acquis et utilisés très simplement.



Colonel Alain Sevilla, Cdt en second de la région de gendarmerie de Franche-Comté.

Et chez les privés?

En revanche, le monde privé connaît ce nouveau danger et certaines entreprises ont pris les mesures nécessaires pour y parer.

M. André Kudelski, de la maison du même nom, a souligné quelques points:

- > les nouvelles technologies servent à tous, pirates compris
- > les Etats connaissent des frontières et un cadre légal, les pirates non
- > les Etats et leur police sont lents à la réaction, les pirates non. Ils sont rapides et s'adaptent très vite
- > tous consommateurs mais aussi tous potentiellement pirates ou victimes

Depuis 25 ans la maison Kudelski poursuit la piraterie informatique et développe de nouvelles technologies de sécurité. Mais cela n'a pas de fin. Depuis 15 ans, elle collabore avec des polices et des magistrats du monde entier, mais on ne nous en a pas dit le coût ...



M^{me} Solange Ghernaouti-Hélie, depuis le 1^{er} janvier 2014, chevalier de l'ordre français de la Légion d'honneur.

8^e Forum

Le colonel Bergonzoli l'a annoncé: il y aura bien un 8^e Forum en 2014 mais il se fera sans la collaboration du Centre de formation du Chablais, c'est-à-dire sans la participation de l'armée.

Cadre légal déficient

La Suisse est une cible prioritaire de la cyber-criminalité mais on n'a pas conscience du risque économique encouru.

M. le procureur Jean Treccani du canton de Vaud a souligné les faiblesses légales du code pénal pour lutter contre ce phénomène. Des attaques graves et répétées sont qualifiées de contraventions par le CPS. Comme il s'agit très souvent de délits commis à l'échelle de la planète, il doit recourir à la collaboration internationale pour faire avancer ses enquêtes. Le magistrat a assuré qu'il faisait rire de lui et de la procédure suisse au vu des peines encourues par les cyber-criminels ... Mais c'est une constatation mondiale, globalisée pourrait-on dire: les profits criminels sont importants et le risque pénal encouru relativement faible.

«Les premières menaces viennent de l'environnement proche.»

La balle est dans le camp de la Confédération

Il est ressorti qu'il manque en Suisse une volonté forte à Berne pour lutter contre ces pratiques frauduleuses. On se sent démuni par exemple face aux autorités des Etats-Unis d'Amérique qui ne veulent pas répondre aux demandes qui leur sont envoyées. Certains ont avancé l'idée de menacer de couper «gmail» pour être entendus ...

Il faut que la Berne fédérale prenne ses responsabilités d'autant plus qu'il s'agit d'un problème qui doit se résoudre à l'échelon mondial. Il faut décloisonner les esprits en ce sens. Plusieurs acteurs sont concernés, dont la police et l'armée ce qui a fait ressurgir l'idée d'un département fédéral de la sécurité, mieux à même de centraliser les questions et d'y donner des réponses. Car si l'on pense que cinq départements fédéraux gèrent des problèmes ayant trait à la sécurité, à quoi s'ajoutent des polices cantonales et communales, si l'on réfléchit à la peine que tous ces organismes ont pour se coordonner, pour réagir et pour agir ensemble, on imagine sans problème toute la latitude qui est laissée aux cyber-criminels ...

A Berne encore, il faudrait modifier le code pénal de façon à pouvoir punir plus sévèrement les cyber-criminels. Les policiers le savent, il faut du temps et de la patience, beaucoup de patience entre le constat d'un problème légal à résoudre et sa résolution.

On l'a lu plus avant, la lutte contre la cyber-criminalité a un coût. La Confédération n'a pas alloué de budget permettant ce combat et il manque de nombreux spécialistes en la matière.

Que font-ils en France voisine?

Nos voisins français, avec leur organisation étatique très centralisée, ont pris conscience qu'il s'agit d'un problème planétaire mais les autorités en charge de la cybersécurité estiment que les entreprises françaises sont mal protégées, seules les plus mondialisées sont à peu près armées. Plusieurs soucis: l'imagination des criminels semble sans limite et beaucoup de difficultés à identifier le délinquant: ingénieur modèle le jour, il peut devenir un pirate le soir, voire un militant nationaliste la nuit.

Des chiffres ont été donnés (Le Figaro du 27 septembre 2013): en France, il y a un nouveau virus toutes les 15 secondes, 25% des attaques ciblées causent un préjudice, 250 000 débits frauduleux à la carte bancaire sur Internet par an, 100 000 dollars US par jour, soit le montant des recettes pour le seul virus *zeroAccess* et 2,8 millions d'euros, à savoir le coût moyen pour une entreprise d'un vol de données réussi par des hackers. Ajoutez encore à ces chiffres une petite particularité: depuis 2011, les agents sont invités à ne plus enregistrer les escroqueries sur Internet car il n'y a pas eu dépossession physique de la carte et les banques finiront bien par rembourser. De ce fait, le nombre des délits (annoncés) a passé de 37 357 en 2009 à 29 796 en 2012 ...

Et maintenant, que va-t-il se passer?

En guise de conclusion, la cyber-criminalité est un problème sous-estimé et il ne s'agit pas d'une mode passagère. Un premier combat à gagner est celui de la prise de conscience du risque. Gageons que ce 7^e Forum aura permis d'avancer dans ce but. Il faut aussi lever deux tabous:

«Pour un simple citoyen, il est facile et pas cher de faire l'espion.»

- > L'Etat est protecteur des droits mais aussi des biens
- > Il faut définir la limite entre ce qui est de l'ordre public et l'ordre privé

Et le mot de la fin à M^{me} Ghernaouti-Hélie: «Ces nouveaux risques nous obligent à réinventer la sécurité afin de les maîtriser au mieux et préserver nos valeurs mises en danger par la technologisation de la société.» ■