Projet présenté par le Conseil d'Etat

Date de dépôt : 16 décembre 2015

Projet de loi

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

ATAR ROTO PRESSE – 200 ex. – 01.16

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.

Certifié conforme
La chancelière d'Etat : Anja WYDEN GUELPA

EXPOSÉ DES MOTIFS

Mesdames et
Messieurs les Députés,

Contexte

La généralisation du numérique, particulièrement d'Internet, dans la vie quotidienne des entreprises et des particuliers modifie profondément les modes de fonctionnement sociaux et économiques, accélérant la mise à disposition de l'information et son accessibilité. Internet est devenu un support incontournable, ainsi que le met en évidence le taux de pénétration de l'informatique domestique et des connexions à Internet. La diffusion auprès des utilisateurs est renforcée par la multiplication des supports, notamment mobiles (smartphones, tablettes, mais également véhicules, etc.) et la multiplication des fonctionnalités accessibles par Internet et d'autres types de connexions. L'évolution en matière de trafic de paiement est particulière illustrative, qu'il s'agisse de l'e-banking et plus récemment des moyens de paiement sans contact physique (par Bluetooth et d'autres technologies).

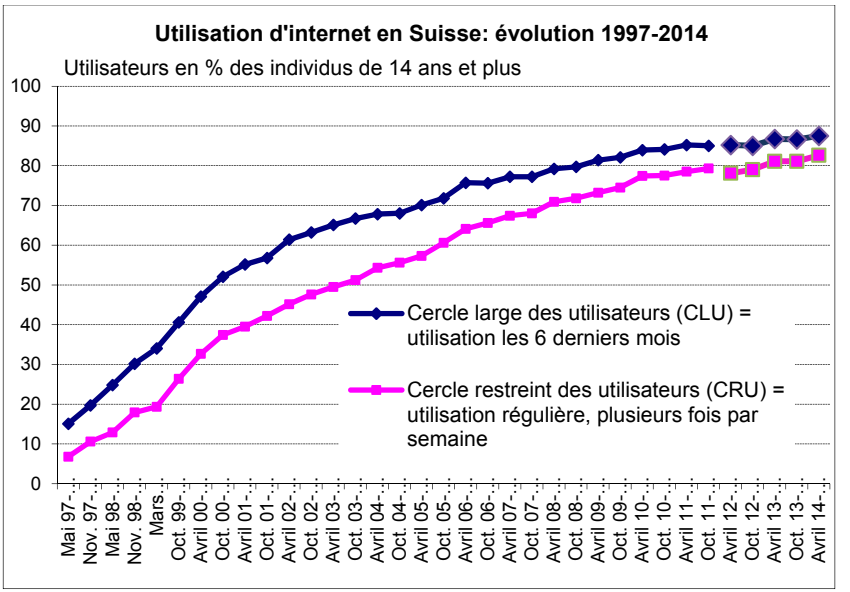
Les cibles ou les victimes potentielles de la cybercriminalité sont notamment l'ensemble des infrastructures publiques, les acteurs économiques toutes catégories et tailles confondues, et le public au sens large.

Les polices suisses ont pris la mesure de l'évolution récente de cette nouvelle forme de criminalité et tendent à regrouper leurs moyens d'investigations au sein de pôle de compétence régionaux, tout en structurant les compétences d'actions entre les autorités fédérales et les instances cantonales.

La police genevoise dispose, avec la brigade de criminalité informatique (BCI), de compétences avérées en investigations numériques. L'expérience accumulée depuis près de 10 ans en fait un pôle reconnu dans ce domaine parmi les polices suisses. L'évolution récente de la cybercriminalité exige toutefois un renforcement des moyens opérationnels à disposition. Il s'agit de renforcer les capacités d'investigations et de traitement de données numériques et de moderniser l'infrastructure informatique (hardware, software) en collaboration étroite avec la DGSI.

Evolutions récentes des technologies de l'information : quelques faits

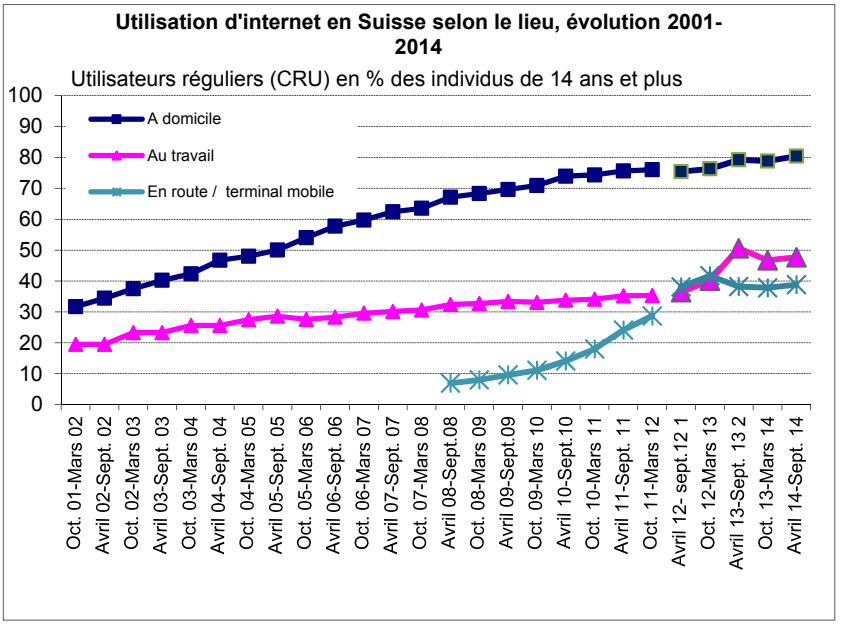
Afin d'illustrer la place désormais incontournable qu'ont prise les nouvelles technologies de l'information, voici quelques faits extraits des données de l'Office fédéral de la statistique[1].



