KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internetkriminalität
Service de coordination de la lutte contre la criminalité sur Internet
Servizio di coordinazione per la lotta contro la criminalità su Internet
Cybercrime Coordination Unit Switzerland

Service de coordination de la lutte contre la criminalité sur Internet

Rapport annuel 2013

SCOCI – 10 ANS

Service de coordination de la lutte contre la criminalité sur Internet (SCOCI)
Nussbaumstrasse 29
3003 Berne
www.scoci.ch
www.cybercrime.ch

Publié le: 27 mars 2014

Photographie: Thinkstock, SCOCI

AVANT-PROPOS

de Monsieur le Conseiller d'Etat Christoph Neuhaus,
Président du comité directeur du SCOCI

"Rien n'est permanent, sauf le changement", disait déjà le philosophe grec Héraclite. En persévérant on arrive à tout, et celui qui n'avance pas, recule. Ces petites maximes bien connues de tous s'appliquent particulièrement bien au SCOCI. Tout d'abord parce qu'une année Internet correspond, comme l'indique une étude réalisée par le site ibusiness.de, à quatre années de la vie réelle. Ensuite parce que le SCOCI dispose désormais de dix ans d'expérience dans ce domaine. Il s'agit pour lui de rester visionnaire et novateur comme à ses débuts et de continuer à regarder vers l'avenir.

Aujourd'hui, plus de huit Suisses sur dix naviguent plusieurs fois par semaine dans le World Wide Web. De nouveaux champs d'activité et terrains d'engagement font leur apparition chaque jour. Tant le policier que le juriste y sont confrontés. A l'heure actuelle, notre police et notre justice disposent des ressources nécessaires pour assurer, dans la vie réelle, la sécurité de huit millions de personnes. Mais que se passe-t-il si 2,7 milliards de personnes provenant du monde entier s'ajoutent en un clic de souris? Et, même si tous les utilisateurs d'Internet ne sont de loin pas malintentionnés, comment gérer la situation quand ce chiffre atteindra 3,5 milliards d'internautes en 2017, comme le prévoit Europol?

En 2013, un "botnet" (réseau de machines zombies) a été découvert, qui avait ceci de particulier: un quart des ordinateurs infectés qu'il contrôlait étaient en fait des objets, et plus précisément des télévisions, réfrigérateurs et autres appareils électroménagers. Alors que se passera-t-il en 2020 lorsque 200 milliards de ces objets seront connectés à Internet? Quel sera l'impact pour chacun d'entre nous? Quelles seront les conséquences sur la place économique suisse ou pour les autorités de poursuite pénale? En passant du service de renseignement à la Police judiciaire fédérale, le SCOCI s'est implanté au niveau international en tant que partenaire à part entière des autorités d'enquête telles que l'agence *European Cybercrime Center* d'Europol (EC3) ou l'*Interpol Global Complex for Innovation* (IGCI) à Singapour. Les bases d'une coopération internationale efficace en matière de lutte contre cette nouvelle forme de criminalité sont posées. La Suisse dispose du savoir-faire, des ressources et des conditions optimales pour relever ce défi.

Sur le plan fédéral, le SCOCI soumettra au Conseil fédéral d'ici fin 2016 un concept découlant de la mesure 6 (vue d'ensemble des cas et coordination de cas complexes intercantonaux) de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC M6). D'une part, le défi consiste à trouver une solution satisfaisante pour tous et financièrement viable afin de lutter de façon optimale contre la cybercriminalité organisée, et ce dans un contexte où les coupes budgétaires sont monnaie courante. D'autre part, il s'agit de définir une répartition des tâches entre les autorités de poursuite pénales fédérales et cantonales, de sorte à ce que le projet ne soit pas remis en cause pour des raisons d'attribution. Il importe de ne pas laisser passer la chance que représente le projet SNPC M6 pour nous tous, et cela malgré l'importance que nous donnons au fédéralisme. Car c'est le fédéralisme lui-même que nous cherchons à protéger par ces mesures.

La prochaine décennie représente un grand challenge pour le SCOCI: il devra se pencher sur des questions de fond et relever d'importants défis. Nul doute qu'il le fera avec l'engagement qu'on lui connaît, avec toute son énergie et son esprit visionnaire, toujours tourné vers le futur (numérique).

Table des matières

1. L'essentiel en bref

- En 2013, le SCOCI a reçu au total 9208 annonces par le biais de son formulaire en ligne. Cela représente une augmentation de 11,7 % par rapport à l'année précédente.

- 61 % des annonces concernaient des infractions contre le patrimoine, lesquelles ont continué à augmenter par rapport aux infractions contre l'intégrité sexuelle. Ainsi, la tendance observée l'année précédente se poursuit en 2013.

- Dans 356 cas, la pertinence pénale de l'annonce a permis de transmettre directement une dénonciation à des autorités ou organisations nationales ou internationales.

- La recherche active sur les réseaux *peer-to-peer* (P2P) a permis au SCOCI d'identifier en 2013 238 utilisateurs échangeant de la pédopornographie.

- Des investigations préliminaires secrètes et des enquêtes menées par le SCOCI en vertu du code de procédure pénale (CPP) ont abouti en 2013 à 17 dénonciations aux autorités cantonales compétentes et à 176 dénonciations aux autorités de poursuite pénale étrangères.

- Le SCOCI a commencé avec succès les travaux de mise en œuvre de la mesure 6 de la Stratégie nationale de protection de la Suisse contre les cyberrisques. Pendant l'année sous revue, il a réalisé une analyse détaillée du projet et a défini l'organisation du projet.

- Le 22 décembre 2013, en marge de son 10ème anniversaire, le SCOCI a créé deux nouveaux canaux de communication avec l'ouverture de ses comptes Facebook (www.facebook.com/scoci.ch) et Twitter (@KOBIK_Schweiz).

2. Rétrospective: le SCOCI a 10 ans

2000–2002: naissance d'un projet

En juin 2000, la Conférence des commandants des polices cantonales de Suisse (CCPCS) institue un groupe de travail intercantonal[1] (GT BEMIK) chargé de procéder à un examen approfondi des qualifications et des conditions-cadres pour la création d'une cellule nationale de monitoring et de formuler des propositions concrètes à cette fin. Face aux besoins urgents en matière de coordination policière, le GT BEMIK, sous la direction d'Adrian Lobsiger (aujourd'hui directeur suppléant de fedpol) propose une série de mesures concrètes et recommande à l'unanimité la mise sur pied d'un service national de coordination en matière de cybercriminalité.

Au début de l'année 2001, s'appuyant sur les recommandations du GT BEMIK, le Département fédéral de justice et police (DFJP) et la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) décident de lutter conjointement contre la criminalité sur Internet. Le mandat, l'organisation et le financement d'un service national de coordination sont définis dans le cadre d'une convention administrative.

Le comité et le plénum de la CCDJP se prononcent à l'unanimité pour la mise en œuvre de la convention administrative. Par lettre du 4 février 2002, le président de la CCDJP invite les cantons à inscrire les montants nécessaires à leur budget 2003. Tous les cantons, à l'exception du canton de Zurich, confirment par la suite leur participation au projet. Pour sa part, le 20 février 2002, le Conseil fédéral réaffirme son intention de mettre sur pied avec les cantons, à compter du 1er janvier 2003, un centre national de coordination afin de lutter plus efficacement contre la cybercriminalité (SCOCI).

1er janvier 2003: coup d'envoi

Le SCOCI commence ses activités le 1er janvier 2003 par la mise en place d'un formulaire d'annonce quadrilingue sur Internet (cf. ci-contre). Outre ce formulaire, le site www.cybercrime.admin.ch contient également des informations de fond sur le SCOCI et sur la criminalité sur Internet en général. Le lancement du SCOCI rencontre un large écho médiatique, notamment de la part des médias électroniques et de la presse spécialisée dans les technologies de l'information. Plusieurs articles de fond et interviews permettent ensuite d'en donner une image plus complète. Au terme de ses six premiers mois d'activité, un communiqué de presse consacre le lancement réussi du SCOCI.

[1] GT BEMIK = groupe de travail chargé de la lutte contre les abus dans le domaine des technologies de l'information et de la communication

Mai 2003: début de la recherche active

Début mai, le service de coordination lance le monitoring Internet en mettant tout particulièrement l'accent sur les réseaux P2P. La première étape consiste à rechercher les fichiers illégaux mis à disposition par des utilisateurs disposant d'une adresse IP suisse. Après avoir achevé les travaux préliminaires, le cas est transmis sous la forme d'une dénonciation au canton compétent.

9 janvier 2004: publication du 1er rapport annuel du SCOCI

Le premier rapport d'activité retrace brièvement l'historique du SCOCI, la constitution du comité directeur et le recrutement de l'équipe du SCOCI. Il comprend par ailleurs des données statistiques, accompagnées de commentaires, sur les annonces et la recherche active. On constate que 6457 annonces ont été reçues du public au cours de la première année et que la recherche active (monitoring) a permis de préparer 100 dénonciations à l'intention des cantons.

2004: première réorganisation

Afin de renforcer et d'unifier la conduite de l'équipe du SCOCI, décision est prise de transférer au Service d'analyse et de prévention (SAP) le service Clearing du SCOCI, jusque-là rattaché à la Police judiciaire fédérale (PJF).

2005: rattachement à la Section MELANI / Cybercrime

L'intégration organisationnelle du Clearing SCOCI s'est achevée avec le regroupement des domaines Analyse et Clearing du SCOCI et de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) au sein de la nouvelle Section MELANI / Cybercrime. Suite à l'adhésion du canton de Zurich, l'équipe de monitoring s'est agrandie d'un collaborateur et comporte désormais neuf personnes.

2005–2006: intensification du travail de prévention

Dans le cadre de la campagne de prévention lancée en 2005 "Stop pornographie enfantine", le SCOCI collabore étroitement avec la Prévention suisse de la criminalité (PSC) et participe à différents colloques et formations. Ces activités ont finalement conduit à la création du projet de blocage des systèmes de noms de domaine en 2007. Le SCOCI est également devenu partenaire du programme de prévention "Security for Kids" de Microsoft Suisse.

2006: Accord avec la police nationale de la Principauté de Liechtenstein

Selon l'accord conclu avec la police nationale de la Principauté de Liechtenstein, le SCOCI fournit depuis 2006 des prestations en faveur de la Principauté.

2007: mise en place du projet de blocage des systèmes de noms de domaine

Depuis 2007, les sites de pédopornographie sont bloqués en Suisse à l'aide du logiciel de filtrage "Child Sexual Abuse Anti-Distribution Filter". Le projet est fondé sur une coopération volontaire entre le SCOCI et les principaux fournisseurs d'accès à Internet (FAI) du pays. Le SCOCI s'engage à fournir aux FAI une liste actualisée des sites Internet publiant des contenus pédopornographiques constituant une infraction pénale. La liste est établie sur la base des annonces de la population. De leur côté, les FAI bloquent les sites en question sur la base de leurs conditions générales.

2007: nouveau record de communication

La cinquième année de service du SCOCI est marquée par une nette augmentation des annonces émanant de la population. Le SCOCI accomplit en 2007 un énorme travail de tri portant sur plus de 10000 annonces reçues et affirme son rôle d'interlocuteur national en matière de criminalité sur Internet. Cette nette augmentation du nombre d'annonces est due à une forte hausse des cas relevant de la criminalité économique et à quelques citoyens actifs qui pour certains ont envoyé plusieurs dizaines de communications par mois. La direction du SCOCI tire un bilan positif de ces cinq dernières années: en tant que centre de compétence national, le SCOCI possède les instruments nécessaires pour faire face aux défis du futur.

2008: changement au sein du SCOCI

Différentes adaptations ont lieu en 2008, dans la structure du personnel et dans l'équipement technique, en vue de la prochaine intégration du SCOCI à la Police judiciaire fédérale. L'infrastructure informatique est modernisée et complétée par des acquisitions de matériel et de logiciels supplémentaires.

2009: intégration à la Police judiciaire fédérale

Au 1er janvier 2009, MELANI et le SCOCI sont séparés. Ce dernier est intégré à la Police judiciaire fédérale auprès de fedpol alors que MELANI, intégrée au SAP de fedpol, rejoint le Service de renseignement de la Confédération (SRC) nouvellement créé. De par son intégration à la PJF, le SCOCI assume désormais de plus en plus de tâches opérationnelles et policières, notamment la coordination d'enquêtes nationales et internationales et l'échange d'informations de police judiciaire. Cette évolution a nécessité diverses adaptations dans l'organisation et dans la politique du personnel. Il a également été décidé de fusionner les commissariats Monitoring et Clearing conduits séparément jusque-là pour les réunir au sein du nouveau commissariat SCOCI.

2010–2011: renforcement de la recherche active

Le SCOCI renforce ses capacités en matière de recherche active, ce qui se traduit par une augmentation des dénonciations remises aux cantons. En 2010, le SCOCI consacre beaucoup de ressources aux investigations secrètes.

A partir du 1er janvier 2011, la plupart des polices cantonales se retrouvent contraintes de renoncer à enquêter de manière secrète et préventive sur des pédocriminels lorsqu'elles ne disposent pas d'élément de soupçon, car leur loi cantonale sur la police ne constitue pas une base légale suffisante. Cette carence dans les lois cantonales est apparue lors de l'entrée en vigueur du nouveau code de procédure pénale (CPP).

