Conseil d'Etat
Staatsrat

CANTON DU VALAIS
KANTON WALLIS

RÉPONSE AU POSTULAT

Auteur	Commission de la sécurité publique, par les députés Anton Lauber et Géraldine Arlettaz-Monnet
Objet	Quels moyens pour lutter contre la criminalité informatique et économique ?
Date	8.5.2017
Numéro	4.0262

Le postulat demande l'établissement d'un rapport sur les phénomènes relevant de la cybercriminalité et de la criminalité économique ainsi que sur leurs conséquences.

Ce document est annexé à la présente réponse et résume la nécessité de renforcer la section financière d'un analyste financier supplémentaire et le groupe investigation numérique d'un ingénieur en informatique spécialisé en cybercrime.

Il est proposé l'acceptation du postulat.

Conséquences sur la bureaucratie :	Néant
Conséquences financières :	CHF 240'000 (2 x CHF 120'000.-)
Conséquences équivalent plein temps (EPT) :	2 postes attribués au budget 2018
Conséquences RPT :	Néant

Sion, le 9 janvier 2018

Département de la sécurité, des institutions et du sport
Police cantonale

Departement für Sicherheit, Institutionen und Sport
Kantonspolizei

CANTON DU VALAIS
KANTON WALLIS

Rapport

Destinataire Conseil d'Etat

Auteur Christian Varone

Date 9 janvier 2018

"Quels moyens pour lutter contre la criminalité informatique et économique ?"

Postulat No 4.0262 déposé pour la Commission de la sécurité publique, par les députés Anton Lauber et Géraldine Arlettaz-Monnet (08.05.2017)

Conformément au postulat déposé par la Commission de sécurité publique, nous vous fournissons ci-après le rapport sur les phénomènes relevant de la cybercriminalité et de la criminalité économique ainsi que sur leurs conséquences.

1. Criminalité informatique

Il convient, avant toute autre analyse, de comprendre que même s'ils sont indissociables, les domaines de la **cybercriminalité** et de ce que l'on appelle actuellement l'**inforensique** constituent deux entités distinctes en termes d'approche policière.

En effet, la cybercriminalité englobe l'ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier l'Internet, et se décline en deux sous-catégories, à savoir :

- la cybercriminalité au sens étroit, qui implique l'utilisation concrète des systèmes informatiques et des réseaux de télécommunications pour commettre des infractions (accès indu à un système informatique, soustraction de données, détérioration de données, etc.)
- la cybercriminalité au sens large, qui englobe les infractions dites « classiques » mais dont les auteurs utilisent comme vecteur les outils technologiques actuels (escroqueries dans le cadre de petites annonces frauduleuses ou « à la romance », sextorsion, pornographie interdite, grooming (prise de contact en ligne avec des mineurs), phishing, etc.)

L'inforensique, ou informatique légale, fait quant à elle référence à l'application de techniques et de protocoles d'investigations numériques respectant les procédures légales et permettant de collecter, de conserver et d'analyser des preuves issues de supports numériques ou de l'Internet à l'attention des Autorités de poursuite pénale.

Dès lors, si **la cybercriminalité est l'affaire de tout policier**, l'**inforensique** fait appel à des connaissances techniques spécifiques et reste du ressort de personnel spécialement formé (policier ou civil), en particulier du **groupe investigation numérique** de la police cantonale valaisanne.

Le groupe précité traite en moyenne une **soixantaine de dossiers par année**. Ce chiffre ne reflète cependant pas celui, non quantifié, des délits ou des crimes cybernétiques qui passent souvent inaperçus, tant pour la police que pour les médias et donc pour la société en général. Lorsqu'ils touchent des établissements financiers ou des entreprises, ces délits ne sont en effet que rarement dénoncés pour éviter notamment le déficit d'image que cela pourrait engendrer. Les particuliers eux-mêmes hésitent parfois à dénoncer ceux dont ils sont victimes, par honte de leur propre comportement ou par peur des conséquences que cela pourrait avoir sur leur vie privée et/ou professionnelle.

