« La cybercriminalité est la nouvelle menace du XXIe siècle »

Commissaire de police depuis 1976, Mireille Ballestrazzi s'impose, à 61 ans, comme la deuxième femme à occuper le prestigieux poste de directrice générale de la Police judiciaire. Également présidente du comité exécutif d'Interpol, le réseau international des polices, elle décrypte pour La Tribune comment les forces de l'ordre françaises, européennes et internationales luttent contre la cybercriminalité. Elle revient aussi sur les missions du tout nouveau Complexe mondial Interpol pour l'innovation de Singapour, une forteresse high-tech consacrée à la lutte contre les cybermenaces.

À l'heure où Internet s'immisce partout, y compris dans nos objets connectés du quotidien, et que le Dark Web monte en puissance, la cybercriminalité s'impose comme « la menace du XXIe siècle » et pose un défi d'une ampleur inégalée aux forces de police.

LA TRIBUNE - Avec la numérisation de la société et de l'économie et le développement des nouvelles technologies, les crimes et délits se multiplient dans le cyberespace. Comment les forces de police abordent-elles cette problématique?

MIREILLE BALLESTRAZZI - La cybercriminalité est clairement la nouvelle menace du xxie siècle. Elle force les polices à repenser leurs moyens d'action, à se mettre au niveau techniquement et à développer des outils transnationaux, car l'échelle devient mondiale. Le cybercrime est d'autant plus difficile à appréhender qu'il prend des formes diverses et n'a, par définition, pas de frontières. Il peut s'agir d'apologie du terrorisme, de réseaux de pédopornographie ou de proxénétisme, ou encore d'attaques contre des systèmes de données, comme celle qu'a connue récemment

TV5 Monde. Internet donne aussi aux malfaiteurs un nouveau terrain de jeu pour mettre en place des escroqueries comme la fraude à l'e-paiement, le blanchiment d'argent ou le trafic de stupéfiants. Le cyberespace permet l'expression de menaces inédites par l'utilisation des nouvelles technologies, mais il étend aussi le périmètre des crimes « classiques ». Avec la démocratisation de l'accès à Internet et l'innovation constante autour des nouvelles technologies, la cybercriminalité devient un enjeu de société, à la fois pour les gouvernements, les entreprises et les citoyens. Et ce n'est que le début : toutes les études tablent sur une augmentation significative du nombre de crimes liés à Internet dans les années et décennies à venir. Il s'agit d'un vrai défi pour les États et les polices du monde entier.

En tant que présidente du comité exécutif d'Interpol, vous avez inauguré, en avril dernier, le Complexe mondial pour l'innovation, situé à Singapour et spécialisé dans la lutte contre la cybercriminalité. C'est l'outil qui manquait pour être à la hauteur de l'enjeu ?

Il est essentiel que la police tente d'avoir une longueur d'avance sur les malfaiteurs. Lutter efficacement contre le crime en général et contre la cybercriminalité en particulier demande la mise en place d'outils globaux. Interpol, dont le siège est à Lyon, remplit déjà cette mission. Il dispose de bases de données massives, sur la pédopornographie par exemple, alimentées par l'ensemble des polices du monde. En revanche, les crimes sur Internet nécessitent une attention particulière. C'est pourquoi les 190 membres d'Interpol ont accepté à une quasi-unanimité l'ouverture de cette nouvelle structure à Singapour. Le Complexe mondial transcende le modèle traditionnel répressif en matière d'application de la loi, en utilisant toutes les possibilités de l'ère numérique.

Quelles sont ses missions ?

C'est un centre ultramoderne, doté d'ordinateurs de grande capacité. Le choix s'est porté sur Singapour, car Lyon n'avait pas la place pour l'accueillir. Il dispose d'experts et d'équipements à la pointe du progrès, au service de deux grandes missions. D'abord, la recherche autour du développement des nouvelles technologies par les criminels, de manière à fournir aux services de police des outils de riposte adaptés. Ensuite, le Complexe fournit une aide aux enquêteurs du monde entier, via des formations, des échanges d'informations et un renforcement des capacités d'intervention. Il travaille aussi avec d'autres organismes transnationaux comme Europol, le réseau des polices des pays de l'UE. Actuellement, le centre compte 95 personnes, mais l'effectif va monter en puissance pour atteindre 160 employés d'ici à 2018-2019.