De toute évidence, Internet a pénétré en profondeur les foyers helvétiques. Sans grande surprise, nous constatons une augmentation régulière et soutenue des utilisateurs de la toile. Plus de 87% des habitants de notre pays y accèdent plusieurs fois par semaine. L'utilisation d'Internet n'est pas l'apanage des jeunes générations. A terme, l'intégralité de la population sera connectée à Internet.

De plus, Internet mobile modifie profondément le comportement des acteurs depuis 2008. Des premiers wifi aux réseaux cellulaires de quatrième génération (4G), la capacité à échanger des données a pris un essor considérable.

[1] http://www.bfs.admin.ch/bfs/portal/fr/index/themen/16/04/key/approche_globale.html



La nouvelle forme de délinquance qui en découle s'est également développée. Les cyberattaques récentes d'entreprises de la place, le développement des cas d'escroquerie dits de « *social Engineering* » ne sont que quelques exemples des cyberrisques encourus par les acteurs économiques.

De plus, la diffusion fulgurante des technologies de l'information auprès du grand public exige désormais, dans quasi tous les domaines de l'enquête judiciaire, la mise en œuvre de capacités d'extraction et de traitement de données numériques.

A cela s'ajoute le fait que la criminalité sous toutes ses formes, y compris le terrorisme, utilise également les techniques de communication numérique qui nécessitent des moyens d'investigation adéquats.

Afin de faire face aux besoins actuels et à un horizon de 5 ans, il est impératif de renforcer les compétences de la police genevoise en matière d'investigation numérique. Il s'agit de renforcer les besoins en spécialistes et de se doter des infrastructures informatiques propres à garantir un haut degré de performance. Ce renforcement s'inscrit dans la coordination nécessaire tant au niveau suisse qu'entre les cantons concordataires (GE; VD; VS; FR; JU et

NE). Le présent projet de loi d'investissement vise à doter la police genevoise des moyens nécessaires.

Phénomènes cybercriminels

Le développement susmentionné, à la fois technologique et sociétal, génère de nouvelles menaces et de nouvelles formes de criminalité.

Selon le concept de mise en œuvre de la *Stratégie nationale de protection de la Suisse contre les cyberrisques* (SNPC): « Lorsque des actes punissables sont commis par, au moyen ou contre des technologies de l'information et de la communication (TIC), on parle de cybercriminalité ».

La distinction est faite entre la cybercriminalité au sens strict et la cybercriminalité au sens large: la cybercriminalité au sens strict concerne les actes punissables qui sont commis à l'aide des technologies de l'information et de la communication (TIC) ou qui profitent des points faibles de ces technologies. La cybercriminalité au sens large utilise Internet en tant que moyen de communication, les possibilités offertes telles que le trafic de courriels ou l'échange, respectivement la mise à disposition de données utilisées abusivement à des fins illicites.

En 2015, l'Office fédéral de la police a édité une tabelle structurelle regroupant l'ensemble des phénomènes cybercriminels recensés. Cette tabelle s'applique bien évidemment à la situation dans le canton de Genève.

Ces phénomènes sont regroupés en trois catégories d'infractions soit :

1. ***Cybercriminalité économique***
   - A. Phishing *(méthode pour obtenir des données personnelles)*
   - B. Hacking *(accès non autorisé à un système informatique tiers)*
     1. Introduction dans des sites web
     2. Défiguration de sites web
     3. Piratage de compte (hijacking)
   - C. Malware *(programme informatique qui exécute des fonctions nuisibles)*
     1. Ransomware ou crypto-Ransomware *(logiciel malveillant qui prend en otage des données personnelles)*
     2. Cheval de Troie e-banking
     3. Spyware *(logiciel espion)*
     4. Rogueware / Scareware *(faux antivirus, faux logiciel de sécurité)*

D. Botnet *(groupe d'ordinateurs qui ont été contaminés par un ou plusieurs malware)*
E. Dos / DDoS *(attaques dirigées contre un ordinateur le rendant indisponible)*
F. Cyber-escroquerie *(délits d'escroquerie commis par le biais d'Internet)*
   1. Faux ordres de virement internationaux
   2. Magasins en ligne frauduleux
   3. Fausses annonces immobilières
   4. Sociétés de transport fictives
   5. Fausses requêtes d'aide
   6. Fausses confirmations de paiement
   7. Fraude à la commission
   8. Fraude aux sentiments
G. Money & Package mules *(transfert d'argent ou de colis par un tiers)*
H. Sextorsion *(chantage au moyen d'une vidéo reproduisant des actes sexuels)*