Une étude KPMG intitulée « Clarity on Cyber Security » et réalisée cette année pour la troisième fois, révèle qu'au cours des 12 derniers mois, 88% des entreprises interrogées ont été victimes d'attaques, contre 54% l'année précédente. Outre l'interruption de l'activité commerciale pour plus de la moitié de celles-ci, plus d'un tiers des sondés ont dû essuyer des pertes financières. Cette étude estime à près de 200 millions de francs le coût des dommages causés par la cybercriminalité aux entreprises en Suisse en 2014. On ne parle pas ici des **particuliers** également victimes de ces phénomènes et qui peuvent perdre de **quelques centaines de francs à plusieurs dizaines, voire centaines de milliers de francs par cas**.

La récente cyberattaque mondiale au moyen du « rançongiciel *WannaCry* » et le nombre de machines infectées dans le monde démontre à elle seule le potentiel préjudice qu'une telle attaque peut provoquer.

Une autre étude du cabinet d'audit « PricewaterhouseCoopers » fait état d'une augmentation de 48% des incidents de sécurité répertoriés dans le monde en 2014, sur un an (près de 43 millions d'incidents, soit près de 117'000 par jour en moyenne).

Même si la prévention a certainement amélioré la capacité de résilience des particuliers et des entreprises face aux phénomènes cybercriminels, il semble évident que la dématérialisation progressive mais constante de notre société qui se virtualise ne peut qu'attiser l'intérêt et les moyens mis en œuvre par les cybercriminels qui y voient une manne financière potentielle intarissable. La « richesse » affichée par la Suisse ne peut donc qu'attiser, de toute évidence, les convoitises dans ce domaine.

Au vu de ce qui précède, une réflexion fondamentale est menée depuis plusieurs années au sein du Réseau national de sécurité (http://www.svs.admin.ch/) et des discussions liées à la possible mise en place d'un véritable centre de coordination suisse en matière de phénomènes cybercriminels. La police fédérale est d'ailleurs en pleine restructuration. De son côté, la centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI – www.melani.admin.ch), qui collabore étroitement avec les entreprises, publie un bulletin semestriel donnant un état de la situation sécuritaire en matière cyber.

Sur un plan cantonal, la police valaisanne diffuse régulièrement, par le biais de la section idoine, des **messages de prévention destinés à la population ou aux entreprises**, ceci dans un cadre général de prévention contre la criminalité sous toutes ses formes.

Nous relevons également qu'afin de sensibiliser l'ensemble des forces policières aux phénomènes de cybercriminalité, une formation ad hoc a été mise en place en collaboration avec l'ILCE de Neuchâtel. Une approche du même type est maintenant proposée au sein de l'Académie de police de Savatan.

Concernant les compétences techniques supérieures nécessaires à la sauvegarde et à l'analyse des traces numériques, le groupe investigation numérique de la police cantonale valaisanne compte, depuis 2006, **deux collaborateurs issus de ses rangs** et au bénéfice d'un CAS en investigation numérique obtenu auprès de la HE-ARC de Neuchâtel. Ils appuient l'entier des forces de police du canton pour les enquêtes en matière de cybercriminalité et l'exploitation des données y relatives saisies.

A titre de comparaison, voici la situation actuelle des cantons du concordat RBT en termes d'effectifs au sein des unités d'enquêtes en matière de criminalité informatique :

- Genève : 10 personnes
- Vaud : 4 personnes (5ème unité accordée et en cours d'engagement)
- Fribourg : 4 personnes (5ème en cours d'engagement – 6ème prévue à moyen terme)
- Neuchâtel : 2 ETP (engagement de 2 autres ETP en cours – objectif = 5 ETP dans l'année)
- Jura : 1 ETP
- Tessin : 8 personnes (dont 3 s'occupant également de l'ACO)
- Berne : 18 personnes

Pour rappel, le canton de Zürich s'est doté, en 2013, d'un centre de compétence en cybercrime dans lequel sont rassemblés notamment des procureurs et des spécialistes en informatique. Le Conseil d'Etat zürichois a annoncé, au début de cette année, la création de 20 nouveaux postes de spécialistes pour le renforcer, dont 10 informaticiens.

Sous l'égide de la CCDJP, une étude est en cours quant à la faisabilité d'un tel centre en Suisse romande dans le cadre du concordat RBT. A ce jour cependant et à notre connaissance, aucun échéancier n'a encore été établi.

2. Criminalité économique

La criminalité économique est silencieuse et ravageuse. Elle ne touche pas au sentiment de sécurité de la population, tant qu'elle ne perturbe pas l'ordre public et qu'elle n'est pas entachée de violence. Elle a pourtant un pouvoir destructeur, en gangrénant nos institutions, en déséquilibrant les rapports économiques et en démantelant le patrimoine de personnes morales et physiques.