Concrètement, comment se passe la collaboration internationale pour lutter contre une cybermenace ?

Prenons l'exemple de la pédopornographie, qui prospère sur Internet. Il existe des sites d'une horreur absolue. Grâce à sa base de données, Interpol peut découvrir un réseau. Mais souvent, l'initiative part d'un pays membre, qui identifie un certain nombre d'adresses IP problématiques et ouvre une enquête judiciaire. Internet étant mondial, les adresses IP concernent souvent plusieurs États. Interpol contacte alors le bureau central d'Interpol dans chaque pays concerné pour mettre en place une coopération internationale. Celle-ci permet de partager les informations et de mener des actions simultanées comme l'arrestation, au même moment et dans plusieurs pays, de plusieurs organisateurs d'un réseau pédopornographique. Il arrive très régulièrement que la police française ou la gendarmerie participe à ce genre d'opérations. De même, la police judiciaire est en lien direct avec Singapour via un commissaire de police qui y est détaché. Nous collaborons aussi avec EC3, la plateforme d'Europol vouée à la cybercriminalité. L'objectif de toutes ces structures est d'être plus efficace sur le terrain mais aussi d'éviter les doublons, car lutter

contre la cybercriminalité coûte très cher. Pourquoi faire enquêter plusieurs équipes, séparément, dans différents pays, quand on peut avoir une vision d'ensemble ?

Comment prenez-vous en compte le Dark Web, les tréfonds d'Internet, véritable repère de cybercriminels ?
Mireille Ballestrazzi occupe la fonction de directrice centrale de la police judiciaire et préside le comité exécutif d'Interpol depuis novembre 2012. © Fournis par La Tribune Mireille Ballestrazzi occupe la fonction de directrice centrale de la police judiciaire et préside le comité exécutif d'Interpol depuis novembre 2012.

Nous sommes démunis face au Dark Web. La quasi-totalité de nos actions se concentrent sur le Web ouvert, qui est déjà très large. Le Dark Web est un vrai problème, car les malfaiteurs les plus pointus techniquement l'utilisent de plus en plus pour des actions liées au terrorisme, aux trafics de stupéfiants ou au blanchiment d'argent. Nous sommes démunis, car nous n'avons pas assez d'outils pour l'explorer. Par définition, on ignore ce qui se passe sur le Dark Web, donc il est très difficile de le combattre. Nous échangeons régulièrement avec le FBI pour mesurer la menace du Dark Web et pour mettre au point des outils technologiques qui nous permettront d'identifier les malfaiteurs qui y opèrent.

Quels sont les pays les plus ciblés par les cyberattaques et ceux qui produisent le plus de cybercriminels ?

En volume, l'essentiel de notre action porte sur les escroqueries et les fraudes. Les pays les plus riches sont, logiquement, les plus ciblés par les cybercriminels. Ils en produisent aussi beaucoup, même si les malfaiteurs peuvent provenir de toutes les régions du monde, y compris de pays qui sont moins attaqués, comme l'Afrique de l'Ouest. La filière nigériane, notamment, fournit beaucoup de pirates numériques qui agissent partout.

L'État français a-t-il pris la mesure des enjeux autour de la cybercriminalité ?

Avec les États-Unis et l'Allemagne, la France est l'un des pays précurseurs dans la lutte contre la cybercriminalité. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a été créé en 2001 par le ministère de l'Intérieur. C'est l'une des premières structures au monde. Sa création, qui remonte à avant même le 11-septembre, a fait office de déclic pour mettre en place un vaste réseau international qui garantisse une réponse coordonnée face aux cybermenaces. La France est régulièrement citée en exemple, notamment en Europe, car elle a des enquêteurs d'excellent niveau, spécialisés en criminalité informatique. Ce n'est pas non plus un hasard si le siège d'Interpol se situe à Lyon. À titre de comparaison, la plateforme européenne Europol a vu le jour il y a seulement deux ans.

Comment s'organise la lutte contre la cybercriminalité en France ?