Certains cantons comme Schwyz, Argovie et Obwald avaient identifié ces lacunes à temps et avaient adapté en conséquence leur loi sur la police au 1er janvier 2011. De son côté, le DFJP a trouvé une solution avec la CCDJP qui a permis au SCOCI, en s'appuyant sur une nouvelle base légale, d'étendre ses activités de monitoring sur Internet au domaine de la pédocriminalité. Grâce à une convention passée avec le Département de la sécurité du canton de Schwyz, le SCOCI est en mesure, à la demande des cantons, d'effectuer des investigations secrètes préventives et ainsi de surveiller les forums de discussion à partir du 1er janvier 2011. Le travail dans le domaine des investigations secrètes du SCOCI est encore basé, en 2013, sur le droit policier du canton de Schwyz et sur une autorisation du tribunal des mesures de contrainte de ce même canton. Nous avons ainsi la garantie que les pédocriminels ne puissent profiter d'aucun vide juridique sur Internet.

2011: Collection nationale de fichiers et de valeurs de hash (CNFVH)

Depuis plusieurs années, l'ancien groupe de travail Banque de données d'images (rebaptisé par la suite "groupe de travail CNFVH") travaillait à la création d'une collection nationale d'images et de valeurs de hash concernant le matériel pédopornographique. Après la reprise du projet en 2010 par le SCOCI, ce projet rebaptisé "Collection nationale de fichiers et de valeurs de hash (CNFVH)" connaît d'importants progrès en 2011. Les corps de police cantonaux sont instruits avec succès et les premiers lots d'images des archives cantonales livrés au SCOCI.

2011–2012: Stratégie nationale de cyberdéfense (appelée par la suite "Stratégie nationale de protection de la Suisse contre les cyberrisques")

Le SCOCI siège depuis mai 2011 au sein de l'équipe de projet de la Stratégie nationale de cyberdéfense et représentera également, lors de la mise en œuvre de la stratégie, les intérêts des autorités de poursuite pénale cantonales et nationales.

Le 27 juin 2012, le Conseil fédéral approuve la Stratégie nationale de protection de la Suisse contre les cyberrisques. Avec cette stratégie, le Conseil fédéral, en collaboration avec les autorités, les milieux économiques et les exploitants d'infrastructures critiques, compte réduire les cyberrisques auxquels tous ces acteurs sont exposés quotidiennement. La fin de la période de mise en œuvre est prévue en 2017.

Janvier 2012: Convention du Conseil de l'Europe sur la cybercriminalité

En ratifiant la Convention du Conseil de l'Europe sur la cybercriminalité, la Suisse s'engage à intensifier sa participation à la lutte internationale contre la criminalité informatique. Le Conseil fédéral a fixé au 1er janvier 2012 l'entrée en vigueur de cette convention et des modifications législatives nécessaires.

Octobre 2012: mise en service de la CNFVH

La collection nationale de fichiers et de valeurs de hash (CNFVH) est en service depuis octobre 2012. Tous les tests et adaptations du système ont pu être achevés avec succès.

Décembre 2012: la Suisse rejoint la Global Alliance against Child Sexual Abuse Online

La conseillère fédérale Simonetta Sommaruga, accompagnée de collaborateurs du SCOCI en qualité d'experts, s'est rendue à Bruxelles pour négocier l'adhésion de la Suisse à cette Global Alliance.

Janvier 2013: European Cybercrime Center auprès d'Europol

Depuis 2011 déjà, le SCOCI est un membre actif des projets CYBORG et TWINS d'Europol. Ces deux projets, classés thèmes majeurs par Europol, relèvent de l'agence *European Cybercrime Center* (EC3), qui a entamé ses activités le 1er janvier 2013.

Depuis 2011, le SCOCI est membre des projets Focal Points CYBORG et TWINS d'Europol. Ces deux "Focal Points"[2] relèvent de l'agence *European Cybercrime Center* (EC3), qui a entamé ses activités le 1er janvier 2013. Sis auprès d'Europol à La Haye, le centre de lutte contre la criminalité sur Internet EC3 fournit un support opérationnel aux Etats de l'UE et met à disposition ses connaissances spécialisées dans le cas d'enquêtes menées conjointement à l'échelle communautaire. Ses collaborateurs se concentrent sur la criminalité organisée en ligne. Le centre cible tout spécialement ses activités sur la lutte contre l'exploitation sexuelle des enfants sur Internet et contre les délits financiers. En outre, les attaques contre les infrastructures sensibles et les systèmes d'information font aussi partie de ses domaines d'intervention. Le rôle du centre consiste enfin à établir des analyses et des évaluations permettant de déceler les menaces à temps et de les déjouer.

2013: début de la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques

Dans le cadre de la mise en œuvre de la mesure 6 de la Stratégie nationale de protection de la Suisse contre les cyberrisques, le DFJP a pour tâche, en collaboration avec les cantons, d'élaborer d'ici à fin 2016 un concept dont le but est de "garantir la vue d'ensemble des cas et coordonner les cas complexes intercantonaux". Ce concept porte aussi sur la définition d'interfaces avec d'autres acteurs dans le domaine de la réduction des cyberrisques, sur la coordination avec la présentation de la situation et sur les ressources et les adaptations juridiques – tant au niveau de la Confédération qu'à celui des cantons – qui sont nécessaires pour le concrétiser. En 2013, nous avons déjà pu procéder à une analyse du projet et à la définition de l'organisation du projet.

[2] Les "Focal Points" sont des divisions au sein d'Europol qui se consacrent spécialement à la coordination et l'analyse de cas internationaux complexes. Elles ont été constituées à partir des anciens AWF (Analysis Work File).

Décembre 2013: lancement des comptes Facebook et Twitter

Le 22 décembre 2013, le SCOCI ouvre deux nouveaux canaux d'information avec la création de ses comptes Facebook et Twitter.

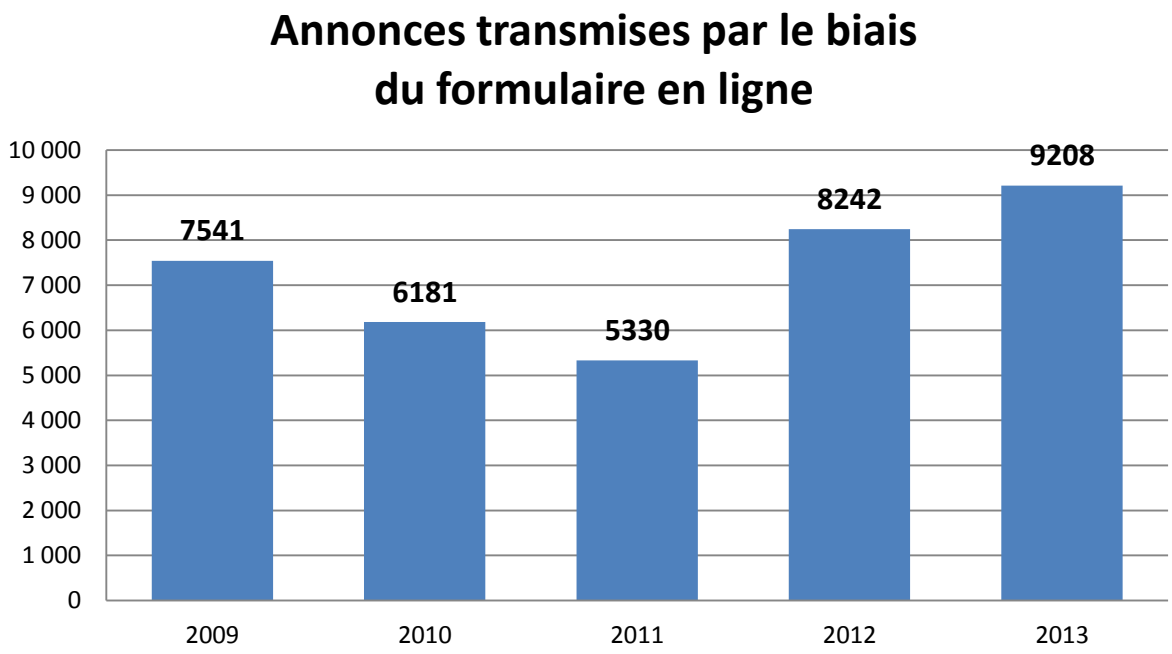
3. Le SCOCI comme interlocuteur

Le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) est l'interlocuteur principal des personnes souhaitant signaler l'existence de contenus suspects sur Internet. Les annonces, qui parviennent au SCOCI par le biais du formulaire en ligne (www.cybercrime.ch) et peuvent donner lieu à des poursuites pénales, font l'objet d'un premier contrôle et d'une sauvegarde des données avant d'être transmises aux autorités de poursuite pénale compétentes en Suisse et à l'étranger.

3.1. Nombre d'annonces reçues

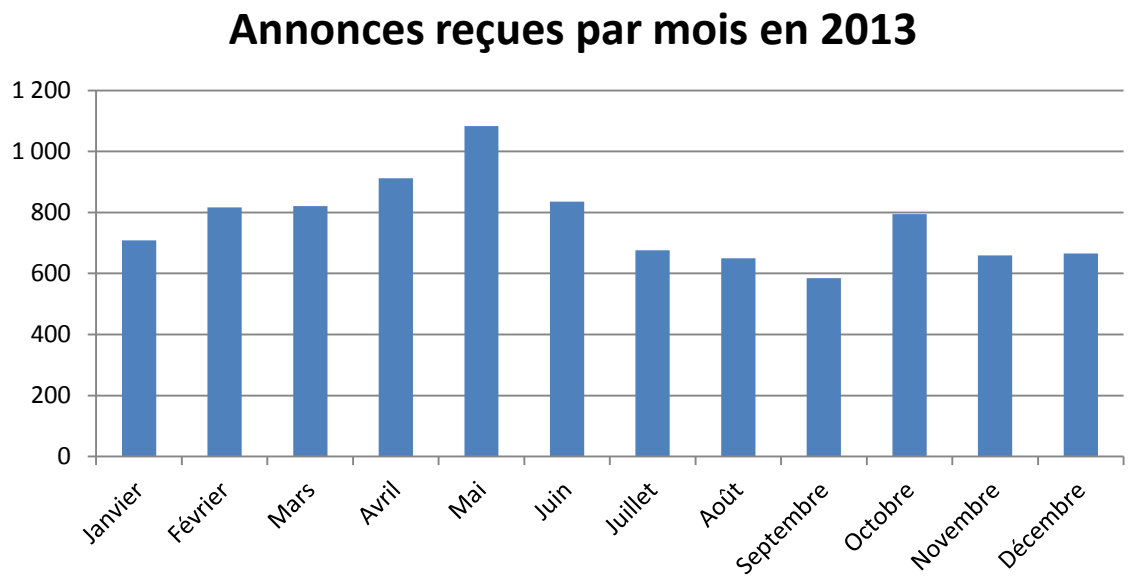
Entre le 1er janvier 2013 et le 31 décembre 2013, le SCOCI a reçu au total 9208 annonces par le biais de son formulaire en ligne sur le site www.cybercrime.ch. Cela correspond à une augmentation de 11,7 % par rapport à l'année précédente (8242 annonces).

Le nombre d'annonces reçues ne permet pas de tirer de conclusions pertinentes quant à l'augmentation ou la diminution de la criminalité sur Internet ou des contenus illégaux sur Internet. Il ne reflète que la perception de la criminalité sur Internet par la population et sa volonté de communiquer activement ses soupçons aux autorités.



Graphique 1: annonces reçues par année, par le biais du site www.cybercrime.ch

En moyenne, le SCOCI a reçu 767 annonces par mois. On constate néanmoins de fortes variations entre mai (1083 entrées) et septembre (585 entrées). Ces fluctuations s'expliquent par des événements concrets et limités dans le temps, par exemple la publication d'une annonce dans la presse par le SCOCI.



Graphique 2: annonces reçues par mois, par le biais du site www.cybercrime.ch (total: 9208 annonces)

3.2. Types d'infractions enregistrées

86 % des annonces reçues en 2013 (7910 annonces) se sont avérées pertinentes du point de vue du code pénal. Les autres annonces concernent entre autres des infractions à la LCD[3] (290 annonces), à la LDA[4] (24 annonces), au CC[5] (40 annonces), à la LStup[6] (14 annonces) et à la LBA[7] (7 annonces). Dans environ 10 % des cas annoncés, le contenu n'était pas punissable.

Les affaires annoncées peuvent être classées en deux catégories. Dans la catégorie criminalité sur Internet au sens strict, on classe les infractions commises à l'aide des technologies d'Internet ou qui utilisent des points faibles de ces technologies. Il s'agit par exemple d'actes de piratage informatique, d'attaques de déni de service distribué (DDoS) ou de création et de mise en circulation de logiciels malveillants. Toutes ces infractions pénales ne sont possibles que depuis l'existence d'Internet ou ne visent que ces technologies. La criminalité sur Internet au sens plus large comprend l'utilisation abusive d'Internet comme moyen de communication, par exemple dans le cadre de l'échange de courrier électronique ou de données à des fins illégales. On peut citer à ce titre l'envoi massif de pourriels, les arnaques sur les plateformes de petites annonces ou la distribution de pornographie illégale.

De nombreux états de fait rapportés ne sont pas poursuivis d'office et requièrent par conséquent une dénonciation pour déclencher une procédure. Dans ce genre de cas, le SCOCI renvoie les auteurs de l'annonce vers les services de police cantonaux compétents en la matière.