La lutte contre la **criminalité économique, dite complexe**, est menée par **la Section financière**, qui doit faire face à une complexification du monde financier, nécessitant des connaissances techniques de plus en plus pointues et des analyses financières propres à faire la démonstration de procédés criminels de plus en plus élaborés. Elle collabore en outre avec la Police judiciaire fédérale dans la lutte contre le crime organisé et le blanchiment d'argent.

Ce qui a véritablement changé au cours des dernières années, c'est l'avènement de l'internet, qui a rendu le monde économique accessible à toute personne connectée et qui a dématérialisé les relations entre individus. Si l'e-banking, l'e-trading, les moyens de paiement en ligne, les réseaux sociaux, la vente en ligne, la VoIP, sont autant de facilitateurs de la vie quotidienne, ils n'en sont pas moins une aubaine pour des personnes peu scrupuleuses. Le champ d'action de la criminalité économique s'est ouvert un marché mondial, d'un seul clic de souris.

Outre la criminalité économique proprement dite, la Section financière coordonne et conduit l'action, sur le plan cantonal, du traitement des **phénomènes cybercriminels** (escroqueries au faux héritage, à la romance, à la vente en ligne, etc.), pour lesquels les messages de prévention demeurent la mesure la plus efficace, à l'encontre de criminels agissant depuis l'étranger.

Dans le cadre du concordat réglant la coopération en matière de police en Suisse romande, il a notamment été décidé de la mise en œuvre d'une base de données commune dans la lutte contre les escroqueries commises par le biais d'internet. Cette coopération nécessitera toutefois une implication cantonale dans la gestion et l'analyse des données, compte tenu des infractions croissantes en la matière.

Le préjudice de la criminalité économique se chiffre, pour notre seul canton, **à plusieurs dizaines de millions, voire centaines de millions de francs suisses par année**. Il ne s'agit que de la partie émergée, soit les annonces faites aux services de police.

La Section financière de la Police cantonale valaisanne est dotée de **11 unités plein temps**, **dont deux collaborateurs germanophones et un analyste financier**. Cette entité traite une centaine de requêtes par année, avec des enquêtes dont la durée de traitement peut varier de quelques mois à plusieurs années.

La Section financière s'est adjointe les services d'un analyste financier à la fin des années 90, suite à des affaires ayant défrayé la chronique. L'apport technique et théorique d'un personnel spécialisé et formé, hors du cursus policier, est aujourd'hui indissociable du fonctionnement d'une section spécialisée dans la lutte contre la criminalité économique. Au fil du temps, la Section financière a accru sa technicité et sa capacité d'analyse, notamment par l'apport de l'analyste et une volonté des collaborateurs de se former via un cursus de formation supérieure. Le système a toutefois atteint ses limites au vu de la complexité croissante des enquêtes, du volume en termes d'analyses que celles-ci impliquent et du niveau d'analyse qui est aujourd'hui requis. La Section financière est victime, en quelque sorte, de sa spécialisation, dont le modèle a fait ses preuves, et qui en fait un acteur incontournable pour traiter les affaires économiques complexes. Le corollaire en est une hausse constante des sollicitations.

3. Conclusions

L'ère du numérique et de la globalisation a modifié les comportements sociaux, si bien qu'aujourd'hui, les outils de communication et les supports numériques font partie intégrante du matériel saisi aux fins de preuve. La part et la complexité de ceux-ci ne cessant de croître, l'effectif et les compétences du groupe investigation numérique atteignent leurs limites. En comparaison intercantonale, le canton du Valais fait figure de parent pauvre en termes d'effectif et de compétences externes. L'engagement d'une unité supplémentaire issue d'une formation tertiaire (ingénieur en informatique) est devenu indispensable au vu des nécessités d'enquête en inforensique.

Il en va de même s'agissant de la criminalité économique proprement dite. L'engagement d'un deuxième analyste financier permettrait d'augmenter sensiblement les capacités en termes d'analyse et de facto le volume d'affaires traitées par la section financière s'agissant d'enquêtes particulièrement complexes. Les ressources actuelles sont insuffisantes pour répondre à satisfaction tant aux attentes des justiciables qu'à celles des autorités judiciaires en charge de l'instruction.