Date de dépôt : 4 avril 2016

Rapport

de la Commission des travaux chargée d'étudier le projet de loi du Conseil d'Etat ouvrant un crédit d'investissement de 1 200 000 F pour la lutte contre la criminalité informatique et la cybercriminalité

Rapport de M. Jean-Louis Fazio

Mesdames et
Messieurs les députés,

La Commission des travaux s'est réunie le 23 février 2016, sous la présidence de M[me] Bénédicte Montant, pour étudier ce projet de loi 11788.

Elle a pu bénéficier de la collaboration de M. Pierre Maudet, conseiller d'Etat, M. Eric Favre, directeur général DSE, et M. Patrick Ghion, capitaine de la police judiciaire.

Que toutes ces personnes soient ici remerciées de leurs apports appréciés aux travaux de la commission.

Présentation

M. Maudet remercie la commission et indique que ce projet de loi revêt une importance stratégique majeure pour le bon fonctionnement de la police et de la sécurité du canton. Il rappelle que le PL a fait l'objet d'une discussion et d'une accélération puissante en fin d'année 2015, à la faveur des événements ayant secoué la France en novembre. Il indique que M. Ghion est capitaine de la police judiciaire et, jusqu'à peu, chef de la brigade de la criminalité informatique (BCI), notamment chargé de la lutte contre la cybercriminalité. Il souligne qu'il y a peu d'affaires criminelles qui aujourd'hui n'impliquent pas les services de cette brigade et il précise que, en parallèle, il y a de plus en plus de cas qui relèvent directement de la

ATAR ROTO PRESSE – 200 ex. – 04.16

cybercriminalité en tant que telle. Il observe que le PL est très modeste et que la somme en jeu est, selon lui, ridicule en regard des enjeux.

M. Ghion remercie la commission et indique qu'il va d'abord faire un retour sur la BCI. Il rappelle premièrement que la BCI est située dans la section forensique de la police judiciaire, mais qu'elle est aussi au service d'autres services comme par exemple la brigade de la sécurité internationale. Il précise que le premier cas de cybercriminalité a été traité par deux personnes en 1996. Il souligne que la naissance du groupe de criminalité informatique a eu lieu en 1998 et que la BCI a finalement vu le jour en 2003. Il explique que le métier de base de la criminalité informatique est l'analyse de supports de données à hauteur de 25%. Il souligne que, pour l'affaire Adeline, une personne a dû travailler durant toute une nuit pour pouvoir remonter sur les intentions de l'auteur, à travers les données retrouvées sur les supports informatiques apportées à la BCI. Il indique que c'est grâce à ce qui a été trouvé que l'on a probablement pu éviter un nouvel assassinat. Il indique ensuite que les enquêtes internet et l'Open Source Intelligence (OSINT) représentent 33% du travail de la BCI. M. Ghion souligne que ce que l'on recherche sur Google ne donne accès qu'à une petite partie de ce qui existe et que le Darkweb est donc constitué de la plus grande partie des données stockées sur internet. Il ajoute que la crypto-monnaie va à l'avenir occuper de plus en plus les enquêteurs et il évoque brièvement une affaire d'extorsion et de chantage en bitcoin, ayant eu lieu l'année passée. Enfin, il explique qu'a terme ils aimeraient pouvoir effectuer des patrouilles internet sur les réseaux sociaux, notamment pour voir comment les jeunes s'y comportent et pouvoir le cas échéant faire face à un éventuel problème ; il précise néanmoins que la BCI n'en a actuellement pas les moyens. Il indique ensuite qu'une grande partie du travail de la BCI concerne la téléphonie mobile au sens large (19%), non seulement les téléphones mobiles mais aussi les tablettes, les GPS et tous les autres objets connectés. Il précise que l'objet connecté d'un criminel et à même de fournir des informations sur l'activité de ce dernier. Par ailleurs, il indique que Google et Levi's se sont réunis pour créer un tissu connecté ; il explique qu'il y a donc de plus en plus d'objets qui vont donner en permanence des informations sur les comportements des individus. Il relève que chaque laboratoire a un spécialiste et il souligne que plus de mille téléphones sont analysés par année. Il précise que, compte tenu du nombre de cas à analyser, ils ont créé des laboratoires délocalisés à l'aéroport et à l'Hôtel de Police pour les affaires de peu d'importance. Il en vient ensuite aux véhicules avec de l'informatique embarquée qui occupent pour le moment 1% du travail de la BCI ; il précise que ce taux va néanmoins augmenter avec l'évolution de ce type de technologie. Il relève que cette

