Lutte contre la cybercriminalité : l'ère de la mutualisation

Autor(en): **Ghion, Patrick**

Objekttyp: **Article**

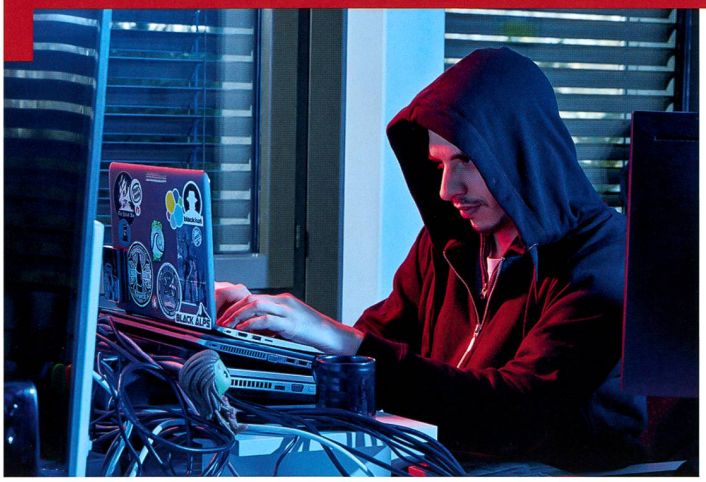
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2020)**

Heft 6

PDF erstellt am: **26.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-913939



La stratégie nationale de protection contre les cyberrisques (SNPC), qui touche aussi l'organisation policière, atteint ses objectifs. Depuis 2019, la Police cantonale de Genève héberge le Centre de Compétences Cyber au profit des cantons de la Suisse occidentale.

Cyberdéfense

Lutte contre la cybercriminalité – L'ère de la mutualisation

Cap Patrick Ghion
Chef de la section forensique au sein de la police cantonale de Genève

La lutte contre la cybercriminalité a connu un essor sans précédent au cours des dix dernières années. Le développement des moyens techniques et informatiques ainsi que des procédures d'enquêtes et d'analyses, le renforcement des moyens humains et matériels et pourtant, incidemment il semblait de plus en plus évident que ces axes de développement auraient une limite, ne serait-ce que financière.

Aussi, il a fallu réinventer la lutte contre la cybercriminalité sous une ère collaborative, mutualisant, autant que faire se peut, les ressources humaines et matérielles permettant la découverte de preuves dans le cadre d'enquêtes pénales et ainsi, procéder à l'identification des auteurs.

La Suisse et son système fédéraliste propre confèrent une grande autonomie aux cantons, notamment en matière d'organisation policière et, de ce fait à la lutte contre la cyber criminalité.

Or, il est rapidement apparu qu'il deviendrait impossible à chaque police cantonale de développer l'ensemble du spectre des moyens de lutte contre la cyber criminalité pour des affaires parfois minimes ou n'apparaissant qu'une ou deux fois par an. En d'autres termes, il devenait totalement contre-productif d'investir des moyens financiers, humains et de formation auprès de chacune des polices cantonales. Non seulement, la rentabilité des investissements pouvait être négligeable, mais le fait d'avoir plusieurs enquêteurs spécialisés n'ayant que peu l'occasion de s'adonner à certaines formes d'investigation, diluait le savoir-faire et ainsi réduisait l'efficacité générale.

Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022

Alors que les réflexions se menaient afin d'optimiser la lutte contre la cyber criminalité auprès des polices cantonales, le 18 avril 2018, le Conseil fédéral adoptait la nouvelle Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour les années 2018 à 2022.

Reposant sur les travaux réalisés dans le cadre de la première stratégie qui concerna les années 2012 à 2017, des compléments ont été apportés en collaboration avec les milieux économiques, les cantons et les hautes écoles.

Un des dix champs d'action de cette stratégie, la poursuite pénale, touche directement l'organisation policière et la façon dont les polices cantonales vont pouvoir développer une collaboration efficace et efficiente.

Un des aspects les plus marquants en ce qui concerne la mutualisation des moyens est la création de centres régionaux de compétences. Ces centres ont pour objectifs de développer des moyens et des compétences particulières à mettre au profit des autres polices cantonales.

C'est ainsi que la police cantonale de Genève héberge aujourd'hui le Centre de Compétences Cyber (CCC) pour la Suisse occidentale au profit de l'ensemble des cantons du concordat de coopération policière romand. L'objectif est d'identifier les moyens d'enquêtes nécessitant un investissement important, soit en termes d'équipement technique, de moyens informatiques ou encore de formations très spécifiques. Par ailleurs, il s'agit d'identifier ces mêmes moyens dans une perspective d'utilisation marginale, soit utilisée rarement et pour des domaines très spécifiques.

Police cantonale de Genève : Une forme d'organisation de lutte contre la cyber criminalité

Comme déjà évoqué, chaque police cantonale a le loisir de développer des moyens qui lui sont propres afin de lutter contre tel ou tel phénomène, notamment la cyber criminalité.

L'exemple de la police cantonale de Genève n'est donc qu'un parmi ceux des autres cantons. La problématique de la lutte contre la cyber criminalité a été adressée de longue date à Genève puisque les premiers cas sont apparus en 1996. La création d'un Groupe de Criminalité Informatique (GCI) en 1998 a été la première pierre à l'édifice de ce qui est aujourd'hui devenu le Centre de Compétences Régional en matière cyber. En 2003, ce groupe a été consolidé sous la forme de la Brigade de Criminalité Informatique (BCI) dont la dénomination demeure encore aujourd'hui.

