Catherine Chambon

Focus sur la cybercriminalité

Interviewée juste avant les attentats de janvier dernier, Catherine Chambon, commissaire divisionnaire, nous expose la nouvelle orientation sur la lutte contre la cybercriminalité impulsée par le ministère de l'Intérieur. Arrivé à la conclusion que la répression seule ne peut pas constituer une réponse suffisante à ce phénomène en pleine croissance, il a décidé de mettre l'accent sur la prévention, l'anticipation, l'information de tous les acteurs concernés que ce soient les forces de l'ordre, les entreprises ou le grand public. Cela s'est traduit par la création, en avril dernier, de la sous-direction de la lutte contre la cybercriminalité, dont Catherine Chambon a pris la tête.

Sylvie Rozenfeld : Lors de sa publication, le 30 juin dernier, le rapport du procureur Marc Robert avait mis en lumière la nécessité de mieux définir, connaître et prévenir la cybercriminalité, avec une meilleure coordination des acteurs. Ce rapport qui avait été finalisé bien avant sa publication officielle a semble-t-il inspiré le ministère de l'Intérieur qui a créé la sous-direction de la lutte contre la cybercriminalité de la Direction nationale de la police judiciaire (DNPJ). Pourquoi cette sous-direction ?

Catherine Chambon : La sous-direction spécialisée dans la lutte contre la cybercriminalité (SDLC) a été créée par arrêté du 29 avril 2014 pour adapter le dispositif du ministère de l'Intérieur à la généralisation de l'utilisation des nouvelles technologies dans la commission des infractions et pour accentuer la cohérence des actions de prévention à l'égard du grand public et des entreprises. Cette création exprime la volonté du ministère d'adapter le dispositif national opérationnel. Elle fait écho aux réflexions en Europe, au niveau international mais aussi national sur les actions à mener, la manière d'appréhender cette nouvelle forme de criminalité et de la combattre. En 2014, Interpol a créé un complexe mondial de l'innovation et Europol le EC3 (European Cybercrime Center). Parallèlement, la DCPJ (Direction centrale de la police judiciaire) a mené une réflexion visant à la modernisation de ses missions et de ses structures à l'horizon 2025, afin de préparer et anticiper les évolutions dans tous les domaines de la lutte contre la criminalité organisée, dont la cybercriminalité.

« Nous servir du creuset que représentent l'Office et les autres services d'enquêtes pour en tirer des analyses très recoupées et produire des résultats auprès des entreprises, du public pour qu'ils s'en imprègnent et mettent en place des mesures adaptées »

En raison de son ampleur, de la globalisation et de sa vitesse ?

Effectivement, la nuisance de la cybercriminalité s'étend et s'accentue, les cybercriminels se spécialisent. Le volet de la prévention s'impose encore davantage pour la protection du tissu économique national notamment.

C'est une des raisons d'exister de cette sous-direction. L'autre objectif est d'améliorer la communication entre les services de police, de gendarmerie, de sécurité intérieure de manière générale et les acteurs de lutte contre la cybercriminalité, que ce soient des services opérationnels ou pas. Au sein de la sous-direction, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), organe à vocation interministérielle, occupe une place essentielle. Il faut aussi aider les entreprises, en prenant en compte la question de la sécurité économique, mais aussi inciter les particuliers à se prémunir contre les risques, à être pro-actifs et à devenir les acteurs de leur propre sécurité.

L'Office n'a-t-il pas toujours pratiqué la prévention et de la formation ?

C'est exact et c'est sur cette expérience qu'il convient d'optimiser le dispositif. Nous devons nous servir de ce creuset que représentent l'Office et les autres services d'enquêtes pour en tirer des analyses très recoupées et produire des résultats auprès des entreprises, du public pour qu'ils s'en imprègnent et mettent en place des mesures adaptées. Les mesures encouragées institutionnellement pour les PME sont essentiellement celles préconisées par l'Anssi. Mais elles ne sont pas suffisamment connues des chefs d'entreprise et notamment ceux des PME. Une partie du public est ignorante ou mal informée de l'existence de l'outil de l'Etat. L'Anssi prodigue des conseils sur les règles d'hygiène, mais quelles sont les attentes d'un petit chef d'entreprise, en termes de sécurité, d'accompagnement, de prise en compte de l'impact sur son fonctionnement ?