technologie va beaucoup plus loin que les données GPS, car l'on peut par exemple désormais déterminer les temps d'ouverture et de fermeture des portes ou du coffre d'un véhicule, qui peuvent être déterminantes pour une enquête autour d'un meurtre. Il relève que la sécurité autour de cette technologie reste toutefois une faiblesse puisqu'il est actuellement très facile de pirater une voiture avec de l'informatique embarquée.

M. Ghion affirme ensuite que la question de l'interception reste problématique car il n'y a aucun moyen de pouvoir lire des données qui ont été cryptées à l'avance par le fournisseur d'accès avant d'être mises en ligne sur le réseau, si ce n'est l'utilisation d'un cheval de Troie pour tenter de prendre le contrôle de la machine. Il explique qu'il n'y a eu pour le moment que deux cas de ce type dans l'histoire de la BCI. Il souligne ensuite que l'augmentation des malware a été de 114% en 2014 et qu'elle s'explique surtout par la simplicité de la mise en œuvre d'un malware. Il mentionne le cas célèbre d'un encaveur valaisan, qui a occupé beaucoup de temps à la BCI ; il souligne qu'il est premièrement nécessaire d'isoler le malware et savoir comment il fonctionne, potentiellement quelles données il récupère, et idéalement de pouvoir déterminer où il les envoie. Par la suite, il précise qu'ils ont aussi un laboratoire vidéo qui représente le 10% du travail de la BCI. Il souligne que de nombreuses sociétés de vidéosurveillance possèdent des codecs pour pouvoir crypter les images et donc avoir la mainmise sur leur flux de vidéos. Il explique qu'ils sont donc obligés de transformer les flux vidéo pour qu'ils soient visibles par le PJ et les inspecteurs qui vont devoir analyser le flux et améliorer les images. Il donne l'exemple des recherches autour de la vidéo du motard ayant traversé le canton à toute vitesse qui ont permis de retrouver la personne en question. Il souligne qu'il n'y a actuellement qu'un spécialiste de la question au sein de la BCI.

M. Ghion en vient ensuite au PL 11788 et indique qu'il y a des achats qu'ils ne peuvent pas prévoir à l'avance puisqu'ils sont tributaires de l'actualité criminelle. Il donne l'exemple d'un appareil, permettant de faire des analyses sur un disque dur tout en faisant des copies de données, acquis lors de l'affaire Adeline. Il précise que l'équipement des nouveaux collaborateurs est aussi l'un des enjeux de ce PL puisque la BCI désire augmenter ses effectifs pour améliorer ses compétences. Il souligne que cet équipement est conformé d'ordinateurs d'analyse, un matériel cher car il doit faire fonctionner un logiciel spécifique d'analyse dont les critères sont bien établis pour qu'il puisse être efficace. Concernant l'application d'analyse et le réseau protégé, il explique que la mise à disposition des données est déterminante pour le confort de l'enquête. Il précise que, pour des affaires de pédopornographie de 2003, il fallait trier tous ce qui était légal ou non et

imprimer ensuite chaque photo au coût de 5 F par copie. Il relève qu'il est aujourd'hui beaucoup plus confortable que la masse de données soit accessible grâce à des logiciels permettant d'indexer ces dernières. Il explique par la suite que la BCI traite des aspects techniques des enquêtes de l'IGS, pour lesquelles il est demandé de pouvoir séparer certaines informations du réseau propre de la BCI et de les mettre dans un réseau protégé séparé. Concernant la mise à niveau de l'infrastructure de stockage, il explique que la BCI dispose d'un réseau propre de stockage et que la surface dévolue à ce stockage est beaucoup plus grande que celle de l'ensemble des espaces de stockage de l'Etat de Genève. Il précise qu'il est important de pouvoir mettre à niveau les infrastructures pour garantir la pérennité des données et un accès suffisamment rapide aux données pour l'enquête. Ensuite, il aborde la mise en production du SPEC numérique et souligne que la BCI stocke les pièces à conviction des auteurs d'infractions, ce qui nécessite la mise en place d'un système d'effacement de ces données numériques pour respecter la loi. Il souligne enfin que les objectifs visés par le PL sont respectivement de s'adapter aux nouvelles menaces, de moderniser et sécuriser l'infrastructure de la BCI et, enfin, de réduire le délai de traitement des pièces pour pouvoir fournir un service optimal à la population. Il indique qu'ils ont pris comme indicateurs la moyenne de traitement d'une pièce, le socle de pièces en attente et le taux de résolution des affaires. Il précise qu'ils oscillent actuellement entre 60 et 80 pièces en attente et qu'il n'est pour le moment pas possible de diminuer ce chiffre.