La BCI est aujourd'hui dotée de moyens humains importants puisqu'elle est composée de 16 inspecteurs de police et de trois ingénieurs-informaticiens. Ces 19 collaborateurs hautement formés et spécialisés apportent leur soutien quotidiennement aux policiers et aux procureurs genevois.

Les axes développés ces dernières années sont le fruit d'une stratégie de développement à long terme puisqu'un accent particulier est mis sur la détection des phénomènes à explorer sur une projection de trois à cinq ans. C'est cette prospective continue qui a été le fondement pour le développement du Centre de Compétences Cyber à Genève et la mise en place d'une ère collaborative notamment avec les cantons romands.

La BCI genevoise a ainsi développé ses activités autour de plusieurs axes qui peuvent être résumés par, notamment :

- L'analyse de supports de données numériques (cryptographie, stéganographie, RAID (*Redundant Array of Independent Disks), cloud computing*).
- Enquêtes Internet avancées, Open Source Intelligence (OSINT).
- La récupération de données sur les téléphones, tablettes informatiques, GPS.
- La récupération de données sur les véhicules avec informatique embarquée (auto-bateau-avion).
- L'analyse et le retro engineering des Malwares.
- L'utilisation de logiciels spéciaux (interception).
- La manipulation des images vidéo en termes d'éléments de preuve.
- La lutte contre la pédo criminalité sur Internet.

Ces axes ont été développés au fil des ans et comportent une multitude de facettes. La mise en œuvre quotidienne de moyens spécifiques et hautement techniques requiert de la part des spécialistes une mise à jour continue des outils techniques, mais également des standards et des procédures opérationnelles qui peuvent parfois évoluer à 180°.

Police cantonale de Genève: Centre de Compétences Cyber (CCC)

Parmi les spécialisations de la Brigade de Criminalité Informatique évoquées plus haut, deux axes ont été particulièrement développés dans le cadre du CCC pour la mise à disposition des infrastructures techniques et des compétences humaines au profit des cantons romands. Il s'agit de: Analyse avancée pour ce qui touche à l'Internet des Objets ou encore Internet of Things (IoT)

Toutes les polices cantonales disposent de moyens pour l'analyse des téléphones mobiles, des GPS ou encore des tablettes numériques. Il s'agit ici d'apporter un soutien complémentaire lorsque les moyens d'une police cantonale sont épuisés ou n'ont pas donné les résultats escomptés.

A titre d'exemple, un appareil permettant de récolter les données sur les prises ODB2 des véhicules automobiles coûte plusieurs milliers de francs et l'utilisation reste, à l'heure actuelle, marginale par rapport à son prix. En proposant ce service à l'ensemble des polices cantonales romandes, non seulement l'appareil est utilisé de manière régulière, mais le spécialiste de la BCI responsable pour son utilisation acquiert une expertise accrue au vu de son expérience. Ce principe fondamental vaut pour l'ensemble des infrastructures et outils techniques avancés qui sont mutualisés à Genève.

Utilisation de logiciels spéciaux (interception)

Également dans ce domaine, les moyens et les compétences techniques particulièrement avancées permettant la mise en œuvre opérationnelle de tels outils ne pourraient être assurés par l'ensemble des cantons de manière individuelle.

Il va de soi que le Centre de Compétences Cyber rencontre les spécialistes des polices cantonales de façon régulière et que le catalogue des prestations est en développement continu.

Plateforme d'Information de la Criminalité Sérielle en Ligne (PICSEL)

Pour terminer, si le Centre de Compétences Cyber (CCC) a été développé à l'origine pour les aspects énoncés plus haut, une évolution majeure dans la lutte contre les escroqueries sur Internet a été développée de manière collaborative sans précédent en Suisse. Avec une direction auprès de la police cantonale du Jura, une implication importante des cantons de Neuchâtel et de Vaud, le centre PICSEL sera joint au CCC à partir du 1er janvier 2021.

Le succès de cette plateforme d'échange inter cantonale dotée d'un processus de gestion des infractions « cyber » et des traces numériques en fait un outil dont la perspective nationale est déjà en route. Il s'agit ici de méthodes d'analyse criminelle permettant la détection de phénomènes cybercriminels sériels au niveau national. Le centre PICSEL sera placé au sein de la Brigade de Renseignement Criminel (BRC) dont les policiers spécialisés et les analystes disposent d'une expérience très importante dans la colligation de données.

C'est ainsi que, dans un Etat fédératif comme la Suisse, les moyens de lutte contre la cyber criminalité ont été repensés afin de pouvoir agir sur l'ensemble des spectres touchant à cette problématique. L'évolution des mentalités et la volonté de trouver ensemble des moyens afin d'endiguer cette forme de criminalité ouvrent des perspectives collaboratives nouvelles dans le but de protéger et de servir les citoyens.

P. G.

COMMUNICATION SÉCURISÉE ET MONITORING SONT UNE QUESTION DE CONFIANCE

Roschi Rohde & Schwarz SA vous soutient en tant qu'entrepreneur général avec une expertise locale dans le maintien de votre souveraineté numérique.

www.rohde-schwarz.com/ch

ROHDE&SCHWARZ
Make ideas real