---

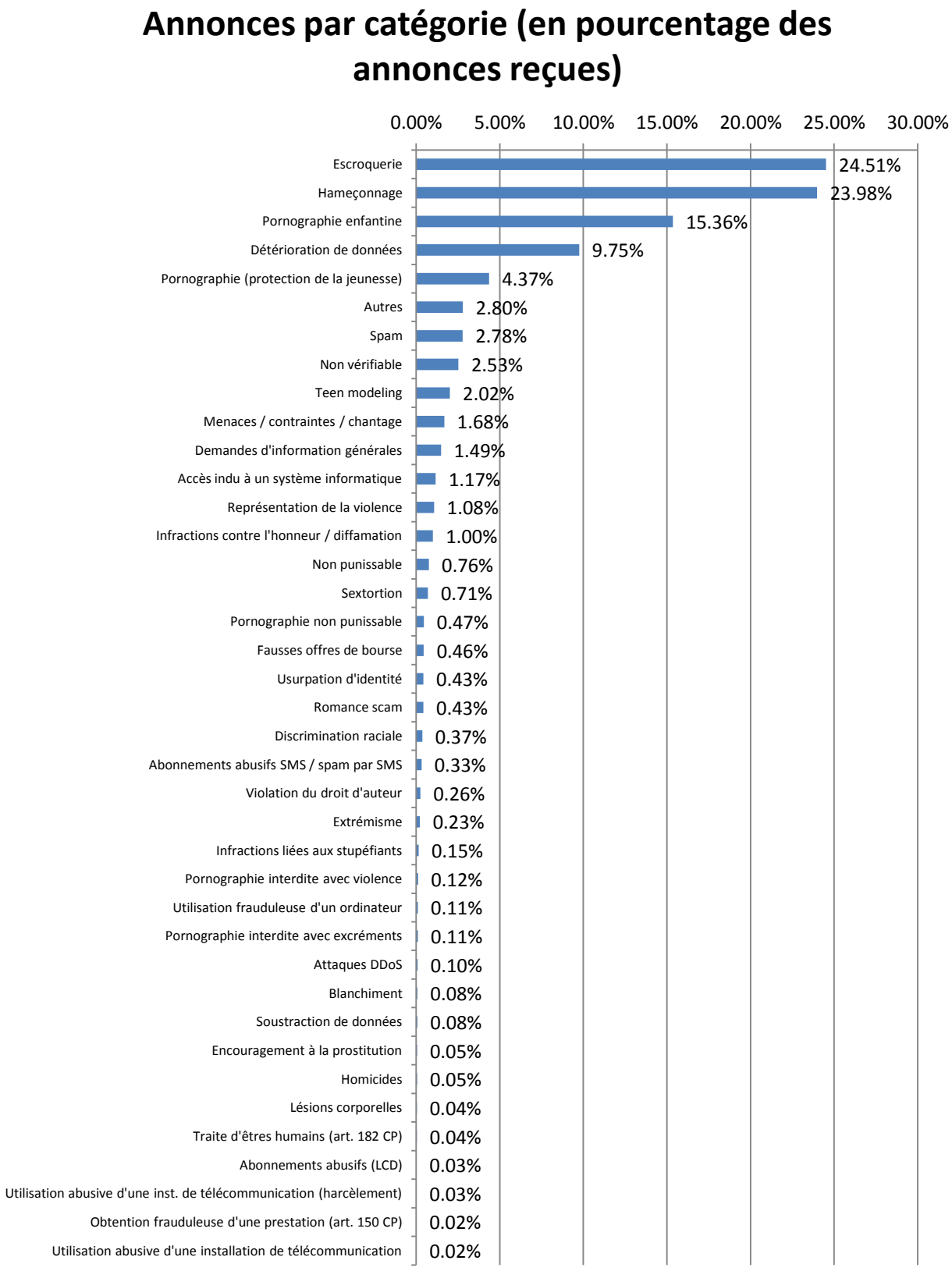
[3] Loi fédérale du 19 décembre 1986 contre la concurrence déloyale, RS 241

[4] Loi fédérale du 9 octobre 1992 sur le droit d'auteur et les droits voisins (LDA), RS 231.1

[5] Code civil suisse du 10 décembre 1907, RS 210

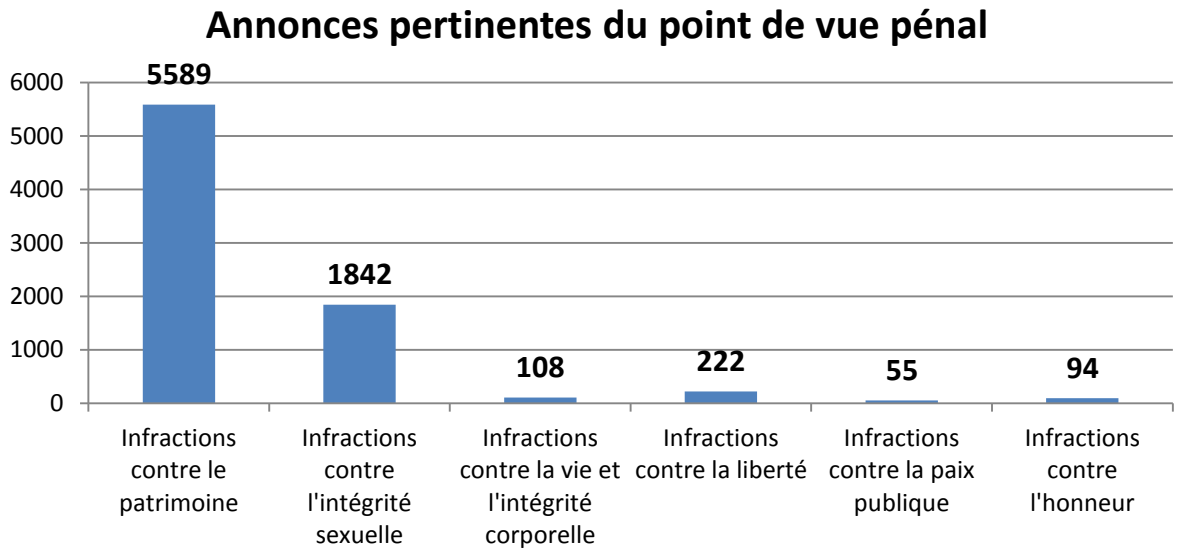
[6] Loi fédérale du 3 octobre 1951 sur les stupéfiants et les substances psychotropes, RS 812.121

[7] Loi fédérale du 10 octobre 1997 concernant la lutte contre le blanchiment d'argent et le financement du terrorisme dans le secteur financier, RS 955.0

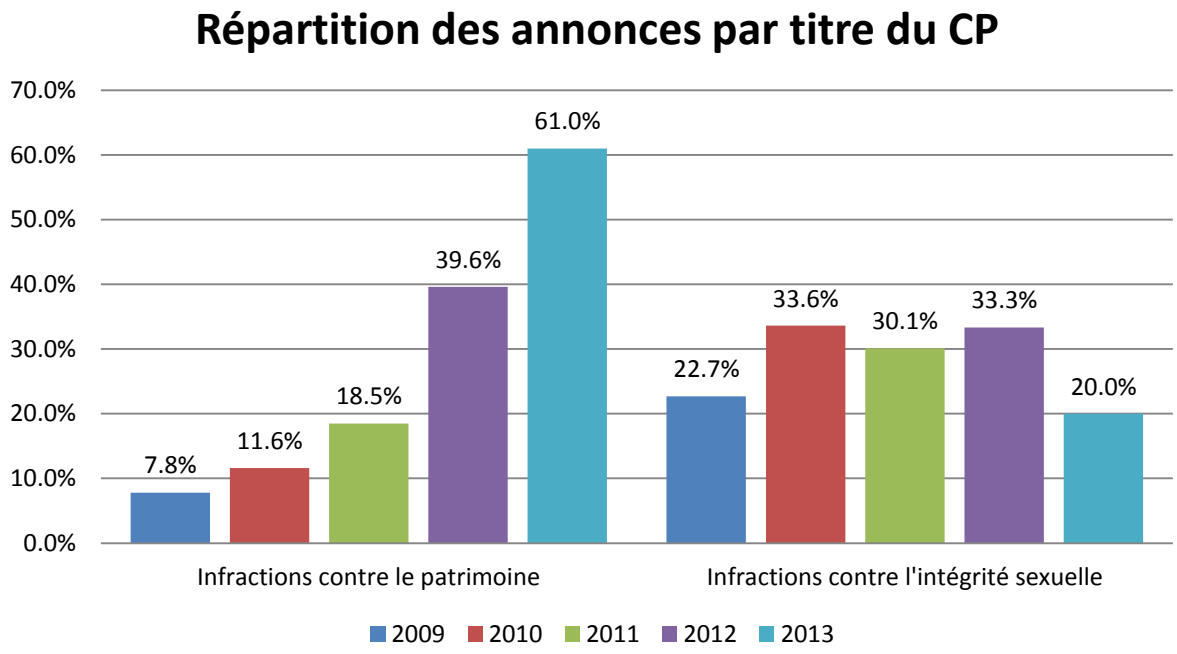


Graphique 3: importance des catégories sur l'ensemble des annonces reçues en 2013

La tendance à l'augmentation des annonces relatives aux infractions contre le patrimoine s'est confirmée en 2013. Au total 60,7 % des annonces reçues concernent ce type d'infraction (art. 137 à 172ter CP). En deuxième position avec 20 % des annonces reçues figurent les infractions contre l'intégrité sexuelle (art. 187 à 212 CP). Cela correspond à une forte diminution de 40,3 % en comparaison avec l'année précédente.

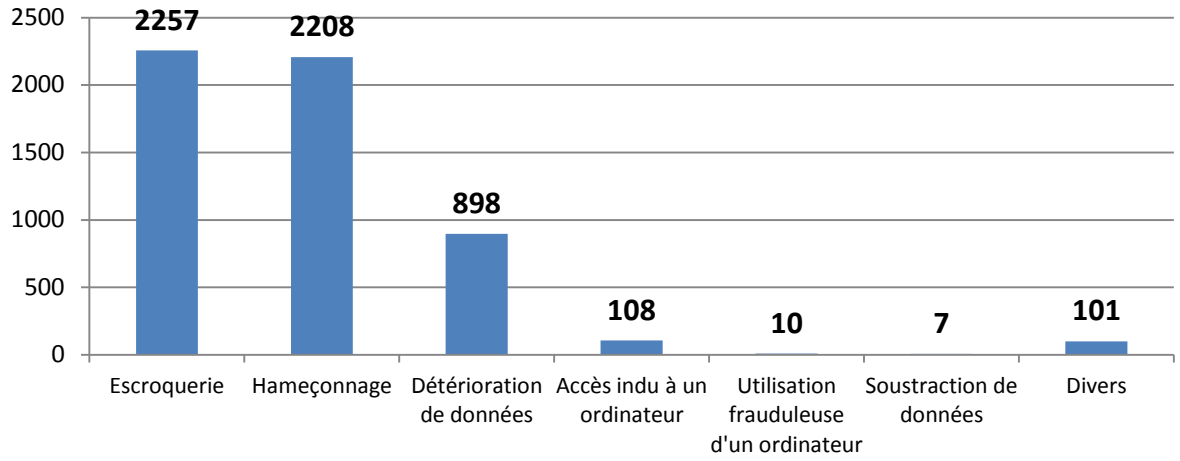


Graphique 4: annonces reçues en 2013, classées par catégorie d'infraction pénale (total: 7910)



Graphique 5: répartition des annonces de 2009 à 2013

3.2.1. Infractions contre le patrimoine



Graphique 6: annonces reçues concernant des infractions contre le patrimoine (total: 5589)

Au cours de l'année sous revue, les infractions contre le patrimoine sont les plus fréquemment annoncées avec un total de 5589, soit 60,7 %. La sous-catégorie "Escroquerie" représente à elle seule 2257 annonces, soit 25 % du volume total des annonces. Les types d'escroquerie sont multiples.

Les annonces concernant des tentatives d'escroquerie sur des sites de vente aux enchères ou de petites annonces ont augmenté. Sur ces sites, les auteurs d'infractions visent tant les vendeurs que les acheteurs, c'est-à-dire aussi bien les personnes intéressées par les produits que les annonceurs. On constate que les escrocs s'efforcent de rendre de plus en plus crédibles leurs tentatives d'escroquerie, par exemple en allant jusqu'à créer des sites web complets d'entreprises de transport fictives, comprenant même un faux système de suivi des paquets afin de faire croire le plus longtemps possible à la victime que la marchandise envoyée ou commandée est encore en route. Les auteurs sont particulièrement bien informés des habitudes en Suisse et mettent ces informations à profit. Par exemple, ils exploitent habilement la pénurie de logements dans les agglomérations en publiant de fausses annonces afin d'appâter les locataires à la recherche d'appartements bon marché dans les régions de Zurich et de Bâle, puis exigent des paiements d'avance pour des biens qui en fait n'existent pas.