2. Cyber-délits sexuels

A. Pornographie interdite *(représentation d'actes d'ordre sexuels avec des enfants)*
B. Grooming *(sollicitation d'enfants à des fins sexuelles par des adultes sur Internet)*

3. Cyber-atteinte à la réputation et pratiques déloyales

A. Cybersquatting *(enregistrement de noms de domaine)*

Lutte contre la cybercriminalité et la criminalité informatique : un axe de la politique criminelle 2014-**2016 convenue entre le Conseil d'Etat et le Ministère public.**

La lutte contre la cybercriminalité et la criminalité informatique constitue l'un des axes (axe n° 9) de la politique criminelle commune 2014-2016 convenue entre le Conseil d'Etat et le Ministère public et est formulée ainsi : « il convient d'accroître la lutte contre tous les types de cybercriminalité, en renforçant notamment les moyens techniques et législatifs à disposition de la police et des autorités de poursuite pénale ».

Les mesures à mettre en œuvre pour sa réalisation sont les suivantes :

– augmentation de la capacité opérationnelle de la BCI;
– renforcement de la formation des inspecteurs et de tous les policiers en matière de nouvelles technologies et de préservation des traces;
– intensification des campagnes de prévention au niveau national, concordataire et cantonal.

La coordination de la lutte contre la cybercriminalité au niveau suisse

Au niveau suisse, le Département fédéral de justice et police élabore d'ici fin 2016, en collaboration avec les cantons, un concept global de traitement des phénomènes de cybercriminalité, dans le cadre de la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques. La police judiciaire fédérale est chargée, par son service de coordination de la lutte contre la criminalité sur Internet (SCOCI), de la mise en œuvre de cette stratégie. A l'avenir, le SCOCI devrait garantir la répartition des tâches entre les instances fédérales et les moyens des polices cantonales. Il devrait également fournir des prestations renforcées en matière d'investigations en relation avec des cas de cybercriminalité particulièrement complexes.

Dans cette optique, la conférence des commandants de police des cantons suisses travaille actuellement au développement d'une stratégie policière de lutte contre la cybercriminalité dans les cantons.

Le développement de la collaboration au sein du nouveau concordat en matière de police en Suisse romande

Un nouveau concordat réglant la coopération en matière de police en Suisse romande entrera en vigueur au 1er janvier 2016. Ce concordat a notamment pour but de garantir et de promouvoir la coopération entre polices pour la réalisation de synergies opérationnelles, techniques, scientifiques et logistiques ainsi que pour la formation y relative.

Le développement d'un pôle concordataire en investigations numériques figure au rang des priorités immédiates et s'inscrit parfaitement dans les lignes directrices stratégiques développées au niveau suisse (voir supra). La centralisation des compétences spécifiques prévoit une mise en commun des ressources et le développement de synergies opérationnelles entre les cantons romands.

La brigade de criminalité informatique (BCI)

Les compétences de la police genevoise, en particulier de la BCI, sont une contribution importante à la création du pôle concordataire susmentionné. La police genevoise devra continuer, à l'instar des autres corps concordataires à disposer de compétences décentralisées. Le présent projet de loi tient compte de l'évolution du contexte national et concordataire du développement des capacités d'investigations numériques en Suisse.

Actuellement, les prestations de la BCI se placent sous deux axes :

– l'aide à l'enquête, notamment par l'analyse des supports de données numériques dans le cadre d'investigations judiciaires ordinaires ne relevant pas forcément du traitement de cybercrimes;
– les enquêtes en cybercriminalité au sens propre.

Les différentes prestations fournies par la BCI sont regroupées au sein des « laboratoires » suivants :

Laboratoires	Prestation	Volume 2014	Importance opérationnelle[2]
Internet	Enquête	33%	1
Analyse de données	Extraction, analyse	25%	1
Téléphonie mobile	Extraction, analyse	19%	1
Vidéo	Extraction, mise à disposition	10%	1
OSINT	Renseignement	6%	2
Malware	Détection, analyse	3%	2
Interceptions	Infection, renseignement, Govware	3%	2
VHC informatisés[3]	Extraction, analyse	1%	3

[2] 1 = forte, 2 = moyenne, 3 = faible
[3] Véhicule avec de l'informatique embarquée.

Ces deux dernières années, la BCI s'est incontestablement hissée en tête des cantons latins, voire sur le plan suisse dans plusieurs domaines :

– Téléphonie mobile : la BCI est l'un des deux pôles de compétences au sein des cantons suisses en matière d'analyse de téléphones mobiles. Depuis de nombreuses années, la BCI organise pour l'ensemble des cantons latins des formations et des séminaires bisannuels dans le domaine.
– Vidéo : le laboratoire vidéo et son organisation est la référence.
– Malware : la BCI a le laboratoire le plus évolué de Suisse avec un personnel hautement qualifié et dont certaines affaires d'importance nationale ont contribué à son renom.
– Interceptions : l'utilisation de chevaux de Troie et de nombreuses heures de pratique sur le terrain placent ce laboratoire parmi les plus expérimentés de Suisse. Un projet de partenariat avec la police cantonale vaudoise est également en cours en vue de mutualiser les ressources humaines et matérielles au profit de l'ensemble des cantons latins. Le projet est actuellement dans l'attente de la révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) sur laquelle travaille actuellement le Parlement fédéral.
– VHC informatisés : il s'agit de l'analyse de données contenues dans les systèmes informatiques embarqués dans les véhicules. La BCI dispose des rares compétences présentes en Suisse en la matière.