C'est la mission confiée à la division de l'anticipation et de l'analyse, au sein de la sous-direction. Elle a vocation à créer cette interface complémentaire avec le grand public et les entreprises. Dans un premier temps, une étude poussée de l'expression de besoins doit être menée et dans un second temps la définition des moyens à mettre en œuvre. Les méthodes de sensibilisation d'un représentant d'une société du CAC 40, d'un artisan ou d'une petite SA diffèrent et doivent être adaptées. L'étude des affaires complexes ou novatrices participe de l'élaboration efficace de contre-mesures à destination des victimes et se décline en une information sur les risques potentiels auxquels sont exposées les entreprises, des conseils en termes d'accompagnement technique, des liens vers des sites officiels, comme la fourniture d'outils simples afin de faire un mini-audit de leur système, résoudre un problème concret, etc.

Dans un premier stade, il s'agit de permettre à l'entreprise d'être vigilante aux risques qu'elle peut rencontrer. Dans un second, elle doit identifier ses risques et la manière de répondre grâce à des méthodes, des procédures internes et la mise en place de mesures de sécurité adaptées à l'analyse de la valeur de son patrimoine immatériel. N'oublions pas que la base de données des clients est un élément essentiel de l'entreprise, tout comme les brevets, le savoir-faire, le planning, etc. Le

dirigeant n'est pas toujours conscient que tous ces éléments doivent être sécurisés. S'il ne le fait pas, il risque de tout perdre. Certes, des polices d'assurance garantissent les pertes d'exploitation, mais elles ne remplacent pas ce qui est perdu. L'utilisation qui en est faite peut être féroce et l'image de l'entreprise peut être très endommagée. Les grandes entreprises en sont très conscientes, les petites ne le sont pas suffisamment encore.

Voilà le dispositif d'accompagnement de la division d'anticipation et d'analyse qui sera mis en place en 2015. Toutes les entreprises ne disposent pas d'un CERT. Sans prétendre à créer une structure telle dans l'immédiat, la priorité est axée sur l'élaboration d'un portail qui mettra à disposition toutes les informations utiles pour les entreprises et le grand public, à partir d'une adresse étatique. Le fonctionnement de la plateforme Pharos est un exemple concret (www.internet-signalement.gouv.fr). Il s'agit d'un point d'entrée unique qui a vocation à redistribuer l'information, après l'avoir analysée.

Qu'est-ce qu'un chef d'entreprise a besoin de savoir ?
Il a besoin de savoir ce qu'il possède de précieux, à quoi il doit faire attention, connaître les modèles qu'il peut mettre en place pour assurer un contrôle managérial de la formation, l'attitude à avoir vis-à-vis des employés, notamment par rapport aux réseaux sociaux, etc. Le chef d'entreprise du XXIème siècle doit identifier le patrimoine immatériel de son entreprise et en connaître la valeur.

Et la deuxième étape ?
Elle sera beaucoup plus lourde à mettre en place et ne le sera pas avant 2016. La première étape sera l'ouverture d'un portail internet. L'objectif est de fédérer, d'organiser ce qui existe, de préparer du contenu avec des capacités de mise à jour pour rester pertinent, suivre l'évolution législative, celle des directives européennes, etc. Ce sont des projets de fond.

« Pharos qui est un outil de connaissance des infractions extrêmement riche qu'il va falloir approfondir »

Allons-nous enfin avoir des statistiques fiables sur la cybercriminalité ?
C'est un axe stratégique confié au préfet chargé des cyber-menaces, nommé en décembre 2014 auprès du ministre de l'Intérieur. En 2015, un travail va être mené par le service central statistique ministériel de la sécurité intérieure, qui a été mis en place en septembre dernier auprès du directeur de la police judiciaire.

Ce service va professionnaliser la démarche et surtout la faire évoluer complètement. L'outil statistique créé il y a une trentaine d'années n'est plus suffisamment fin pour isoler de grandes tendances.