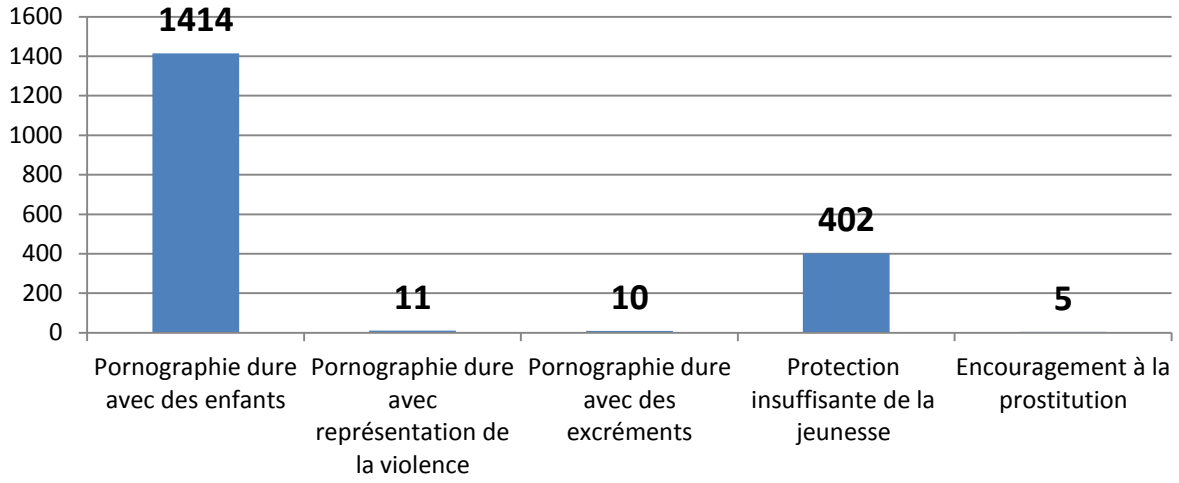
Les tentatives d'hameçonnage ont quant à elles augmenté de manière spectaculaire. Avec un total de 2208 annonces reçues, elles ont plus que triplé par rapport à l'année précédente (662). Les variantes les plus utilisées qui sont mentionnées dans les annonces consistent à envoyer massivement des courriels à des victimes potentielles, sans ciblage particulier, et à essayer de les attirer sur des sites web s'inspirant de services Internet connus, où les victimes doivent indiquer leurs données d'utilisateur (nom d'utilisateur, mot de passe). Environ un cinquième des annonces reçues pour l'hameçonnage concernait des tentatives d'obtention de données de connexion à des services d'instituts bancaires suisses.

Dans le domaine de la criminalité sur Internet au sens strict, on constate une nouvelle augmentation des annonces de plus de 20 % en comparaison avec l'année précédente. L'augmentation des annonces concernant la détérioration des données (898 annonces, +124 %) est significative.

Dans le domaine de la détérioration des données, le modus operandi le plus souvent dénoncé consistait à introduire de manière organisée, mais non ciblée, des logiciels malveillants dans l'ordinateur de particuliers ou d'entreprises. Les rançongiciels (combinaison de rançon et de logiciel) – ransomware en anglais – sont un exemple de ce type de logiciel malveillant. Une fois l'ordinateur infecté, ces logiciels bloquent l'ordinateur de la victime et exigent le paiement d'une rançon en échange du déblocage de la machine. La rançon est payée sous forme de bons échangeables sur des sites de paiement anonyme en ligne. Dans la deuxième moitié de l'année, ce sont les annonces en relation avec une nouvelle variante de rançongiciel (appelé "CryptoLocker") qui ont augmenté. Celui-ci rend les données présentes sur un ordinateur inutilisable en procédant à leur chiffrement. De cette manière, la pression pour le paiement de la rançon est encore plus forte.

Les PME sont de plus en plus touchées par des attaques ciblées contre leurs publications sur Internet et leurs infrastructures de télécommunication. Les auteurs pénètrent sans autorisation dans les systèmes modernes de téléphonie numérique (VoIP) afin d'effectuer des appels longue distance vers l'Afrique ou l'Amérique du Sud, avec pour corollaire des surplus de frais de télécommunication se chiffrant en dizaines de milliers de francs. D'autres attaques visent les données des clients telles qu'adresses e-mail, numéros de téléphone ou données de facturation, accessibles par les failles de sécurité présentes dans les sites web des sociétés. Bien que ce dernier type d'attaque ne cause pas de dommages financiers directs, il occasionne des frais de sécurisation des données, de réinstallation d'éventuelles copies de sauvegarde et de suppression des failles de sécurité utilisées. De plus, ces attaques ont souvent pour conséquence une perte de confiance de la clientèle, un dommage très difficile à chiffrer en termes financiers. De plus, les données volées sont le plus souvent utilisées pour d'autres variantes d'escroquerie, par exemple pour construire des identités fictives ou prendre le contrôle de comptes e-mail dans le but d'envoyer des courriels frauduleux (par ex. fraude à la commission).

3.2.2. Infractions contre l'intégrité sexuelle

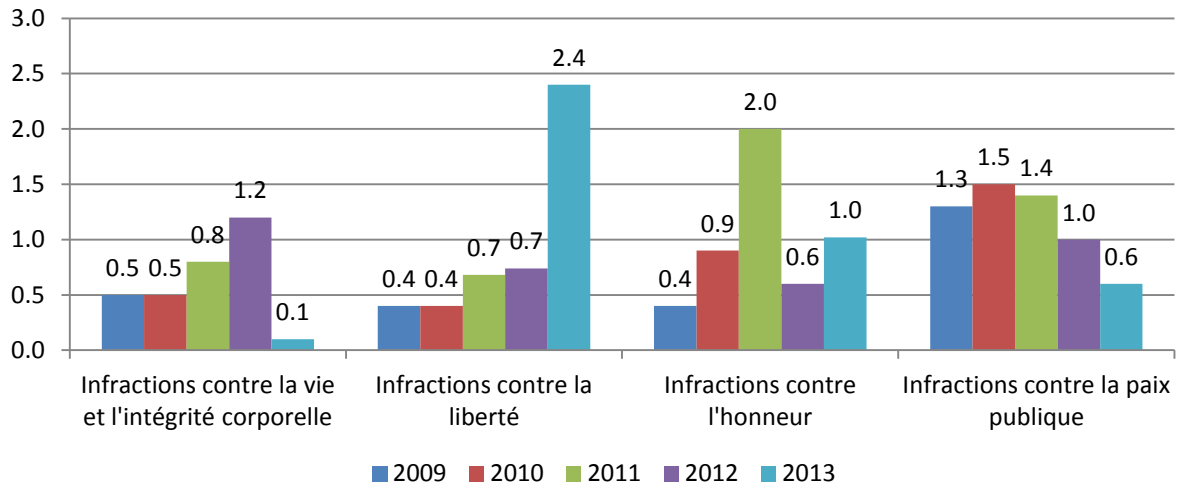


Graphique 7: annonces reçues concernant des infractions contre l'intégrité sexuelle (total: 1842)

Le nombre d'annonces concernant des infractions contre l'intégrité sexuelle a diminué de presque 40 % en 2013, passant de 3083 annonces en 2012 à 1842 annonces en 2013. Dans 402 cas (307 en 2012), le SCOCI a été rendu attentif à des sites avec des contenus pornographiques dont l'auteur de l'annonce estimait qu'ils étaient trop facilement accessibles aux jeunes.

Le nombre de sites web signalés contenant de la pornographie enfantine a fortement diminué, passant de 2684 en 2012 à 1414 en 2013 (-47 %).

3.2.3. Autres infractions



Graphique 8: annonces reçues entre 2009 et 2013 concernant d'autres titres du CP (en pourcentage de l'ensemble des annonces)

Environ 4 % du volume des annonces concernent d'autres infractions prévues dans le code pénal: il s'agit des infractions contre la vie et l'intégrité corporelle, contre la liberté, contre la paix publique et contre l'honneur. Au total, 2,4 % des annonces reçues en 2013 portaient sur des infractions pénales contre la liberté. Les annonces évoquent pour la plupart des cas où des personnes sont invitées, par un interlocuteur le plus souvent féminin et par le biais de sites de rencontre ou des réseaux sociaux, à effectuer des actes de nature sexuelle devant la caméra de leur ordinateur. Peu après, les auteurs prennent contact avec la victime et exigent de l'argent en échange de leur silence, faute de quoi ils publieront la vidéo compromettante sur Internet. Cette année aussi, le nombre d'infractions contre l'honneur est resté relativement bas. Comme en 2012, nous ne constatons pas de tendance à la hausse pour cette catégorie sur la base des annonces reçues.

3.2.4. Synthèse

Le nombre d'annonces concernant des infractions contre le patrimoine a augmenté d'un tiers en 2013, confirmant la tendance de l'année précédente. Dans le même temps, le nombre d'annonces relatives aux infractions contre l'intégrité sexuelle a diminué d'un tiers. Désormais, les catégories "Hameçonnage" et "Escroquerie" dépassent le volume total des annonces liées aux titres du CP relatifs aux infractions contre l'intégrité sexuelle.

3.3. Résultats des activités du SCOCI

Le SCOCI a entrepris différents travaux et pris des mesures sur la base des annonces qu'il a reçues par le biais du formulaire en ligne. Voici une vue d'ensemble des chiffres et informations essentiels:

- Chacune des 9208 annonces reçues a été examinée dans les délais impartis afin de déterminer sa pertinence du point de vue pénal.

- Dans 3457 cas sur 9208, les auteurs de l'annonce ont reçu une réponse personnelle.

- 35 annonces ont, en raison de leur pertinence pénale, conduit directement à la transmission d'une dénonciation à l'autorité ou au canton compétent.

- 321 annonces concernant des sites web au contenu pénalement répréhensible ont été transmises aux autorités de poursuite pénale étrangères (par le biais d'Interpol ou d'Europol) ou à des organisations affiliées (par ex. *inhope*).

- De nombreuses annonces ont par ailleurs conduit à la transmission interne d'indices au Commissariat Criminalité générale, organisée et financière et au Commissariat Pédocriminalité et pornographie de la Police judiciaire fédérale (PJF).

- Les faits les plus signalés ont donné lieu à la publication d'un total de neuf alertes sur le site www.cybercrime.ch géré par le SCOCI. Grâce à la transmission de ces alertes à MELANI, à la Prévention suisse de la criminalité (PSC) et aux médias, une large frange de la population est informée des dangers actuels.

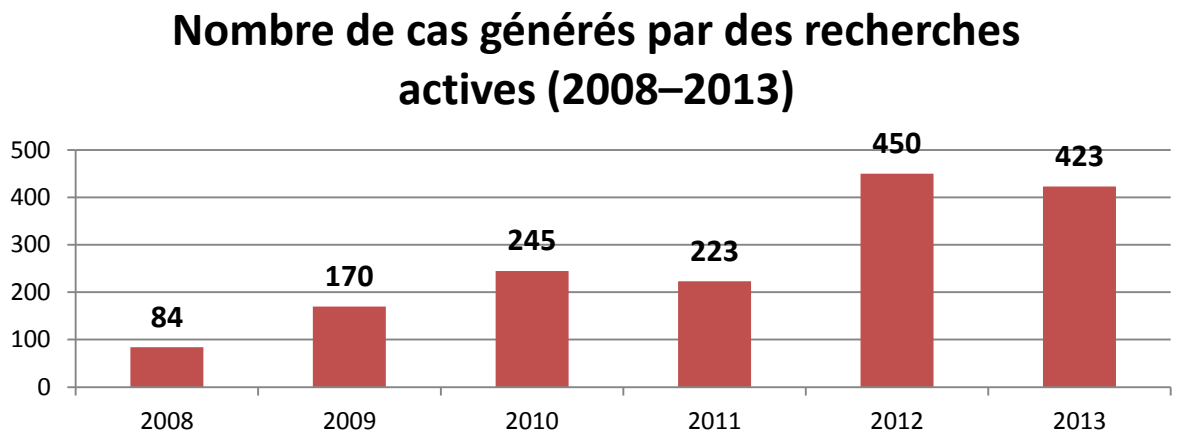
3.4. Exemple de cas

Le SCOCI a été contacté par un fournisseur d'hébergement suisse qui avait constaté que des inconnus utilisaient ses services pour exploiter un magasin en ligne commercialisant des données de cartes de crédit volées. Les informations volées ainsi que les fichiers de journal ont été livrés volontairement par le fournisseur. Le SCOCI a transmis ces données à Europol, qui les a confiées à l'agence *European Cybercrime Center* (EC3) pour effectuer les analyses techniques des données et contacter les instituts bancaires concernés dans le but de faire bloquer les cartes de crédit compromises.

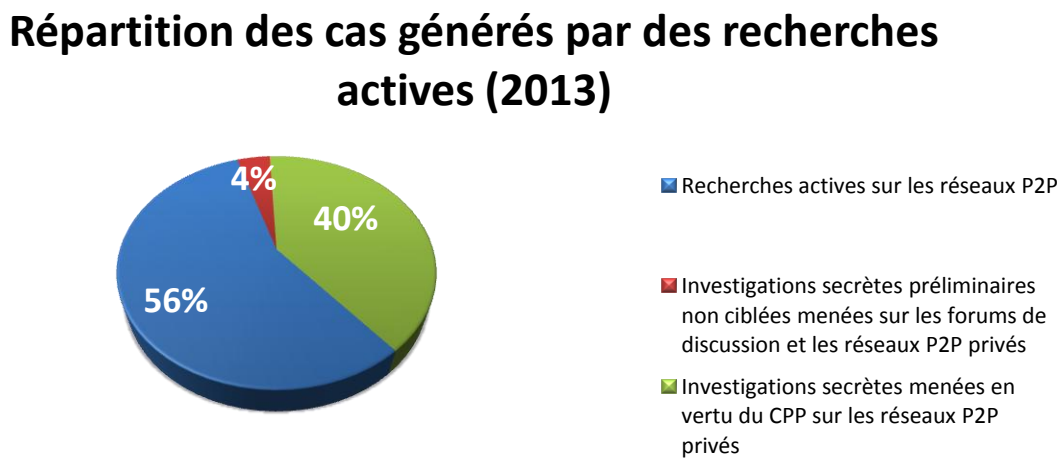
4. Recherches actives (monitoring)

De par ses recherches actives menées sur Internet indépendamment de tout soupçon, le SCOCI est présent sur les domaines d'Internet les moins faciles d'accès pour la population et entend de ce fait exercer une fonction préventive. Le comité directeur du SCOCI redéfinit annuellement les axes principaux d'engagement dans ce domaine. Comme les années précédentes, l'accent a été mis en 2013 sur la lutte contre la pédophilie sur Internet. Cependant, en raison du nombre croissant d'annonces concernant les infractions économiques, le comité directeur a également clairement affirmé que le SCOCI ne devait pas pour autant se détourner de la criminalité économique et de la cybercriminalité au sens strict du terme. Dans la pratique, cette décision a principalement déployé ses effets dans les tâches de coordination et les investigations préliminaires menées par le SCOCI (cf. ch. 5.2).