Laboratoire « Analyse de données numériques »

D'un point de vue historique, l'analyse des données numériques représente le corps du métier de la BCI.

Partant de l'analyse de disques durs, ce type d'analyse s'est peu à peu développé au rythme des avancées technologiques, passant par les différents supports tels que les clés USB, les cartes mémoire (SD, microSD, etc.) ainsi que les différents supports optiques (CD et DVD).

Il est difficile de préjuger en l'état des futurs développements techniques en la matière, mais quels que soient les développements informatiques qui interviendront dans le futur, les données numériques devront toujours être stockées soit sur un support physique soit dans le « Cloud ».

Il est évident que l'activité d'analyse servant à la récupération de données va perdurer en se diversifiant au rythme des supports proposés aux utilisateurs.

Laboratoire « Téléphonie & mobile devices »

Le laboratoire « Téléphonie & mobile devices » traite des téléphones portables, des systèmes de navigation (GPS) mobiles et de tous types de supports de données mobiles comme les ordinateurs de plongée sous-marine par exemple.

Depuis plusieurs années, la police genevoise, pionnière en la matière, a mis en place un système de formation destiné à l'ensemble des inspecteurs de police judiciaire genevois. Cette formation est également dispensée aux policiers spécialisés dans les autres cantons romands. C'est notamment sur la base de cette expérience que les polices romandes ont développé et validé leur concept de formations de base en nouvelles technologies et préservation des preuves. Ce concept prévoit une structuration des compétences sur quatre niveaux (policier de base, spécialiste I et II, expert).

Ce laboratoire BCI est en pleine croissance, non seulement du fait de la courbe des utilisateurs de téléphones mobiles, particulièrement de smartphones, mais également en raison du nombre de plus en plus important d'objets dits « connectés ».

Laboratoire « Enquêtes Internet & OSINT (Open Source Intelligence) »

Les enquêtes Internet représentent une part importante et grandissante dans l'activité du travail de la BCI. En 2014, 36% du volume des affaires traitées relevaient des enquêtes Internet et OSINT.

Si la plupart des affaires ne requièrent que peu de compétences techniques s'agissant de l'identification des adresses IP, il en va autrement des affaires plus complexes dont la variété est infinie.

Le développement de compétences en matière de « Open Source Intelligence (OSINT) » est indispensable à la conduite d'investigations dans de multiples pans de l'activité criminelle. Il s'agit notamment de développer des compétences et des processus de travail propres à recueillir et à traiter des renseignements dans le « dark web », soit des informations non référencées par les moteurs de recherche usuels.

Laboratoire « Vidéo »

Les affaires impliquant les systèmes de vidéosurveillance ont connu un essor considérable ces deux dernières années.

La généralisation de la présence de systèmes de vidéosurveillance et de vidéo-protection privés et publics est une source importante d'indices et d'informations recueillis dans le cadre d'investigations judiciaires dans tous les

domaines de l'activité criminelle; les récents événements l'ont prouvé. La police doit donc disposer d'outils d'analyse d'image performants et validés sous l'angle de la traçabilité forensique, garantissant la non-altération de la source d'origine, au profit des enquêteurs et du pouvoir judiciaire.

L'évolution technologique dans ce domaine est permanente. L'absence complète de standards techniques des fabricants implique le développement de compétences larges et pointues pour le traitement des données vidéo. La BCI doit en outre disposer de capacités de stockage et de traitements importants pour satisfaire aux besoins grandissant des enquêteurs.

Laboratoire « Malware »

Selon un article publié sur ALP-ICT[4] les attaques par Ransomware ont augmenté de 113% en 2014. Parmi ceux-ci, il faut mentionner les « maliciels » qui cryptent les données des victimes les obligeant à payer une somme d'argent pour récupérer leurs fichiers.

Toute personne privée ou entreprise se connectant à Internet devient une cible privilégiée de criminels internationaux en matière de malware.

Il faut rappeler que, si cette forme de criminalité était autrefois réservée à des ingénieurs ou à des techniciens férus d'informatique, il est aujourd'hui aisé de télécharger, y compris pour des utilisateurs non spécialisés, des applications gratuites permettant le paramétrage et la mise en œuvre de « malwares ».

La BCI a développé des compétences propres et avérées pour le traitement et l'analyse de ces « maliciels ».

Laboratoire « Interception »

Le domaine très technique des interceptions consiste à surveiller les conversations audio et data cryptées. Concrètement, les conversations de personnes utilisant des systèmes de messagerie instantanées (ex : WhatsApp, Skype) ne peuvent plus être entendues par les systèmes d'écoute classique. Un nombre grandissant d'activités criminelles se déroulent en utilisant des moyens de télécommunication cryptés, notamment dans le domaine du trafic de stupéfiants, du grand banditisme, mais aussi de la délinquance ordinaire pratiquée en bande, sans parler du terrorisme. Il est nécessaire d'avoir recours à des « govwares » (Government Software) capables d'intercepter les conversations avant ou après leur encodage par le système de messagerie. L'engagement de tels chevaux de Troie utilisé par différentes organisations

[4] http://blog.alpict.com/2015/04/22/les-attaques-par-ransomware-ont-augmente-de-113-en-2014.

gouvernementales est complexe et requiert des compétences spécialisées dont dispose la BCI.