Pouvez-vous nous donner des exemples ?
Les fraudes aux cartes de paiement, par exemple, correspondent selon les infractions à plusieurs index. La mise en relation de ces données avec les statistiques produites par l'Observatoire des fraudes aux moyens de paiement sur des définitions comparables, améliorerait la connaissance des services et faciliterait le pilotage des politiques de lutte contre ces infractions. Cela permet d'étudier la pertinence d'un outil juridique ou d'un autre, mais aussi l'efficacité des services. La cybercriminalité, les atteintes aux systèmes automatisés de données entrent dans l'index 107, qui comporte beaucoup d'infractions.
La cybercriminalité s'insinue dans toutes les infractions. Cela ne veut pas dire que l'infraction se commet par la voie numérique, mais la notion de cyber apparaît fréquemment. L'outil statistique va s'améliorer puisque nous travaillons sur des agrégats qui vont être pris en compte par le service statistique ministériel. Des agrégats sont élaborés en collaboration avec le SSMSI (Service statistique ministériel de la sécurité intérieure) pour donner de la lisibilité à un domaine en pleine mutation.

Qu'est-ce que vous attendez de ce travail statistique ?
Cela va nous donner les tendances de la cybercriminalité au niveau national, quel que ce soit le service saisi, et nous allons pouvoir les mettre en corrélation avec deux autres problématiques d'enquêtes de victimation que mène l'ONDRP (Observatoire national de la délinquance et de la réponse pénale).

Qu'entendez-vous par victimation ?
Sur une thématique donnée, l'Observatoire réalise des enquêtes de victimation. Elle consiste à solliciter des victimes d'infractions, à connaître le mode opératoire utilisé, leur ressenti et leur action après les faits. Est-ce que la personne a fait un signalement, un dépôt de plainte, victime ou pas ? Cela permet de savoir comment le public perçoit cette problématique. Par ailleurs, il y a Pharos qui est un outil de connaissance des infractions extrêmement riche qu'il va falloir approfondir. C'est la source d'information la plus fine dont on dispose. 3 000 signalements sont ainsi déposés par semaine par les internautes sur des contenus illicites de l'internet. En 2009, 59 000 signalements ont été formulés, et 137 000 en 2014. 56 % ont trait à des escroqueries commises sur internet. Enfin dernière chose intéressante à mettre en rapport dans une statistique institutionnelle, ce sont les analyses des entreprises de sécurité ou éditrice de solutions anti-virus qui ont une autre vision du phénomène. Elles voient, à partir de leur base clients, la propagation des risques. L'interaction des différents outils statistiques et le

croisement entre les différentes sources de données seront un atout essentiel à l'adaptation des axes stratégiques du ministère de l'Intérieur dans la lutte contre la cybercriminalité. Cela va nous donner un outil de pilotage très intéressant et nous permettre d'adapter nos réponses, d'anticiper.

J'imagine que vous avez des échanges avec vos homologues étrangers pour nourrir votre connaissance du phénomène.
Tout d'abord, il convient de préciser que l'OCLCTIC est le point de contact national pour Interpol, le G7 et dans le cadre de la convention de Budapest. Europol et Interpol sont des acteurs majeurs de la lutte contre la cybercriminalité. EC3 (Centre européen de lutte contre la cybercriminalité) a été créé en 2013 et en un an, a réalisé un travail très intéressant de rapprochement des équipes. Le J-CAT (Joint Cybercrime Action Taskforce) est une émanation de l'EC3, qui travaille sur des cas précis et qui permet de coordonner des actions au niveau international. Les faits pouvant se produire en différents points de la planète, le J-CAT nous permet d'agir de manière synchronisée sur plusieurs Etats. Par exemple, dans le cas de la Silk Road. Lors de la dernière affaire pilotée par le J-CAT, 400 nœuds Tor ont été démontés simultanément.

Ainsi, l'interpellation simultanée des suspects, le croisement des analyses techniques pour déterminer la nouveauté d'un phénomène ou l'existence d'un variante participent de l'efficacité du JCAT. Toutes ces analyses sont rapprochées, croisées, de manière à produire une information très fiable. Ces données sont traitées et redistribuées en interne pour éclairer la façon d'enquêter, d'analyser les disques durs, de prévenir la commission des infractions. On peut ainsi répercuter cette information technique à ceux qui en ont besoin, les entreprises ou les particuliers.