L'action est coordonnée par le ministère de l'Intérieur, où travaille un « Monsieur cybercriminalité », Jean-Yves Latournerie, dont le rôle est de coordonner les différents services. La police et la gendarmerie ont chacune des enquêteurs spécialisés. La police judiciaire dispose aussi d'une division spéciale, la Sous-direction de lutte contre la cybercriminalité (SDLC). Depuis avril 2014, elle remplace et étend l'action de l'Office, créé en 2001. Quatre-vingts policiers et gendarmes de haut niveau y travaillent pour identifier et anticiper les cybermenaces. L'une de leurs missions est de surveiller le Web. C'est un travail extrêmement difficile, moralement, psychologiquement, notamment pour les agents qui effectuent la veille au sujet de la pédopornographie. Globalement, le champ d'action de la SDLC est plus large que celui de l'Office. Elle prend aussi en compte les attaques subies par les entreprises et les particuliers. Auparavant, les PME dont les systèmes

informatiques étaient attaqués, par exemple, ne savaient pas vers qui se tourner, car les policiers de base n'ont pas forcément la connaissance suffisante pour traiter ce genre de plainte. La SDLC va alors conseiller les victimes qui se tournent vers elle, mais aussi les policiers, pour leur indiquer les questions qu'ils doivent poser et ce qu'il faut mentionner dans la plainte.

Les policiers de base reçoivent-ils une formation pour comprendre les nouveaux enjeux liés à Internet ?

Nous avons un budget consacré à la formation initiale. De nos jours, il est indispensable que chaque policier ait un minimum de connaissances sur ce qu'est Internet, comment fonctionnent les réseaux sociaux, qui sont les grands opérateurs, ce qu'est la cybercriminalité... De nombreux adolescents sont victimes d'arnaques ou d'agressions sur les réseaux sociaux, et de plus en plus de personnes subissent des fraudes sur Internet, liées notamment à l'e-commerce. Si tous les policiers maîtrisent le b.a.-ba d'Internet, ils sauront mieux réagir et aiguiller les victimes. Pour l'heure, ce n'est pas suffisant mais cela va venir. Nous n'avons jamais assez de moyens, mais la France fait partie des pays les mieux dotés au monde.

Une harmonisation des lois et des pratiques au niveau européen est-elle possible?

Des discussions sont toujours en cours, cela avance doucement. Il est clair que l'échelle nationale n'est pas suffisante, il faut agir au niveau européen et mondial. Nous souhaitons que la Convention de Budapest, rédigée par le Conseil de l'Europe en 2005, soit transposée au niveau mondial. Il s'agit du premier traité définissant les grands principes de la cybercriminalité. Il tente aussi d'harmoniser certaines lois nationales pour améliorer les techniques d'enquêtes en augmentant la coopération entre les nations. C'est un combat de longue haleine, car les pays n'ont pas

tous la même vision de ce qu'est la cybercriminalité et comment il faut la traiter. Il est important de s'organiser, car ce n'est que le début. On entre dans un monde connecté.

Demain, il y aura des voitures sans conducteur, par exemple. Cela soulève des questions sur les moyens de prévention et de riposte contre les pirates numériques. Nous sommes dans une course-poursuite permanente pour nous mettre au niveau des cybercriminels, anticiper leurs attaques et utiliser la technologie contre eux. Plus les nouvelles technologies entrent dans notre quotidien, plus les possibilités d'infractions sont grandes, et plus la lutte contre les attaques est complexe.

Source :

http://www.msn.com/fr-ch/actualite/monde/%C2%AB-la-cybercriminalit%C3%A9-est-la-nouvelle-menace-du-xxie-si%C3%A8cle-%C2%BB/ar-AAdvDCy

Info pratique : Attitude à adopter en cas de réception d'un e-mail étrange voire douteux :

http://www.lenetexpert.fr/info-pratique-attitude-adopter-en-cas-reception-dun-e-mail-etrange-voire-douteux/

Signaler des faits relatifs à la cybercriminalité.

http://www.commentcamarche.net/faq/25868-signaler-des-faits-relatifs-a-la-cybercriminalite

http://www.police-nationale.interieur.gouv.fr/Infos-du-site/Nous-contacter

http://www.undernews.fr/culture-web-emploi/decouverte-oclctic-brigade-lutte-cybercriminalite-fraude-informatique.html

http://www.police.be/fed/fr/a-propos/directions-centrales/federal-computer-crime-unit

http://www.sq.gouv.qc.ca/cybercriminalite/cybercriminalite-surete-du-quebec.jsp

http://cybercrime.interieur.gouv.ci/