Elle collabore avec les cantons concordataires afin de développer le maximum de synergies dans ce domaine et de regrouper les compétences.

Laboratoire « Informatique embarquée »

La raison d'être du laboratoire informatique embarquée s'explique par le fait que les véhicules comprennent de plus en plus de composants informatiques.

Ces systèmes font aujourd'hui partie des équipements standards et contiennent des données pertinentes en matière d'investigations judiciaires. Il ne fait aucun doute que les constructeurs automobiles vont encore développer ces systèmes.

Par ailleurs, l'analyse de l'informatique embarquée ne concerne pas uniquement les voitures. Les systèmes de gestion électronique des motos, des aéronefs, des bateaux entre autres peuvent également fournir des informations essentielles dans le cadre d'une enquête judiciaire. La BCI a déjà eu l'occasion de mener des investigations dans ce contexte.

Autres potentiels de développements de la BCI

La brigade devra toujours évoluer et s'adapter aux nouvelles menaces technologiques. Il est donc impératif qu'elle dispose d'une capacité de veille technologique pour faire face aux requêtes nouvelles des enquêteurs confrontés à l'évolution de la cybercriminalité. Le développement d'un pôle régional en matière d'investigations numériques devra fournir les conditions propres à dégager les synergies les plus efficaces en la matière au sein des polices suisses et romandes en particulier.

Risques identifiés

Plusieurs risques ont été identifiés dans le fonctionnement actuel de la brigade de criminalité informatique, soit :

1. ***Plusieurs volets de la lutte contre la cybercriminalité ne sont maîtrisés que par une seule personne***

Les laboratoires « Vidéo », « Malware », « Interception » et « Informatique embarquée » reposent sur les compétences et l'expérience d'un seul collaborateur par domaine. Cela ne permet pas de garantir la prestation opérationnelle attendue dans la durée, ni la diligence de traitement des affaires.

2. Le personnel actuellement disponible ne permet pas d'assurer une veille technologique adéquate

Le domaine de la cybercriminalité évolue rapidement et requiert une forte capacité de veille technologique. Le développement de synergies de collaboration intercantonale devrait contribuer à assouvir ce besoin. Il n'en demeure pas moins que la mise à niveau permanente des connaissances nécessite une formation continue et une veille technologique assidues.

3. Les délais de traitement importants peuvent conduire à l'échec d'une affaire

« *Le temps qui passe, c'est la vérité qui fuit* » est un adage policier des plus explicites. C'est également vrai dans le domaine de l'investigation numérique. Les enquêteurs des brigades doivent pouvoir bénéficier à temps des analyses et des traitements de données fournies par les spécialistes de la BCI. Actuellement, les inspecteurs de la BCI priorisent le traitement des affaires en fonction de l'urgence et de l'importance. Il n'en demeure pas moins que le nombre moyen d'affaires en attente s'élève à environ 70.

4. Des infrastructures informatiques obsolètes et saturées

Les infrastructures actuelles demandent une mise à jour. En l'état actuel, elles font encourir des risques avérés pouvant entraver le fonctionnement des investigations pénales, ainsi que le traitement forensique et le stockage des données récoltées.

Augmentation des effectifs de la BCI

Les besoins de développement de la capacité d'investigation numérique de la police passent par le renforcement de la capacité opérationnelle de la BCI. La police doit disposer d'un pôle de compétence avéré, inscrit dans le contexte du développement de la lutte contre la cybercriminalité au niveau suisse et dans la mise en œuvre du concordat réglant la coopération en matière de police en Suisse romande.

Le renforcement prévu des effectifs policiers est de 7 ETP d'ici 2019. Cela permettra de consolider et de pérenniser les compétences (3 ETP) et de réduire le délai de traitement des affaires (4 ETP). L'augmentation de l'effectif de la BCI se fera par une réaffectation des postes au sein de la police judiciaire. Il n'y a donc pas de nouveaux postes.

Besoins d'investissement et coûts induits liés à l'augmentation de l'effectif de la BCI

Ainsi, à l'horizon 2019, la police devra équiper ses collaborateurs de manière adéquate. Le policier de cette brigade n'a pas un PC standard mais une station de travail forensique équipée généralement de trois écrans et de lecteurs d'interfaces multiples. Elle a la particularité d'être paramétrable pour chaque utilisateur selon le domaine spécifique : traitement du son, de la téléphonie, de l'image, etc. Son contenu est également très différent car des logiciels très pointus sont utilisés pour les traitements des sources multimédias qui sont analysées.