« L'arsenal législatif national est efficace à ce stade et évolue pour s'adapter aux défis de la cybercriminalité »

Considérez-vous qu'aujourd'hui vous disposez d'un arsenal légal suffisant ?
L'arsenal législatif national est efficace à ce stade et évolue pour s'adapter aux défis de la cybercriminalité. La loi du 13 novembre 2014 a ainsi étendu les capacités d'enquêtes sur internet et permet le blocage administratif des sites pédopornographiques ou faisant l'apologie du terrorisme. Le droit international doit encore beaucoup évoluer pour rendre la coopération efficace.

Il faut arriver à une saisine des services la plus anticipée possible. Ensuite, il faut pouvoir accéder à la bonne information, dans les meilleures conditions pour travailler sur les traces laissées et ne pas perdre de temps. La preuve numérique et son imputabilité certaine sont une priorité pour les enquêteurs. Si l'ordinateur d'un individu a été piraté, la recherche des auteurs se poursuit de rebonds en rebonds et la coopération entre en ligne de compte.
Finalement, les conditions de l'enquête s'améliorent.

Il y a cependant des pays qui sont plus ou moins coopérants.
Nous entretenons d'excellentes relations avec un grand nombre d'agences internationales dont le FBI. Quel que soit l'Etat, les relations sont de qualité quoique dépendantes de contraintes différentes, difficilement compatibles parfois avec la célérité souhaitée pour les enquêtes en milieu informatique.

Et le gel des données ?
C'est un procédé efficace. Mais la mise à disposition ultérieurement des données gelées n'est pas toujours aisée. Dans certains cas, le gel n'est pas forcément accepté. Rappelons que la convention de Budapest de 2001 a harmonisé la notion de cybercriminalité au niveau international, elle a aussi posé les bases essentielles de la coopération, etc. Cette convention du Conseil de l'Europe est peu à peu ratifiée par les Etats.

Notez-vous une démarche similaire à la France dans les autres pays ?
L'Office a servi de modèles pour beaucoup de pays. A l'époque, cette démarche très structurée était très novatrice. Certains États ont revu complément le dispositif existant, en Grande-Bretagne avec le NCU (National Cyber Unit) et une forte volonté de centralisation. L'Allemagne a également installé une structure qui supervise les länders.

Vous avez été responsable de l'OCLCTIC au moment de sa création en 2001. Trouvez-vous qu'on a fait beaucoup de chemin depuis ?
Les progrès sont importants. Je pense que c'est même l'un des domaines où on a le plus ressenti d'améliorations dans tous les services : la police, la gendarmerie, les services du Premier ministre, etc. La brigade centrale de lutte contre la criminalité informatique, depuis 1990, a été le socle sur lequel s'est créé l'Office. Les premières grandes affaires sont intervenues dans le domaine des billetteries sur fond d'affaires criminelles ou pour déterminer à partir d'un support informatique l'emploi du temps de la victime d'un assassinat. Deux points d'entrée dans la matière avaient déjà émergés : l'usage de l'informatique pour commettre des infractions financières et un moyen d'investigation comme un autre.

Quelle est l'évolution qui vous paraît la plus intéressante ?
Il n'y a pas eu d'évolution spectaculaire mais progressive qui s'appuie à chaque fois sur du concret. A sa création l'Office comptait 15 policiers, en 2005, 60 personnels y étaient affectés. A la sous-direction, nous avons plus de 75 policiers et gendarmes hautement spécialisés travaillent à la lutte contre la cybercriminalité.

Combien de postes vont être créés ?
L'objectif est de doubler les effectifs, en diversifiant les recrutements pour apporter des analyses techniques systématiques et alléger l'activité opérationnelle des contraintes techniques. Cela permettra de restituer l'information à la division de l'anticipation et de l'analyse, au bureau de la coordination pour la rediffuser aux services d'enquêtes sous forme de modèles, d'améliorer l'information des investigateurs spécialisés, d'alimenter la formation continue de la police et la gendarmerie, de sensibiliser les magistrats à certains phénomènes pour leur faciliter l'approche des dossiers dans leurs enquêtes, d'alimenter le laboratoire technique et Pharos, etc. Ensuite, un cercle vertueux se crée.