M. Maudet indique que la volonté politique de renforcer les compétences et les effectifs de cette brigade remonte pour sa part à trois ans en arrière. Il souligne qu'ils ont rajouté un axe dédié à la cybercriminalité dans la lutte contre la criminalité en septembre 2014 et que cela sera vraisemblablement confirmé avec le procureur général à l'horizon du mois de septembre 2016. Il observe qu'il y a vraiment un besoin mais sans doute aussi une capacité de pouvoir projeter la police dans des activités nouvelles. Il souligne que l'on a parfois le sentiment que l'on a toujours une guerre de retard dans ce domaine spécifique et il estime que, moyennant quelques efforts, l'on pourrait augmenter l'attractivité de la police, en envisageant cette dernière d'une nouvelle manière et en faisant venir des talents sans liens directs avec la police. Il indique enfin qu'il a la volonté de faire de Genève un véritable pôle dans l'IT, aussi au niveau de la sécurité.

Questions

Un commissaire se demande si ces interfaces et collaborations sont compatibles avec les systèmes présents dans les autres cantons, fédéraux et étrangers.

M. Ghion indique qu'il fait partie d'un concordat latin qui se réunit de manière pluriannuelle pour discuter des différents moyens utilisés et essayer d'avoir une vue commune sur les investissements à effectuer et sur la possible mutualisation pour l'achat d'un certain matériel.

M. Maudet souligne que la perception de l'acuité de cette problématique varie d'un canton à un autre. Il relève que le Conseil d'Etat préconise une attitude proactive qui consiste à dire qu'il y a suffisamment d'intérêts sécuritaires en jeu pour prendre quelques risques et marquer un certain volontarisme, avec néanmoins le risque parfois de faire des erreurs. Il indique qu'il a coutume de dire qu'avec ces appareils, l'agresseur n'a jamais été aussi proche et le juge n'a jamais été aussi loin. Il explique qu'ils ne veulent donc pas vendre une technologie dont on connaît aussi les limites.

Le même commissaire souligne que Genève a souvent eu une réputation de ville d'espions. Il se demande si le BCI est capable de détecter ce type d'activités et de surveillance.

M. Maudet indique qu'il existe un cadre législatif extrêmement strict, voire inexistant. Il précise que l'on n'a pas d'autres outils que le code de procédure pénale. Il précise qu'actuellement, à la Commission judiciaire, des discussions ont lieu sur la base légale, tenant compte de l'avis du TF, qui devrait permettre à la police de pratiquer trois types de mesures intrusives et sous contrôle judiciaire. Par ailleurs, il souligne que les services secrets genevois sont les seuls à ne pas pouvoir pratiquer des écoutes téléphoniques.

M. Ghion indique que la police a une brigade de sécurité intérieure qui travaille, sous l'égide de la Confédération, avec un département de contre-espionnage.

Un commissaire pose une question sur la sécurité des sites sensibles, comme par exemple la police, le corps judiciaire, l'Etat, l'hôpital, les SIG,… Il se demande si la BCI collabore avec ces différentes entités dans le but de les protéger.

M. Ghion indique que la BCI n'a pas de relation avec ces entités visant à faire de la prévention.

M. Maudet rappelle que, au début de l'année 2013, il y avait eu un débat sur les risques humains autour de l'administration fiscale et les systèmes informatiques. Il précise qu'une prise de conscience des risques en matière de

sécurité a eu lieu, permettant notamment de déterminer où il pourrait y avoir un risque d'usage intrusif ou abusif du système informatique.