Investissement d'équipement des nouveaux collaborateurs : 150 000 F

Les achats pour les enquêtes spécifiques couvrent l'acquisition de nouveaux logiciels et de matériel nécessaires pour mener à bien certaines investigations nécessitant des moyens informatiques particuliers. Il s'agit de pouvoir exploiter les nouvelles technologies et de suivre les évolutions imposées par les fabricants, que ce soit en termes de changement de format des supports numériques comme par exemple les cartes SIM (devenues au fil du temps mini puis nano), les connecteurs des appareils téléphoniques ou de formats de stockage, comme c'est le cas notamment dans le domaine de la vidéo.

Achats pour enquêtes spécifiques : 160 000 F

Les coûts induits (budget de fonctionnement) correspondent aux licences des logiciels informatiques. Ils sont réévalués chaque année en fonction du nombre de collaborateurs. Pour les 4 prochaines années, le coût annuel est estimé à 100 000 F.

Investissements en matière d'infrastructure de stockage et de modernisation des serveurs

L'infrastructure de stockage de la BCI doit être à la pointe de la technologie et doit être sécurisée pour traiter les données et le faire dans la plus grande confidentialité. Une nouvelle architecture sera mise en place pour garantir la pérennité, pouvoir supporter une croissance importante des volumes à traiter (la taille des fichiers vidéos, avec les nouveaux équipements offrant non seulement la haute définition HD mais désormais le 4K, croît de manière exponentielle) et augmenter la performance. Il est important de rappeler que le principal objectif est de rechercher une trace numérique. Vu la nécessité de considérer tous les liens avec cette trace, la quantité d'informations numériques à traiter est en croissance continue et le traitement de ces informations

volumineuses ne doit pas se faire au détriment de la rapidité d'obtention des résultats vitaux pour l'avancement de l'enquête.

Infrastructure de stockage moderne et performante : 500 000 F

Cette estimation est le fruit d'une étude menée par un bureau d'ingénierie, spécialisé dans ce type de demande, réalisée cette année. Par ailleurs, de nouveaux serveurs spécifiques à la BCI vont être mis en place pour bénéficier des dernières évolutions, notamment en gain de vitesse de traitement et de sécurité des systèmes.

Les coûts induits de cette partie pour les 4 ans : 200 000 F

Mise à disposition des données saisies au Ministère public et pièces à conviction numériques

La police, en particulier la BCI, doit pouvoir décrypter et analyser les données saisies en masse dans le cadre d'une enquête. Une application doit être mise en place pour permettre le décryptage, l'indexation, la recherche, l'extraction et l'analyse de données numériques non structurées. L'application offrira un accès au Ministère public adapté selon les cas :

– dans une affaire classique, le travail de recherche est effectué par la police et les éléments jugés utiles sont mis à la disposition du Ministère public;
– dans une affaire complexe, l'ensemble des données sont mises à disposition du Ministère public qui, lui, effectue les recherches en fonction de ses besoins;
– en cas de tri lors d'une demande de levée de scellés, les données saisies sont traitées pour prendre en compte la protection du secret professionnel (art. 271 CPP).

Un réseau protégé permettant la consultation, le transfert et l'échange sécurisé de données entre le Ministère public et la police sera déployé par la DGSI.

Application de décryptage, d'analyse et de recherche numérique ainsi que réseau protégé : 270 000 F

Le service des pièces à conviction (SPEC) doit pouvoir gérer non seulement les pièces courantes, mais également l'ensemble des fichiers numériques et assurer la gestion des copies et la destruction en fin d'utilisation des éléments non retenus dans le jugement qui eux seront archivés.

La BCI doit adapter l'application actuelle pour les pièces numériques. Celles-ci proviennent soit de copies effectuées à partir de pièces physiques

(supports tels que clés USB, disques durs, etc.), soit à partir de données provenant de sources immatérielles (ex. OSINT – Open Source Intelligence).

Les pièces à conviction physiques sont copiées de façon forensique et stockées sur les serveurs de la BCI. La DGSI effectue une copie de sauvegarde des données numériques sur un serveur parallèle. Une fois le traitement des données numériques terminé, ces données sont archivées.

Adaptation de l'outil de gestion des pièces à conviction : 120 000 F

Les coûts induits de l'application de recherche, le réseau sécurités et l'outil de gestion des pièces à conviction sont estimés, pour 4 ans, à 150 000 F.

En résumé, le présent projet de loi sollicite un crédit d'investissement global de **1 200 000 F** pour les années 2016-2019, réparti comme suit :

– Equipement de nouveaux collaborateurs : 150 000 F
– Achats spécifiques pour enquêtes : 160 000 F
– Infrastructure de stockage : 500 000 F
– Application de décryptage, d'analyse et de recherche numérique, réseau : 270 000 F
– Adaptation du SPEC : 120 000 F

La répartition prévue par année est la suivante :

Année	2016	2017	2018	2019	TOTAL
Police					
Achats spécifiques enquêtes	40 000	60 000	40 000	20 000	**160 000**
DGSI					
Equipement des nouveaux collaborateurs sur 4 ans	37 500	37 500	37 500	37 500	**150 000**
Application de décryptage, d'analyse et de recherche numérique ainsi que réseau protégé	100 000	170 000			**270 000**
Mise à niveau infrastructure de stockage	200 000	200 000	100 000		**500 000**
Adaptation du SPEC	40 000	60 000	20 000		**120 000**
TOTAL	**417 500**	**527 500**	**197 500**	**57 500**	**1 200 000**

Le chiffrage de ces coûts d'investissement et de fonctionnement a été soumis à l'expertise d'une société externe qui a procédé à une revue qualité.