En 2013, ces recherches actives ont permis d'établir 423 dénonciations, ce qui représente une légère diminution – soit de 6 % – par rapport à 2012.



Graphique 9: procédures pénales ouvertes dans le cadre de recherches actives (2008–2013)



Graphique 10: origine des dénonciations générées par des recherches actives (total: 423)

4.1. Recherches actives sur les réseaux *peer-to-peer* (P2P)

Sur 423 dénonciations, 238 ont été générées par les recherches actives menées par le SCOCI dans les bourses d'échange publiques P2P. Ces dossiers visent des internautes qui échangent activement de la pornographie dure impliquant des enfants au sens de l'art. 197, al. 3, CP. Le nombre de cas annoncés a reculé de 47,1 % par rapport à 2012 (450). Le nombre de dossiers envoyés aux cantons a donc atteint le niveau constaté en 2011, et ce quand bien même le monitoring a été effectué avec la même intensité et selon les mêmes critères qu'en 2012.

Bien que le SCOCI recherche spécifiquement des utilisateurs domiciliés en Suisse, il a traité, pendant l'exercice sous revue et pour des raisons techniques, dix cas d'infractions de personnes domiciliées à l'étranger. Le SCOCI a transmis les résultats de ces investigations aux Etats compétents par le biais d'Interpol.

4.2. Investigations préliminaires secrètes non ciblées

L'accord sur la collaboration lors d'investigations préliminaires sur Internet visant à lutter contre la pédocriminalité (monitoring des forums de discussion en ligne), conclu entre fedpol, le SCOCI et le Département de la sécurité du canton de Schwyz, règle les modalités de l'engagement de collaborateurs du SCOCI en tant qu'agents infiltrés pour lutter contre la pédocriminalité sur Internet[8]. Conformément audit accord, les collaborateurs du SCOCI mènent des investigations préliminaires secrètes exclusivement sous mandat et contrôle de la police cantonale schwyzoise. Cet accord garantit ainsi que la surveillance préventive en matière de pédocriminalité sur Internet puisse continuer à être effectuée non seulement par les cantons, mais aussi par un service centralisé à l'échelon national.

Les investigations préliminaires secrètes menées par le SCOCI en 2013 ont conduit dans 17 cas à une dénonciation aux cantons compétents. Trois de ces dénonciations reposaient sur des investigations menées sur des forums de discussion en ligne pour enfants. Toutes les trois avaient pour objet des tentatives d'actes d'ordre sexuel avec des enfants au sens de l'art. 187 CP.

Dans les quatorze autres cas, les investigations préliminaires secrètes ont eu lieu dans des bourses d'échange privées P2P. Dans ces cas, contrairement aux sites P2P classiques, l'échange s'est effectué directement entre différents ordinateurs par le biais de raccordements privés chiffrés, raison pour laquelle l'investigation préliminaire secrète s'avère nécessaire pour entrer en contact avec les auteurs de ce type d'échange. Dans ce genre d'enquêtes, la plupart des dénonciations avaient pour objet la possession et la diffusion de pornographie illicite en vertu de l'art. 197, ch. 3 et 3^{bis}, CP.

4.3. Investigations secrètes fondées sur le CPP

Pour la première fois en dix ans d'existence, le SCOCI a été chargé par différents Ministères publics cantonaux de mener, au titre d'autorité directement subordonnée

[8] Engagement au sens de l'art. 9d de l'ordonnance du 22 mars 2000 du canton de Schwyz concernant la police cantonale (PolV – SRSZ 520.110).

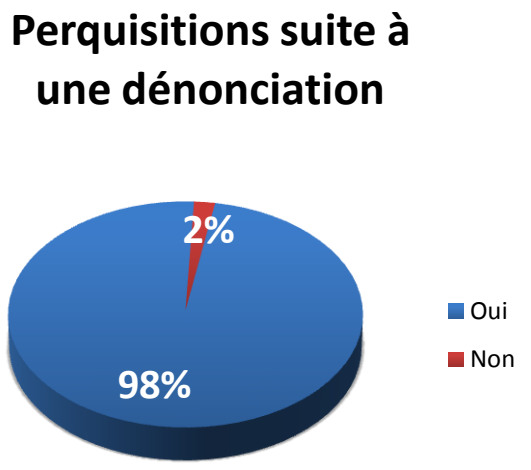
et dans le cadre d'une procédure cantonale, des investigations secrètes fondées sur le CPP. Ces investigations secrètes au sens de l'art. 285*a* ss CPP se sont déroulées exclusivement dans des bourses d'échange P2P privées. Elles ont généré au total 168 dénonciations, transmises aux autorités policières compétentes en Suisse et à l'étranger.

Les communautés P2P privées pouvant être reliées entre elles dans le monde entier, il s'avère difficile de cibler les recherches sur des auteurs d'infractions suisses. Au cours des enquêtes ordonnées, deux utilisateurs suisses ont pu être identifiés. Les 166 autres dénonciations ont toutes été transmises aux autorités étrangères de poursuite pénale dans le cadre de l'échange international d'informations de police.

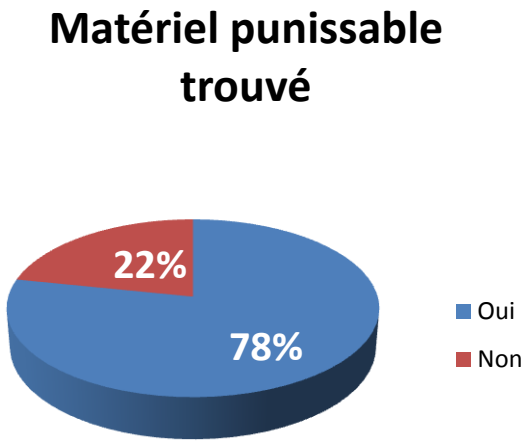
4.4. Feed-back des cantons

En cas de soupçon fondé d'infraction, le SCOCI transmet les cas aux cantons compétents (cf. graphique 11). Afin d'avoir une vue d'ensemble des mesures engagées dans les cantons, le SCOCI demande aux cantons des informations sur la suite donnée à ces dossiers (mesures de police engagées ou résultat des procédures judiciaires).

Afin de pouvoir suivre la situation actuelle, seuls les feed-back rendus en 2013 par les cantons ont été pris en compte ci-après. La plupart des dénonciations ont été établies sur la base des recherches actives menées en 2012 sur les réseaux P2P (417). Elles concernent donc des personnes qui participent activement à l'échange de contenus punissables à caractère pédopornographique.



Graphique 11: perquisitions domiciliaires en 2013



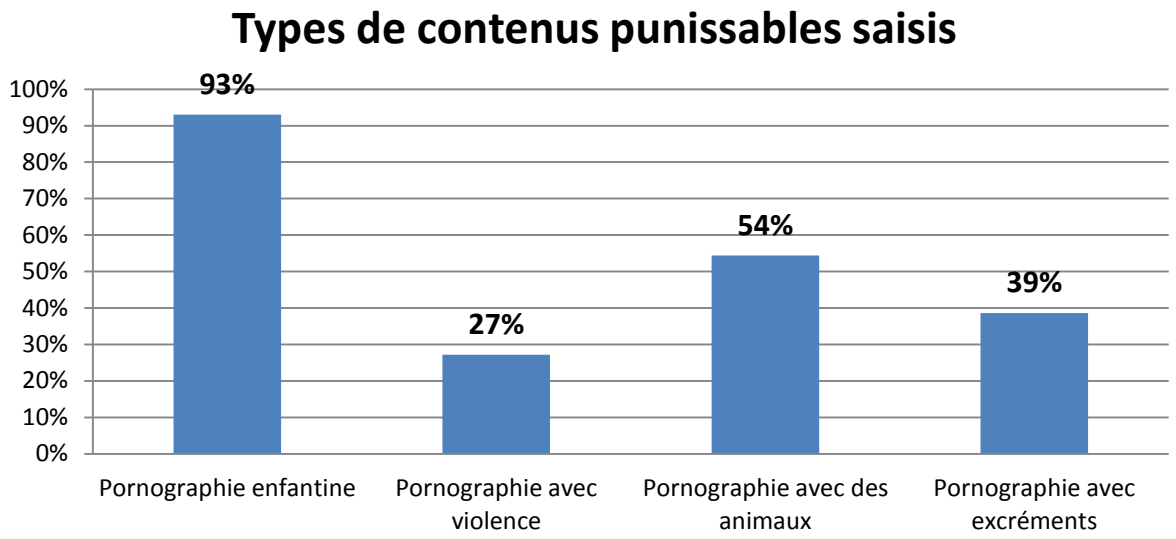
Graphique 12: matériel punissable en 2013

Les deux graphiques ci-dessus montrent que 98 % des dénonciations transmises par le SCOCI ont été à l'origine de perquisitions domiciliaires effectuées par les autorités de police cantonales.

4.4.1. Feed-back des autorités de police cantonales

Dans 78 % des cas, ces perquisitions ont permis de saisir du matériel illégal. Les raisons des perquisitions infructueuses sont diverses. Par exemple, un raccordement sans fil ouvert et non protégé ou le transfert de données vers des services de stockage en nuage (*cloud services*) empêchent en général une sauvegarde efficace des preuves et une identification certaine des suspects.

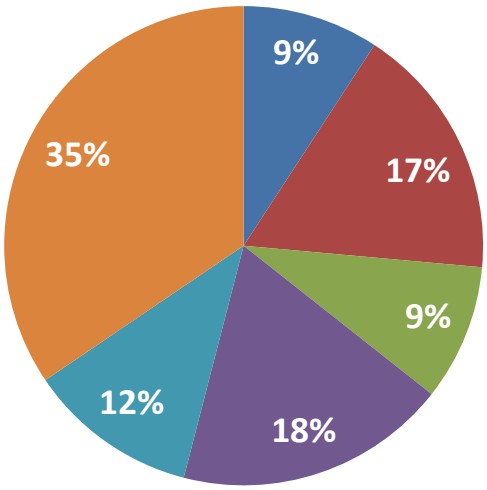
93 % du matériel illégal saisi contenait du matériel pornographique impliquant des enfants. Ce haut pourcentage n'a rien d'étonnant car ce type de contenus est justement ciblé dans le monitoring des réseaux P2P et constitue de ce fait la grande majorité des dénonciations transmises aux cantons. Il est toutefois intéressant de relever que dans plus de la moitié des cas, un autre élément constitutif de la pornographie illégale (art. 197 CP) a été constaté (cf. graphique 13) et que plus d'une perquisition sur deux a permis de saisir du matériel de pornographie impliquant des animaux.



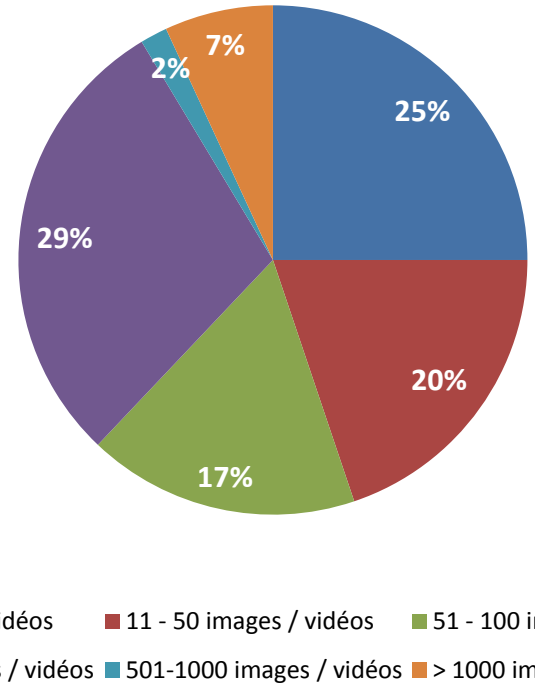
Graphique 13: quel type de matériel a été saisi en 2013 au cours des perquisitions?

Les feed-back des autorités de police cantonales indiquent que, concernant le type de matériel illégal saisi au cours des perquisitions, il s'agit de fichiers-vidéos (films) dans 94 % des cas et de fichiers-images (photographies) dans 66 %. Très souvent, les deux types de fichiers sont saisis simultanément. Au total, les perquisitions ont permis de saisir plusieurs millions de fichiers-vidéos et de fichiers-images.