M. Favre ajoute que, dans ce PL, la partie de l'infrastructure est mise en place par la DGSI. Il souligne qu'il y a néanmoins un problème légal et de compétence pour certains éléments et qu'ils doivent donc, pour ces derniers, passer la main à la police. Il souligne qu'un rapprochement est cependant né entre la DGSI et la police, notamment grâce à ce PL. Il rappelle que les infrastructures mentionnées ici sont bien sous la gestion de la DGSI, comme le reste de l'informatique de la police.

Un député observe que, en termes de cybercriminalité, l'arnaque aux faux sentiments est quelque chose de fort courant. Il désire savoir ce qu'il en est des collaborations avec Interpol, compte tenu du fait que la cybercriminalité est très souvent internationale. Il se demande si une augmentation des moyens de la BCI permettrait donc une meilleure collaboration internationale.

M. Ghion relève que l'on touche ici à la question des escroqueries sur internet, ce qui constitue le 33% des affaires qui concernent la BCI. Il indique que l'on peut parfois remonter les adresses IP qui vont mener au loueur de la ligne. Il observe que, lorsque ce dernier se trouve en Suisse ou dans un pays voisin, l'on arrive chez une personne. Il souligne cependant que la plupart de ces arnaques concernent des pays africains, où les adresses IP regroupent tout un quartier. Il indique que l'on peut donc arriver parfois vers un cybercafé, mais sans pouvoir déterminer qui est le coupable puisqu'il n'y a souvent pas de système de caméras de surveillance dans ces établissements. Par ailleurs, il souligne que les transferts d'argent ne sont pas non plus la manière la plus simple de remonter vers le criminel, les arnaqueurs en question passant par un compte en Grande-Bretagne, avant que l'argent ne soit renvoyé vers le destinataire final.

M. Maudet observe que cette question concerne moins ce PL que des mesures de prévention pour lesquelles il y a déjà un budget existant. Il considère qu'il est difficile de conscientiser les personnes et les pousser à ne pas être des « pigeons ». Il observe que l'on constate par ailleurs une recrudescence de vols de personnes âgées, mais il précise que cela ne concerne pas que le volet de la cybercriminalité et que la lutte doit passer par un contact de police de proximité pour atténuer la facilité avec laquelle l'on atteint les publics les plus vulnérables.

Une députée se demande si la BCI travaille principalement avec le ministère public ou si elle effectue aussi des enquêtes préventives.

M. Ghion souligne qu'ils ne travaillent que sur requête des polices ou sur mandat du ministère public, car ils manquent de moyens légaux et économiques pour pouvoir effectuer des enquêtes préventives.

Une députée désire savoir s'il y a une charte interne pour le ministère public, l'IGS et les autres services, en ce qui concerne le traitement de données parfois extrêmement sensibles.

M. Ghion explique qu'il y a une procédure VIP pour les affaires particulièrement sensibles et qu'un réseau séparé est donc prévu pour ce type de cas. Il observe en outre que les requêtes du ministère public exigent aussi parfois des mesures particulières de sécurité. Il souligne enfin qu'ils travaillent actuellement à mettre en place une procédure efficace pour la destruction des pièces à conviction.

Un député se demande si ce crédit permettra à la BCI d'être bien équipée, en notamment en regard des polices des autres pays.

M. Ghion explique que, aux Pays-Bas et en France, l'on est mieux équipé qu'ici, mais il considère néanmoins que ce PL va déjà permettre à la BCI d'être bien dotée.

Une députée désire savoir si la BCI peut actuellement travailler sur les réseaux sociaux et ce qu'il en est de ce type d'enquêtes.

M. Ghion indique qu'ils travaillent main dans la main avec la brigade de sécurité intérieure pour certaines affaires, notamment des cas de terrorisme. Il précise que la BCI n'est cependant pas présente sur les réseaux sociaux, hormis dans les cas extrêmes qu'il vient d'évoquer.

Une députée se demande si une veille des réseaux sociaux est possible pour les questions intérieures.

M. Maudet indique que la plupart des services de police effectuent une veille des réseaux sociaux, par exemple pour les questions de prostitution illégale, et pas seulement la BCI.