Ce projet prend en compte les remarques formulées dans le cadre de cette analyse

Retour sur investissement

Le développement de la brigade de criminalité informatique va avoir un impact significatif sur le traitement des affaires de cybercriminalité au sein du canton de Genève. Si un quelconque impact financier est difficilement chiffrable, l'amélioration sensible du service à la population, que ce soit les personnes privées ou les entreprises de la place ne fait aucun doute.

Les objectifs visés par l'évolution de la lutte contre la criminalité informatique au sein du canton de Genève sont de trois ordres :

– **Adaptation aux nouvelles menaces.** Si le niveau technique du personnel de la brigade de criminalité informatique est aujourd'hui reconnu, l'évolution des techniques et l'arrivée sans cesse de nouvelles menaces nécessitent une adaptation permanente du profil de prestation, dans le cadre du réseau de pôles de compétences appelé à se développer au niveau suisse et concordataire. Il est également nécessaire de renforcer la pérennité des savoirs et des compétences en renforçant l'effectif des spécialistes dédiés à la lutte contre la cybercriminalité.
– **Modernisation et sécurisation de l'infrastructure BCI.** L'évolution des nouvelles technologies et le vieillissement des installations actuelles nécessitent une mise à jour et un développement afin de permettre un travail efficace tout en assurant une sécurité optimale des données traitées et des processus de travail en investigations numériques.
– **Réduction du délai de traitement des pièces.** Les données numériques doivent être traitées dans un délai favorisant la résolution des enquêtes.

Indicateurs

Actuellement, le système de gestion des affaires traitées à la BCI permet d'établir que la moyenne de traitement d'une pièce non urgente s'effectue sur une durée de 4 mois. Par ailleurs, la BCI enregistre un socle constant de 70 à 80 pièces. Un indicateur permettra de suivre l'effet de l'augmentation des effectifs sur ces délais de traitement, et ce pour les différents domaines du traitement des données numériques. De même, des indicateurs en matière de taux de résolution d'affaires de cybercriminalité pourront être élaborés.

Risques liés au projet

L'évaluation des risques actuels, liés à l'obsolescence des infrastructures numériques, susceptibles d'entraver non seulement l'acquisition de renseignements numériques dans le cadre des investigations pénales, mais aussi le traitement forensique et le stockage des données récoltées a été fait d'entente avec la DGSI. A cet égard, les mesures préconisées et demandées dans le cadre du présent projet de loi correspondent à la minimisation des risques identifiés par la DGSI.

Les risques émanant de l'augmentation du personnel policier de la BCI sont maîtrisés. La planification de l'augmentation de personnel permet de tenir compte du développement des pôles de compétences au niveau concordataire et de l'évolution de la cybercriminalité à court terme. Elle permet également d'absorber les augmentations d'effectifs tout en garantissant la capacité opérationnelle de la brigade.

Au bénéfice de ces explications, nous vous remercions, Mesdames et Messieurs les Députés, de réserver un bon accueil au présent projet de loi.

Annexes :

1) *Préavis financier (art. 30 RPFCB – D 1 05.04)*
2) *Planification des dépenses et recettes d'investissement du projet (art. 31 RPFCB – D 1 05.04)*
3) *Planification des charges et revenus de fonctionnement du projet (art. 31 RPFCB – D 1 05.04)*

ANNEXE 1

REPUBLIQUE ET
CANTON DE GENEVE

PREAVIS FINANCIER

Ce préavis financier ne préjuge en rien des décisions qui seront prises en matière de politique budgétaire.

1. Attestation de contrôle par le département présentant le projet de loi

- Projet de loi présenté par le département de la sécurité et de l'économie.
- Objet : Projet de loi ouvrant un crédit d'investissement de 1 200 000 F pour la lutte contre la criminalité informatique et la cybercriminalité.
- Rubrique(s) budgétaire(s) concernée(s) : 04.11.00.00 natures 506001 et 520000
- Politique(s) publique(s) concernée(s) : H Sécurité et population
- Coût total du projet d'investissement : 1'200'000 F

Dépenses d'investissement	1'200'000
- Recettes d'investissement	0
= Investissements nets	**1'200'000**

- Coût total du fonctionnement lié :

Charges liéesde fonctionnement	558'000
- Revenus liés de fonctionnement	0
= Impacts nets sur les résutats annuels	**558'000**

- Planification pluriannuelle de l'investissement :

(en mios de F)	2015	2016	2017	2018	2019	2020	2021	2022	Total
Dépense brute	**0.0**	**0.4**	**0.5**	**0.2**	**0.1**	**0.0**	**0.0**	**0.0**	**1.2**
Recette brute	***0.0***	***0.0***	***0.0***	***0.0***	***0.0***	***0.0***	***0.0***	***0.0***	***0.0***
Invest. net	**0.0**	**0.4**	**0.5**	**0.2**	**0.1**	**0.0**	**0.0**	**0.0**	**1.2**

- Planification des charges et revenus de fonctionnement liés et induits :

☒ oui ☐ non Les tableaux financiers annexés au projet de loi intègrent la totalité des impacts financiers découlant du projet.