Nombre de fichiers-images saisis au cours des perquisitions



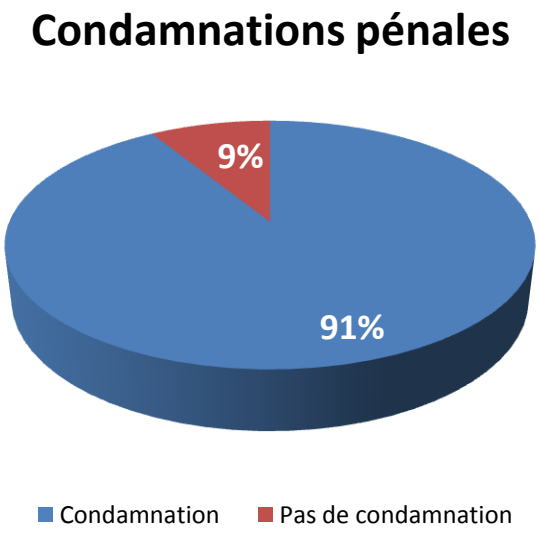
Nombre de fichiers-vidéos saisis au cours des perquisitions



Graphiques 14 et 15: vue d'ensemble de la quantité de fichiers-images et de fichiers-vidéos saisis

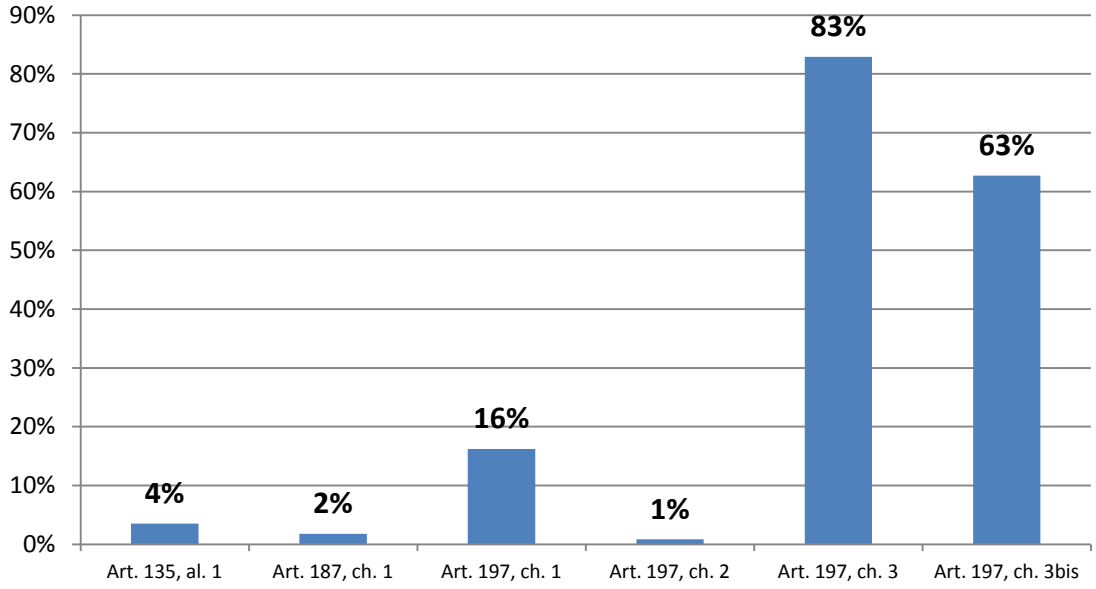
4.4.2. Feed-back des autorités judiciaires des cantons

Selon les données transmises au SCOCI par les autorités judiciaires des cantons, la procédure pénale a été suivie d'une condamnation dans 91 % des cas.



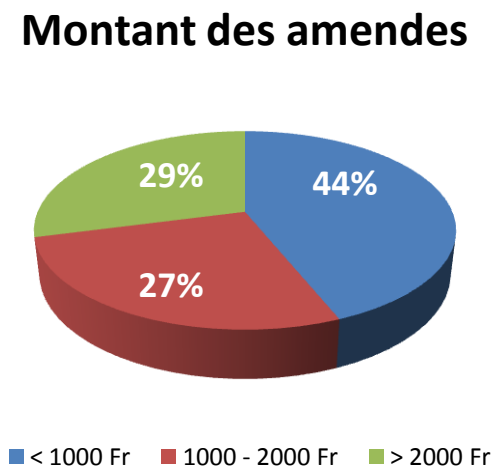
Graphique 16: condamnations pénales en 2013

La plupart des condamnations ont été prononcées pour possession de pornographie dure, sur la base de l'infraction de pornographie visée à l'art. 197 CP et principalement de ses ch. 3 et 3bis.

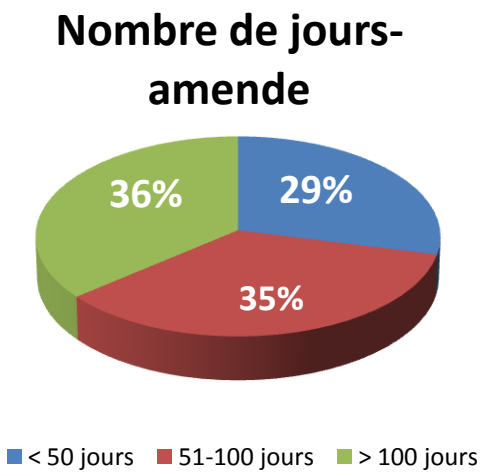


Graphique 17: jugements les plus fréquents en 2013 (en %)

La peine prononcée dans 85 % des cas de possession de pornographie illégale en 2013 est une peine pécuniaire (jours-amende), à laquelle s'ajoute une amende dans 77 % des cas. Dans 91 % des cas, les peines pécuniaires sont assorties d'un sursis. Des sanctions alternatives telles que le travail d'intérêt général, les mesures thérapeutiques, la peine privative de liberté (prison) et des peines pécuniaires fermes ont été appliquées dans 4 % des cas.



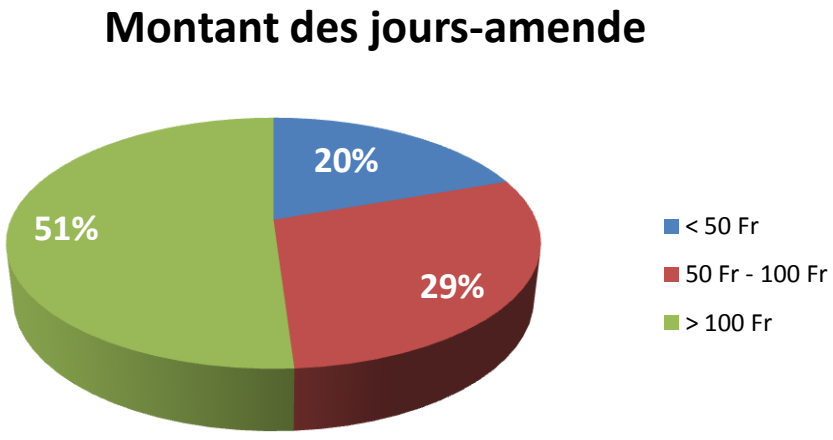
Graphique 18: montant des amendes



Graphique 19: nombre de jours-amende infligés

Dans 44 % des cas, les amendes sont inférieures à 1000 francs et dans 27 % des cas, elles vont de 1000 à 2000 francs. Dans 29 % des cas seulement, les amendes sont supérieures à 2000 francs.

Pour 29 % des peines pécuniaires, le nombre des jours-amende est inférieur à 50. Dans 35 % des cas, ce nombre est compris entre 51 et 100. Enfin, des peines pécuniaires de plus de 100 jours-amende ont été prononcées dans 36 % des cas.



Graphique 20: montant des jours-amende

Dans 20 % des cas, des jours-amende ont été prononcés pour un montant de 1 à 50 francs, dans 29 % des cas de 51 à 100 francs et dans 51 % des cas au-delà de 100 francs.

Précisons en outre qu'à ces amendes s'ajoutent parfois des frais de procédure qui peuvent être élevés.

4.5. Exemples de cas

Au cours de l'année écoulée, trois personnes cherchant le contact avec des mineurs à des fins sexuelles sur des forums de discussion en ligne pour enfants ont pu être identifiées et arrêtées. Dans l'un des cas, l'auteur de l'infraction a cherché, après seulement quelques minutes de conversation, à convenir d'un rendez-vous. Ne sachant pas que la jeune fille de 13 ans à qui il pensait s'adresser était en réalité un enquêteur du SCOCI, il a proposé des actes d'ordre sexuel. Suite à cela, la police cantonale chargée de l'affaire est parvenue, lors du rendez-vous convenu avec la prétendue jeune fille, à arrêter le pédocriminel, qui était alors armé d'un couteau. Ce cas met en évidence le danger réel que constitue la présence de délinquants sexuels sur les forums de discussion en ligne pour enfants.

En 2013, les recherches actives menées par le SCOCI sur les réseaux P2P ont permis de mettre au jour un cas d'abus commis sur un enfant. Dans cette affaire, le SCOCI a transmis aux autorités de police compétentes plusieurs dénonciations portant sur des cas de diffusion illégale de pornographie dans les réseaux P2P. Les investigations ont révélé qu'un père de famille vivant avec ses enfants et sa femme avait abusé sexuellement de sa propre fille âgée de trois ans plusieurs mois durant. Jusqu'à l'annonce transmise par le SCOCI, l'individu n'était pas connu des services de police. Grâce à la collaboration efficace entre le SCOCI et la police cantonale chargée de l'affaire et aux enquêtes très poussées de la police, l'auteur de l'infraction a pu être démasqué et son enfant sera désormais protégée d'autres abus.

Dans un autre cas, les recherches actives ont permis de démasquer un ressortissant allemand participant activement à la diffusion de pornographie enfantine dans des réseaux P2P. Le SCOCI a transmis le dossier aux autorités allemandes via Interpol. Selon les informations fournies par le parquet compétent, le prévenu est un homme de 45 ans, responsable d'une association de jeunesse. Selon les dires de l'individu, l'association traitait principalement de questions concernant la protection de l'enfance et de la jeunesse (violence, pornographie, cybermobbing, limitations d'âge, logiciels consacrés à la protection de la jeunesse, sécurité sur Internet, jeux vidéo, smartphones, conseils en matière de projets dans les médias, etc.). L'association était cofinancée par le Bundesland en question.

Ces cas soulignent l'importance du traitement systématique, par les autorités cantonales, des dénonciations transmises. Faute de ressources suffisantes, certains cantons sont fortement mis sous pression face à l'augmentation constante du nombre de dossiers transmis par le SCOCI. L'énorme surplus de travail que ces dossiers représentent les place parfois face à de grandes difficultés en termes de délais.

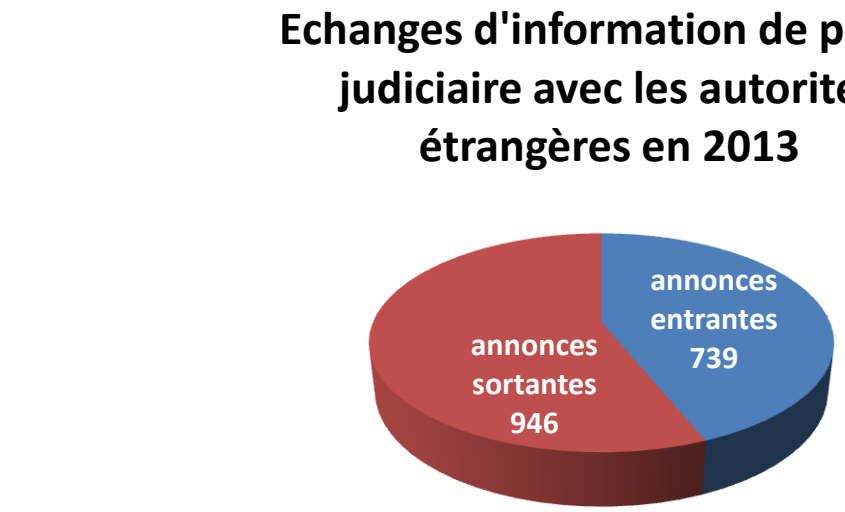
5. Echange d'informations de police judiciaire

5.1. Annonces entrantes et sortantes

Depuis l'intégration du SCOCI en 2009 à la Police judiciaire fédérale et la décision du comité directeur de ne pas éloigner totalement le SCOCI de la criminalité économique et de la cybercriminalité au sens strict du terme, l'échange d'informations de police judiciaire – que ce soit en Suisse ou à l'étranger – a gagné en importance. Le SCOCI est devenu la plaque tournante de l'échange d'informations. En tant que centre de compétence chargé de tâches de coordination, il soutient les cantons dans leurs enquêtes et garantit l'échange d'informations, mettant à profit l'important réseau dont il dispose dans les cantons, à l'étranger, mais aussi dans l'économie privée et le secteur public. Il constitue par ailleurs un relais vers les organisations internationales que sont Interpol et Europol et également vers l'agence *European Cybercrime Center* (EC3).

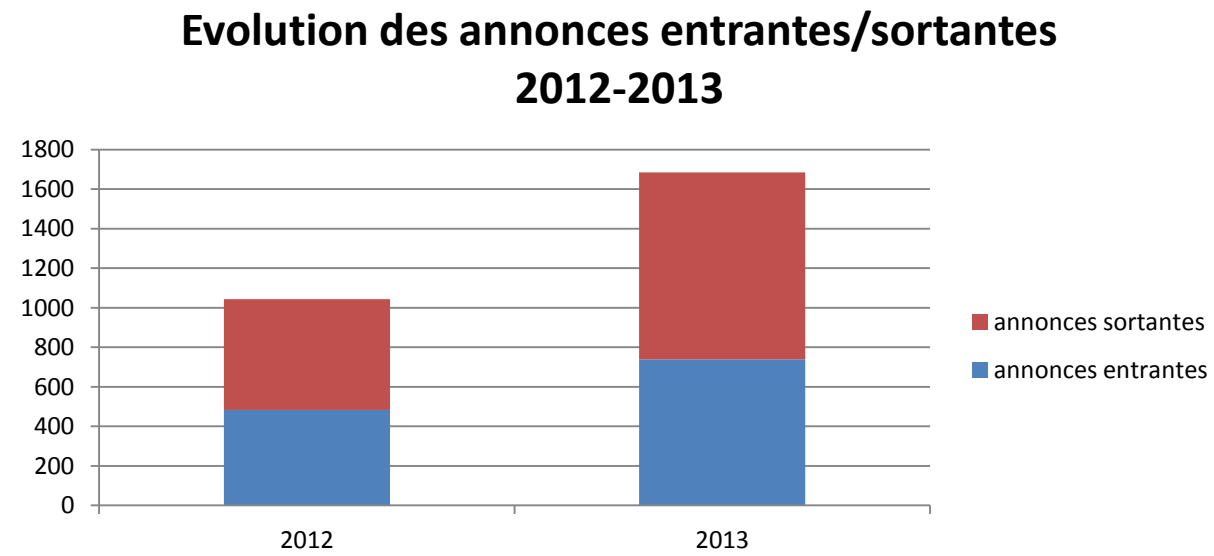
Depuis l'entrée en vigueur de la Convention du Conseil de l'Europe sur la cybercriminalité (CCC) le 1er janvier 2012, la Suisse participe, à l'échelon international, de manière active à la lutte contre la criminalité sur Internet. Cela se traduit en premier lieu par une forte augmentation de l'échange d'informations de police judiciaire avec les autorités étrangères sur des cas entrant dans le champ d'application de la convention. C'est ce que montrent les chiffres présentés ci-après.