Vote

La Présidente met aux voix le PL 11788 :

Entrée en matière :

Pour : 14 (3 MCG, 2 UDC, 4 PLR, 1 PDC, 1 Ve, 3 S)
Contre : –
Abstention : 1 (1 EAG)

Titre et préambule :

Pour : 14 (3 MCG, 2 UDC, 4 PLR, 1 PDC, 1 Ve, 3 S)
Contre : –
Abstention : 1 (1 EAG)

Art. 1 Crédit d'investissement :

Pour : 14 (3 MCG, 2 UDC, 4 PLR, 1 PDC, 1 Ve, 3 S)
Contre : –
Abstention : 1 (1 EAG)

Art. 2 Planification financière :

Pour : 14 (3 MCG, 2 UDC, 4 PLR, 1 PDC, 1 Ve, 3 S)
Contre : –
Abstention : 1 (1 EAG)

Art. 3 Amortissement :

Pour : 14 (3 MCG, 2 UDC, 4 PLR, 1 PDC, 1 Ve, 3 S)
Contre : –
Abstention : 1 (1 EAG)

Art. 4 Suivi périodique :

Pour : 14 (3 MCG, 2 UDC, 4 PLR, 1 PDC, 1 Ve, 3 S)
Contre : –
Abstention : 1 (1 EAG)

Art. 5 Loi sur la gestion administrative et financière de l'Etat :

Pour : 14 (3 MCG, 2 UDC, 4 PLR, 1 PDC, 1 Ve, 3 S)
Contre : –
Abstention : 1 (1 EAG)

La Présidente soumet au vote le PL 11788 :

Pour : 14 (3 MCG, 2 UDC, 4 PLR, 1 PDC, 1 Ve, 3 S)
Contre : –
Abstention : 1 (1 EAG)

Le PL 11788 est adopté.

La catégorie III est préavisée.

Projet de loi
(11788)

ouvrant un crédit d'investissement de 1 200 000 F pour la lutte contre la criminalité informatique et la cybercriminalité

Le GRAND CONSEIL de la République et canton de Genève
décrète ce qui suit :

Art. 1 Crédit d'investissement

Un crédit global de 1 200 000 F (y compris TVA et renchérissement) est ouvert au Conseil d'Etat pour la lutte contre la criminalité informatique et la cybercriminalité.

Art. 2 Planification financière

[1] Ce crédit d'investissement est ouvert dès 2016. Il est inscrit sous la politique publique H – Sécurité et population et les rubriques :
– 04.11.00.00 506001 « Informatique et télécommunications »;
– 04.11.00.00 520000 « Logiciels, application ».

[2] L'exécution de ce crédit est suivie au travers d'un numéro de projet correspondant au numéro de la présente loi.

Art. 3 Amortissement

L'amortissement de l'investissement est calculé chaque année sur la valeur d'acquisition (ou initiale) selon la méthode linéaire et est porté au compte de fonctionnement.

Art. 4 Suivi périodique

[1] Une fois l'an, les bénéficiaires du crédit d'investissement rendent compte de son utilisation à la commission du Grand Conseil qui a préavisé le projet de loi. Ce suivi porte notamment sur l'état de réalisation des projets, la consommation des ressources accordées et la planification retenue pour l'année suivante.

[2] Ce bilan conditionne la libération de la tranche prévue pour l'année suivante, selon la planification retenue.

Art. 5 Loi sur la gestion administrative et financière de l'Etat

La présente loi est soumise aux dispositions de la loi sur la gestion administrative et financière de l'Etat, du 4 octobre 2013.

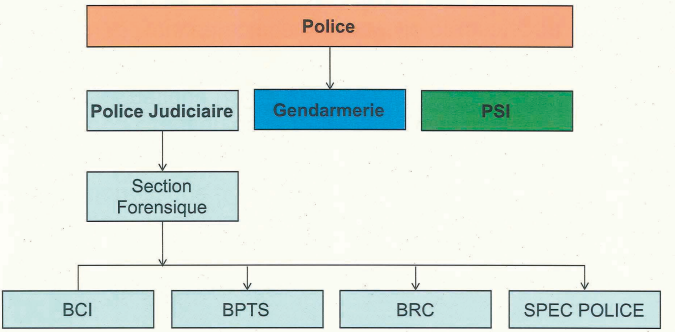
ANNEXE

PL 11788
Cybercriminalité

Agenda

- BCI
  - Organisation
  - Secteurs d'activités
- PL Cybercriminalité
  - Achats spécifiques pour enquêtes
  - Equipement des nouveaux collaborateurs
  - Application d'analyse & réseau protégé
  - Mise à niveau de l'infrastructure de stockage
  - Adaptation du SPEC

Police cantonale genevoise

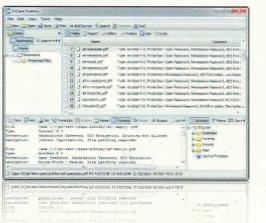


La genèse

- 1996 Première affaire
- 1998 Naissance du Groupe de Criminalité Informatique (GCI)
- 2003 Création de la Brigade de Criminalité Informatique (BCI)
- 2013 Nouveaux locaux, nouvelle organisation, etc.