(en mios de F)	2015	2016	2017	2018	2019	2020	2021	Dès 2022
NET LIE et INDUIT	0.00	-0.01	-0.17	-0.29	-0.40	-0.44	-0.44	-0.44

- Planification financière (modifier et cocher ce qui convient) :

☒ oui ☐ non Le crédit d'investissement sera ouvert dès 2016, conformément aux données des tableaux financier.

☒ oui ☐ non Les charges et revenus de fonctionnement liés et induits de ce projet seront inscrits au projet de budget de fonctionnement 2017.

☐ oui ☒ non Le crédit d'investissement et les charges et revenus de fonctionnement liés et induits de ce projet sont inscrits au plan financier quadriennal 2016-2025.

☒ oui ☐ non Ce projet génère des charges de fonctionnement induites nécessaires à sa réalisation (ces charges n'étant pas comprises dans la demande de crédit du présent projet de loi, elles doivent faire l'objet d'une inscription annuelle au budget de fonctionnement). Ces éléments seront inscrits au projet de budget 2017.

☐ oui ☒ non Autre(s) remarque(s) : ce crédit d'investissement est inscrit au plan décennal des investissement 2016-2025, sous réserve de l'arbitrage du Conseil d'Etat.

Le département atteste que le présent projet de loi est conforme à la loi sur la gestion administrative et financière de l'Etat (LGAF), à la loi sur les indemnités et les aides financières (LIAF), au modèle comptable harmonisé pour les cantons et les communes (MCH2) et aux procédures internes adoptées par le Conseil d'Etat.

Genève, le : 14.12.15 Signature du responsable financier du département investisseur : Dominique RITTER DIRECTEUR DU SERVICE FINANCIER

Genève, le : 14.12.15 Signature du responsable financier du département utilisateur : Dominique RITTER . DIRECTEUR DU SERVICE FINANCIER

2. Approbation / Avis du département des finances

☐ oui ☒ non Remarque(s) complémentaire(s) du département des finances : _____

Genève, le : 14.12.2015 Visa du département des finances :

N.B. : Le présent préavis financier est basé sur le PL, son exposé des motifs, les tableaux financiers et ses annexes transmis le 7 décembre 2015.

1. PLANIFICATION DES DEPENSES ET RECETTES D'INVESTISSEMENT DU PROJET

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

Projet présenté par le département de la sécurité et de l'économie

(montants annuels, en mios de F)		2016	2017	2018	2019	2020	2021	2022	TOTAL
Dépenses d'investissement		0.4	0.5	0.2	0.1	0.0	0.0	0.0	1.2
Recettes d'investissement		*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Investissement net	Durée	0.4	0.5	0.2	0.1	0.0	0.0	0.0	1.2
Informatique - Corporel	5 ans	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.2
Recettes	5 ans	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Informatique (DGSI) - Postes de t	5 ans	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.2
Recettes		*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Informatique (DGSI) - Eqpmts spe	6 ans	0.3	0.4	0.1	0.0	0.0	0.0	0.0	0.8
Recettes		*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*
Informatique (DGSI) - Application	8 ans	0.0	0.1	0.0	0.0	0.0	0.0	0.0	0.1
Recettes		*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*	*0.0*

Remarques :

Date et signature direction financière (investisseur) :

14.12.15 Dominique RITTER DIRECTEUR DU SERVICE FINANCIER

Date et signature direction financière (utilisateur) :

14.12.15 Dominique RITTER DIRECTEUR DU SERVICE FINANCIER

2. PLANIFICATION DES CHARGES ET REVENUS DE FONCTIONNEMENT DU PROJET

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

Projet présenté par le département de la sécurité et de l'économie

(montants annuels, en mios de F)	2016	2017	2018	2019	2020	2021	2022	dès 2023
TOTAL charges liées et induites	0.01	0.17	0.29	0.40	0.44	0.44	0.44	0.44
Charges en personnel [30]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Biens et services et autres charges [31]	0.00	0.15	0.19	0.21	0.21	0.21	0.21	0.21
Charges financières	0.01	0.02	0.10	0.20	0.23	0.23	0.23	0.23
Intérêts [34] 2.125%	0.01	0.02	0.02	0.03	0.03	0.03	0.03	0.03
Amortissements [33 + 366 - 466]	0.00	0.00	0.07	0.17	0.21	0.21	0.21	0.21
Subventions [363 + 369]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Autres charges [30 à 36]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL revenus liés et induits	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Revenus [40 à 46]	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
RESULTAT NET LIE ET INDUIT	-0.01	-0.17	-0.29	-0.40	-0.44	-0.44	-0.44	-0.44
RESULTAT NET LIE	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
RESULTAT NET INDUIT	-0.01	-0.17	-0.29	-0.40	-0.44	-0.44	-0.44	-0.44

Remarques :

Date et signature direction financière (investisseur) :

14.12.15 Dominique RITTER DIRECTEUR DU SERVICE FINANCIER

Date et signature direction financière (utilisateur) :

14.12.15 Dominique RITTER DIRECTEUR DU SERVICE FINANCIER