En 2013, 739 annonces relevant du champ d'application de la CCC ont été reçues, ce qui représente une augmentation de plus de 53 % par rapport à l'année précédente. Le même phénomène est observable pour les annonces sortantes que le SCOCI a rédigées à l'intention des autorités étrangères de poursuite pénale. Au cours de l'année écoulée, le SCOCI a établi, sur demande des cantons ou de sa propre initiative, au total 946 annonces destinées à l'étranger (Interpol et Europol), ce qui correspond à une augmentation de 68 %.



Graphique 21: échange d'informations de police judiciaire avec l'étranger

Une particularité de la CCC consiste à permettre aux autorités de police compétentes, par le biais d'une demande d'entraide judiciaire, la saisie rapide de données (art. 29 ss). A ce propos, le SCOCI a transmis aux autorités étrangères huit demandes des cantons. De leur côté, les autorités étrangères ont transmis quatre demandes aux cantons.

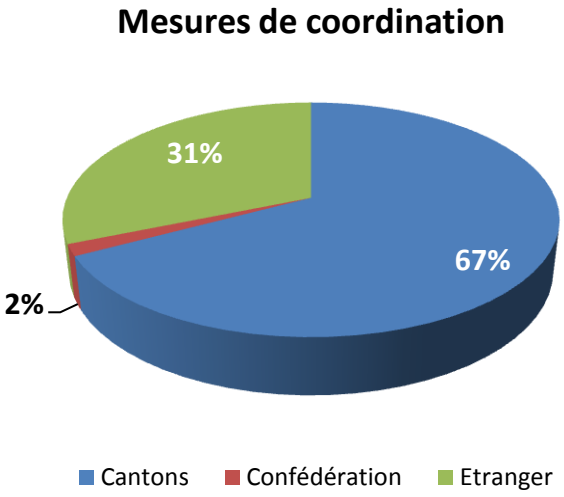


Graphique 22: évolution de l'échange d'informations de police judiciaire en 2012 et 2013

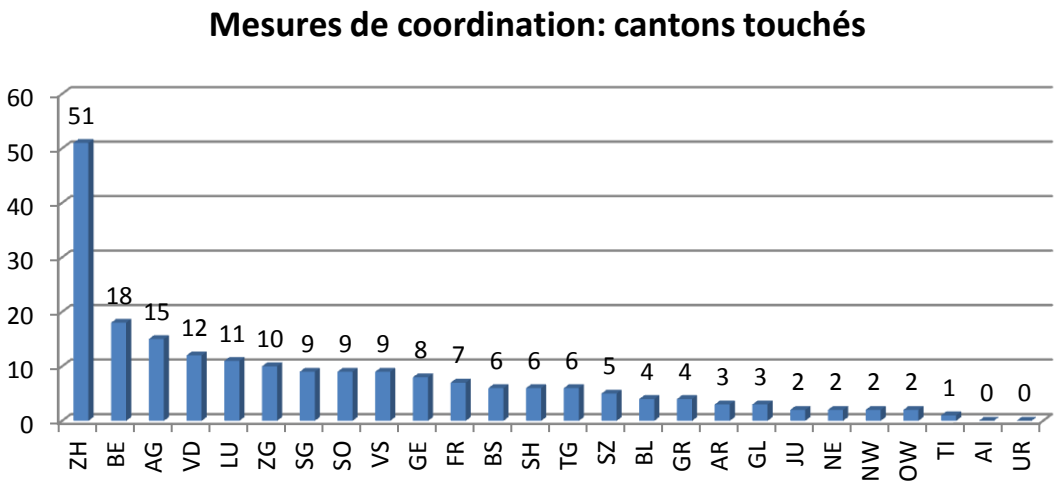
5.2. Procédures de coordination en Suisse et à l'étranger

Dans le cadre de l'échange d'informations de police judiciaire, environ 180 mesures de coordination ont été exécutées.

La façon dont le SCOCI va apporter son soutien dépend de la situation initiale. En particulier, le SCOCI collabore dans le cadre de procédures d'enquête internationales. Dans ce cas, le SCOCI fait figure d'interlocuteur pour les autorités de poursuite pénale nationales et étrangères. Dans d'autres cas, surtout lorsque la compétence cantonale est avérée, le SCOCI a apporté son expertise, que cela soit aux niveaux analytique, technique et juridique, ou lors de l'engagement d'enquêteurs sous couverture.

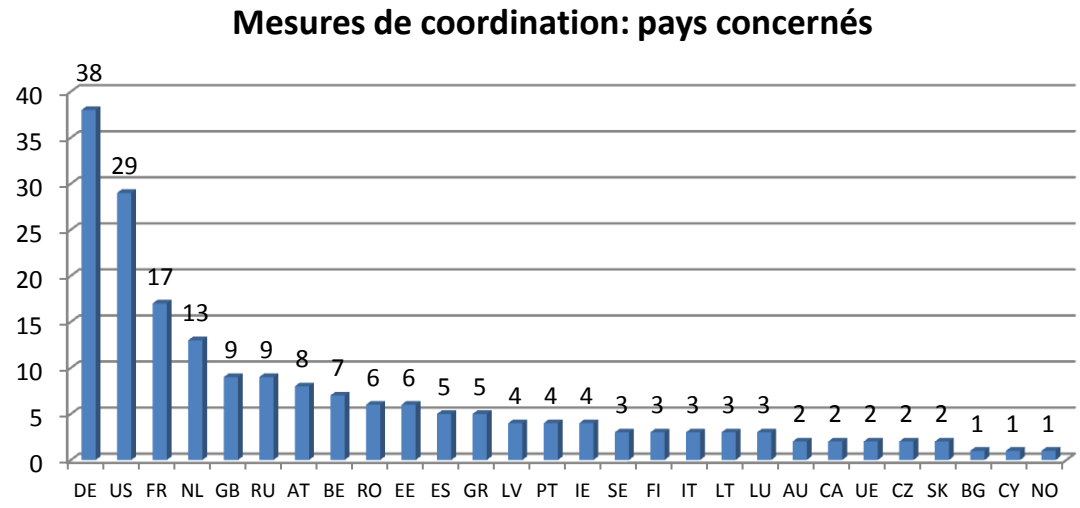


Graphique 23: distribution des mesures de coordination (en %)



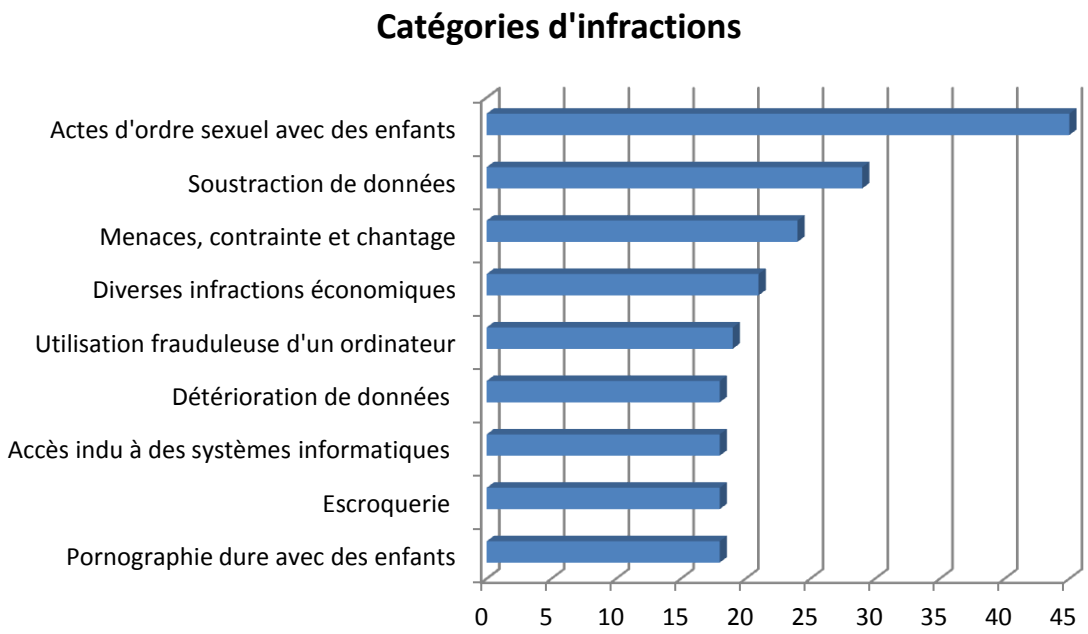
Graphique 24: cantons concernés par des mesures de coordination

Le canton de Zurich a été touché par un nombre de mesures de coordination particulièrement élevé. En regardant ces chiffres de plus près, on constate deux éléments essentiels. Premièrement, Zurich, en tant que centre économique, héberge un grand nombre d'entreprises nationales et étrangères importantes actives dans les domaines de l'information et de la communication. Deuxièmement, le canton de Zurich, en créant un centre de compétence cantonal chargé de la cybercriminalité, a mis en place les conditions nécessaires pour mener des enquêtes dans l'espace virtuel ou pour apporter sa contribution aux enquêtes menées au niveau international.

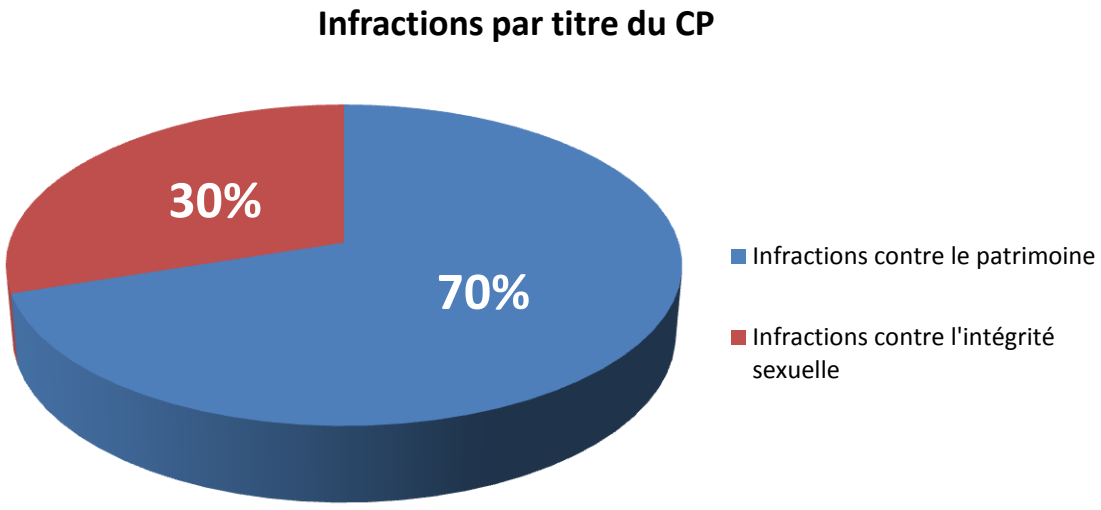


Graphique 25: pays concernés par des mesures de coordination

Dans le cadre des enquêtes menées au niveau international, le SCOCI est un interlocuteur de premier plan et fait le lien entre les différentes parties suisses et étrangères concernées. Cela permet à la Suisse d'avoir une vue d'ensemble sur les cas et les informations et d'entreprendre les démarches nécessaires, dans notre pays comme à l'étranger.