Analyse de supports de données (25 %)

- Corps du métier de la BCI
- Tous types de supports
- Cloud computing



Enquêtes Internet & OSINT (33 %)

- Principale activité de la BCI
- Tabelle des phénomènes cybercrime Fedpol
- Répercussions dans d'autres domaines d'activité
- Open Source Intelligence
- Darkweb, Deepweb…
- Crypto-monnaie (Bitcoins, Dogecoins, Coince West, Biebercoin, etc.)
- Patrouilles Internet

Téléphonie mobile (19 %)

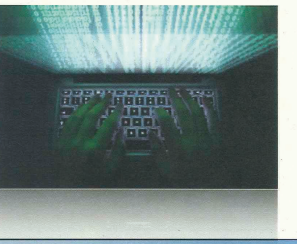
- Mobile devices :
  - Téléphones mobiles
  - Tablettes (iPad, MS Surface, etc.)
  - GPS
  - Diving computers,
  - Connected devices (Jawbones, Google & Levi's Jacquard, etc.)
- Laboratoires délocalisés
  - VHP 7ème étage
  - Brigade aéroport
- Formation continue des inspecteurs PJ
  - Cours de base XRY
  - Formation continue XRY
  - Cellebrite User Forum

Véhicules informatique embarquée (1 %)

- Intégration applicative de l'informatique dans les véhicules (voitures, bateaux, avions, etc.)
- Véhicules automatisés (Google Cars, Tesla, etc.)
- Sécurité d'un ordinateur des années '80.

Interception (3 %)

- Interception et surveillance des données cryptées
- CAJ-N => Variante « A » :
  - Centralisation de l'achat
  - Certification
  - Utilisation
- Social Engineering



Malware (3 %)

- Tabelle des phénomènes cybercrime Fedpol Let C
- Attaques en augmentation de 113 % en 2014
- Isolation du Malware, étude du comportement & destination des données
- Simplicité de mise en oeuvre
- Tout appareil connecté peut être une cible

Vidéo (10 %)

- Récupération de données vidéo
- Mise à disposition sur formats supportés
- Amélioration d'images et de sons
- Travaux sur les images (redressement, etc.)
- Détermination d'indices (taille du suspect par ex.)

PL11788

Achats spécifiques enquête

- Financement des achats nécessaires en fonction de l'actualité criminelle dont la prévision est impossible.
  - Matériel informatique (Hardware)
  - Logiciels spécifiques (Software)
  - Etc.

Equipement des nouveaux collaborateurs

- Equipement informatique et logiciel
- Matériel de corps
- Formation de base
- Etc.

Application d'analyse & Réseau protégé

- Infrastructure de mise à disposition des données extraites pour :
  - Policiers en charge de l'enquête
  - Magistrats du Ministère public
  - Tribunal des Mesures de contrainte
  - Etc.

- Mise en production d'un réseau protégé pour les affaires particulièrement sensibles (IGS, VIP, terrorisme, etc.)

Mise à niveau de l'infrastructure de stockage

- Adaptation du réseau BCI actuellement en production aux nouvelles normes et performances.

Mise en production du SPEC numérique

- La BCI fonctionne comme SPEC numérique
- Nécessité de garantir la pérennité des pièces à conviction (PAC)
- Assurer la destruction des PAC dans les délais légaux

Objectifs visés par le PL

- Adaptation aux nouvelles menaces
- Modernisation et sécurisation de l'infrastructure BCI
- Réduction du délai de traitement des pièces

Indicateurs

- Moyenne de traitement d'une pièce
- Socle de pièces « en attente »
- Taux de résolution des affaires

Merci pour votre attention

patrick.ghion@police.ge.ch