« L'objectif est de doubler les effectifs, en diversifiant les recrutements pour apporter des analyses techniques systématiques et alléger l'activité opérationnelle des contraintes techniques »

Quels sont vos moyens ?
Au niveau central, ce sont 75 spécialistes de haut niveau qui œuvrent pour la lutte contre la cybercriminalité. Sur le territoire national, il y a 400 policiers (ICC) et 260 gendarmes (N-TECH) spécialisés. La SDLC s'appuie sur des antennes régionales constituées au sein des directions interrégionales de la police judiciaire, et des compétences formées au sein dans des directions départementales de la sécurité publique, et d'autres directions de la police nationale.

Cela a un coût.
La formation représente effectivement un investissement important ainsi que le matériel dont sont équipés les ICC (investigateurs en matière de cybercriminalité).

Des budgets supplémentaires ont-ils été alloués ?
Les budgets sont adaptés et progressent naturellement. Mais doit-on revoir ce dispositif ? L'enrichir d'autres outils ? Mettre à disposition d'autres types de matériels qui seraient à diffuser à un plus grand nombre mais à moindre coût, etc. ? Nous travaillons actuellement sur ces sujets avec les directions de la police pour rationaliser et permettre à plus de policiers d'investir le domaine dans la constatation, la prise de plaintes, la récupération d'informations, etc. Que peuvent faire les primo-intervenants ? Jusqu'où peuvent-ils agir ou faire intervenir un spécialiste ? Quelles sont les premières actions à accomplir ? Les bonnes questions à se poser avant d'intervenir ? Il faut donc disséminer cette information auprès de nos services. La police traite 75% de la délinquance, avec 145 000 policiers qui ne sont pas tous sur le terrain, mais qui sont en contact direct avec la délinquance de masse. Il convient de mettre à disposition des outils simples d'utilisation et qui ne mettent pas en péril la preuve qui serait recueillie. Le rôle de la sous-direction consiste donc à formaliser et à finaliser cette démarche de formation des primo-intervenants, d'améliorer le recrutement des ICC, ceux qui sont certifiés et qui représentent nos référents.

Les entreprises continuent-elles d'être réticentes à porter plainte car elles ont peur que le problème devienne public et que cela porte atteinte à leur image ?
Il y a toujours des réticences et il y en aura toujours. D'abord, les entreprises n'ont pas toujours connaissance de ce qui leur arrive. Elles doivent par ailleurs savoir qu'elles ne peuvent porter plainte que s'il y a infraction et que celle-ci n'entraînera pas de perte supplémentaire. Surtout, elles doivent avoir de bons réflexes pour porter plainte.
La médiatisation des affaires judiciaires représente un risque qui peut gêner les entreprises. Néanmoins, la stratégie de la DCPJ est précisément d'éviter la médiatisation et la publicité des affaires.

Les entreprises ne le savent peut-être pas assez ?
Effectivement, l'absence de visibilité nuit à la connaissance du dispositif. C'est une des raisons d'être des projets préalablement évoqués.Les entreprises ont deux possibilités soit elles portent plainte pour se préserver de leurs salariés ou protéger leur image, il s'agit d'une plainte parapluie. Dans ce cas, l'entreprise ne communiquera pas les informations nécessaires au développement de l'enquête. D'autres portent plainte dans le désir de faire aboutir le dossier.

Est-ce que cela débouche sur un procès ?
Si on arrête les auteurs, oui.

C'est peut-être là que réside la crainte de certaines entreprises.
La crainte d'une divulgation d'informations au cours d'un procès peut freiner les chefs d'entreprises.

Est-ce que vous n'êtes pas découragée par l'ampleur de la cybercriminalité ?
Jamais. C'est effectivement une course perpétuelle à la résolution des affaires et à la prévention. La question ici se pose comme dans les autres domaines, comme par exemple le trafic de stupéfiants, la prostitution, la pédopornographie, etc. Le domaine cyber ne se distingue pas spécifiquement.

Propos recueillis par Sylvie ROZENFELD