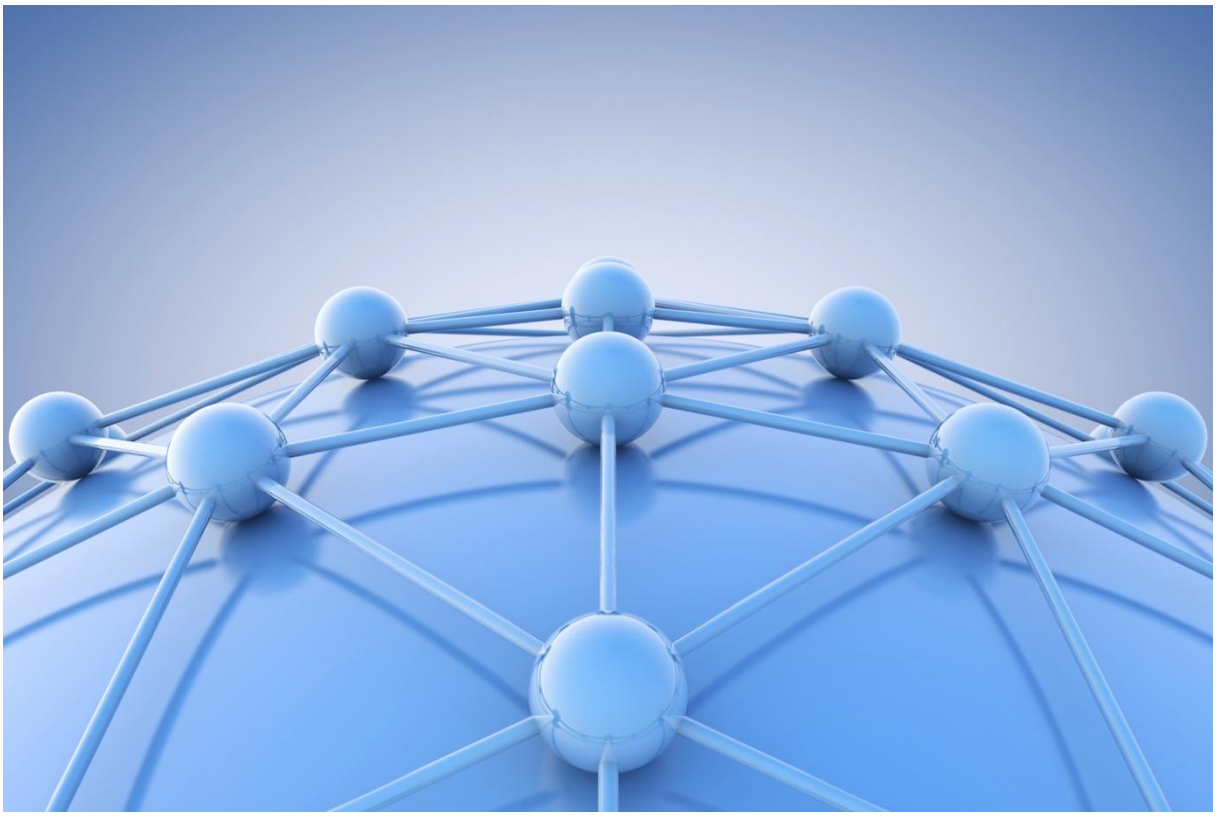
Graphique 26: répartition des mesures de coordination par le SCOCI en 2013, par catégories d'infractions



Graphique 27: répartition des mesures de coordination par le SCOCI en 2013, par titre du CP

5.3. Exemples de cas

Le SCOCI a reçu du BKA/Wiesbaden une annonce l'informant que des inconnus s'étaient introduits dans les systèmes informatiques de l'une des plus grandes entreprises nationales de télécommunication et qu'ils transféraient les données volées par le biais d'un serveur situé en Suisse. En l'espace de quelques heures, le SCOCI avait pris contact avec le centre de compétence zurichois chargé de la cybercriminalité et avait fait saisir les données concernant les raccordements et les contenus conformément à l'art. 29 de la CCC. Une première analyse a permis de remonter la piste jusqu'aux auteurs en Allemagne. Deux jours après, le serveur concerné avait été saisi et analysé une nouvelle fois, d'entente avec le service chargé de l'enquête. Il s'était alors avéré que les auteurs du piratage avaient fait disparaître une grande partie des traces. Si les données n'avaient été saisies qu'à ce moment-là, il aurait été quasiment impossible d'identifier les auteurs.



Le SCOCI a également participé à l'exécution de demandes d'entraide judiciaire déposées par l'étranger. Citons à cet égard le *takedown* de l'entreprise *LibertyReserve* par le *US Secret Service* (USSS). Le SCOCI a fait le lien entre l'Office fédéral de la justice (OFJ), l'USSS, le Ministère public de la Confédération (MPC) et la Police judiciaire fédérale. A cet égard, l'USSS a contacté le SCOCI en amont afin que ce dernier le mette en contact avec les services concernés et qu'il effectue les premières clarifications. En effet, le temps qui se serait écoulé entre le dépôt de la demande d'entraide judiciaire auprès de l'OFJ et son exécution à proprement parler aurait sinon été trop court. Grâce à la fonction de coordination et d'intermédiaire du SCOCI, les services concernés ont pu, lors de la préparation de l'enquête, se concentrer sur leurs tâches principales et procéder à la saisie du serveur requise dans la demande d'entraide judiciaire.

6. Projets

6.1. Stratégie nationale de protection de la Suisse contre les cyberrisques

Le 27 juin 2012, le Conseil fédéral a approuvé la Stratégie nationale de protection de la Suisse contre les cyberrisques. Grâce à cette stratégie, le Conseil fédéral, en collaboration avec les autorités, les milieux économiques et les exploitants d'infrastructures critiques, compte réduire les cyberrisques auxquels tous ces acteurs sont exposés quotidiennement. La stratégie souligne le fait que les risques informatiques sont en premier lieu liés aux tâches et responsabilités existantes. Par conséquent, ces risques devront être traités dans le cadre des processus existants de gestion des risques. Il faut en priorité que les responsables soient mieux informés sur les cyberrisques et apprennent à mieux les percevoir.

Pour ce faire, le Conseil fédéral charge les départements de prendre en main l'application des seize mesures arrêtées, à leur niveau respectif et en collaboration avec les autorités cantonales et les milieux économiques. L'éventail de ces mesures va des analyses des risques pour les infrastructures TIC critiques à l'implication plus forte de la Suisse dans ce domaine au niveau international.

La mesure 6 prévoit de garantir une vue d'ensemble aussi large que possible des cas (infractions) au niveau national et de coordonner les cas intercantonaux complexes. Les informations acquises à partir des vues d'ensemble doivent être intégrées dans une présentation globale de la situation. Dans cet esprit, le DFJP élabore d'ici à fin 2016, en collaboration avec les cantons, un concept de gestion. Ce concept porte aussi sur la définition d'interfaces avec d'autres acteurs dans le domaine de la réduction des cyberrisques, sur la coordination avec la présentation de la situation et sur les ressources et les adaptations juridiques – tant au niveau de la Confédération qu'à celui des cantons – qui sont nécessaires pour le concrétiser. Conformément à la décision du comité directeur du SCOCI et de la direction de fedpol, le SCOCI doit assurer la coordination et l'exécution du mandat en relation avec la mise en œuvre de la stratégie NCS pour fedpol, dont la direction sera assumée par le chef de la PJF.

Il s'agit, dans le cadre de ce projet, d'empoigner les différentes tâches liées au développement et à l'organisation de la vue d'ensemble des cas et d'élaborer avec les cantons un solide concept de mise en œuvre d'une vue d'ensemble au niveau national et de coordination des cas intercantonaux complexes. Il s'agit tout particulièrement de clarifier les problématiques relevant de l'organisation, de la technique, du droit, des ressources (par exemple le personnel, les infrastructures, l'informatique, etc.). Dans un premier temps, une analyse détaillée du mandat a été réalisée et l'organisation de projet a été définie: elle se compose de représentants de fedpol, de la CCDJP, de la CCPCS, de la CPS (anciennement CAPS), d'un représentant de Swiss Police ICT ainsi que d'un représentant du MPC et d'un autre de l'OFJ. En 2014 déjà, le concept passera deux fois en consultation, auprès des cantons et des services concernés.

6.2. Le SCOCI fait son entrée sur les réseaux sociaux

En tant que bureau de communication, le SCOCI doit s'adapter constamment aux développements les plus récents dans et autour d'Internet. Les évolutions technologiques modifient les offres en matière de communication ainsi que l'utilisation qui est faite des médias. Le SCOCI reçoit aussi de plus en plus d'annonces ayant trait à des contenus ou à des comportements potentiellement répréhensibles en lien avec Facebook.

Au vu de cette situation, le SCOCI a proposé à son comité directeur de prendre différentes mesures dans le but d'instaurer un meilleur dialogue avec le public. Le comité de direction a décidé que le SCOCI disposerait dorénavant, entre autres, de son propre profil sur Facebook et Twitter et que son entrée sur les nouveaux réseaux de communication aurait lieu à l'occasion des dix ans du SCOCI. Les nouveaux profils[9] ont été publiés dans trois langues le 22 décembre 2013 et sont à la disposition de la population depuis cette date.

[9] www.facebook.com/scoci.ch et sur Twitter @KOBIK_Schweiz

7. Groupes de travail, partenariats et contacts

7.1. Collection nationale de fichiers et de valeurs de hash (CNFVH)

La CNFVH est en service depuis octobre 2012 et peut être utilisée par les services spécialisés cantonaux et municipaux. Pour que son utilisation soit efficace, la collection doit contenir suffisamment d'images connues classées avec les valeurs de hash correspondantes. Le classement de matériel photo nécessite beaucoup de temps et ne peut être effectué qu'avec le soutien des cantons en raison des ressources limitées du SCOCI.

7.2. Groupes de travail nationaux

Au cours de l'exercice 2013, le SCOCI a été représenté au sein de différents groupes de travail nationaux.

En 2013, le SCOCI a organisé la rencontre annuelle du groupe de travail "Kindsmissbrauch" (abus sur les enfants) aux côtés du Commissariat Pédocriminalité et pornographie de la Police judiciaire fédérale. Le groupe de travail s'occupe de problématiques actuelles ayant trait à des abus sur les enfants et à la lutte contre ces abus, et ceci en collaboration avec des organisations d'utilité publique, des représentants des cantons et la Prévention suisse de la criminalité.

Comme durant les années précédentes, le SCOCI a aussi poursuivi en 2013 son engagement dans le cadre du programme national "Protection de la jeunesse face aux médias et compétences médiatiques". Le SCOCI siège à la fois dans le groupe de travail chargé d'élaborer le programme d'action et dans le groupe d'accompagnement. Ce programme vise avant tout à aider les enfants et les adolescents à utiliser les médias de façon sûre, responsable et adaptée à leur âge.

Depuis 2011, le SCOCI représente fedpol au sein de la commission spéciale de la Prévention suisse de la criminalité. Cette commission a pour fonction d'élaborer des projets et moyens visant à prévenir la criminalité dans les cantons et à évaluer leur mise en œuvre.

Enfin, le SCOCI a poursuivi son engagement dans la mise en œuvre du concept "Sécurité et confiance", coordonné par l'Office fédéral de la communication (OFCOM) et visant à sensibiliser la population à une utilisation vigilante des technologies de l'information et de la communication.

7.3. Collaboration avec d'autres services de la Confédération

Au cours de l'exercice 2013, le SCOCI a poursuivi sa collaboration avec différents services de la Confédération dans le but de lutter contre la criminalité sur Internet. Au sein de fedpol, le SCOCI collabore étroitement avec les commissariats Pédocriminalité et pornographie, Enquêtes TI et Investigations secrètes de la Police judiciaire fédérale, mais aussi avec la Division principale Coopération policière internationale (CPI). En raison de la proximité des thématiques traitées, le SCOCI et le Commissariat Pédocriminalité et pornographie sont par ailleurs en contact particulièrement

étroit. En outre, les contacts ont été élargis ou intensifiés avec d'autres partenaires fédéraux. Citons notamment MELANI, le Domaine de direction Entraide judiciaire internationale de l'OFJ, l'Office fédéral de l'informatique et de la télécommunication (OFIT), l'Office fédéral des assurances sociales (OFAS), l'Office fédéral de la communication (OFCOM), la Commission fédérale contre le racisme (CFR), l'Administration fédérale des douanes (AFD), la Régie fédérale des alcools (RFA), l'Autorité de surveillance des marchés financiers (FINMA), l'Institut fédéral de la propriété intellectuelle (IPI) et la Commission fédérale des maisons de jeu (CFMJ).

7.4. Echanges d'expériences avec les cantons

La collaboration avec les différents représentants des autorités de police et des ministères publics des cantons a été particulièrement intense au cours de l'exercice 2013.

On notera tout spécialement la collaboration et l'échange d'expériences avec le centre de compétence du canton de Zurich chargé de la cybercriminalité, qui a ouvert ses portes en 2013. Les structures clairement établies en matière de lutte contre la criminalité sur Internet, de même que la présence d'interlocuteurs au sein du Ministère public et de la police ont évité à plusieurs reprises que des preuves ne soient détruites ou alors ont permis l'ouverture d'une procédure.

En plus des échanges d'informations habituels avec les cantons, plusieurs séances de travail ont eu lieu, en particulier à propos des investigations préliminaires secrètes (cf. ch. 4.) et du projet de CNFVH (cf. ch. 6.1.).

En outre, la deuxième édition du "Forum Cybercrime Ministères publics – SCOCI" s'est déroulée le 19 novembre 2013. Des experts et des intervenants versés dans la poursuite pénale et le domaine scientifique ont présenté aux participants une vue d'ensemble de la lutte internationale contre la cybercriminalité axée sur la pratique. Ainsi, les participants ont été informés des procédures d'enquête en cours contre des réseaux de machines zombies et contre le blanchiment d'argent par le biais de devises en ligne. De plus, des représentants d'Europol ont présenté les capacités de coordination de l'agence *European Cybercrime Center* (EC3), qui a entamé ses activités à la Haye en janvier 2013. Près de 100 procureurs ont pris part au forum de cette année, ce qui démontre clairement la nécessité d'offrir une formation de ce type. Un débat direct sur les problèmes pratiques rencontrés par les Ministères publics s'est déroulé sous forme de table ronde en présence de représentants des milieux politiques et universitaires comme Luc Recordon, conseiller aux Etats, Daniel Jositsch, conseiller national et Christian Schwarzenegger, professeur de droit pénal à l'Université de Zurich.

7.5. Collaboration avec des ONG

Depuis de nombreuses années, le SCOCI collabore avec l'ONG[10] Action Innocence Genève dans le cadre de la lutte contre la pornographie enfantine. C'est en particulier grâce au soutien de cette organisation que le projet de monitoring des réseaux

10 Organisation non gouvernementale (ONG)

P2P a pu être mis en place et développé avec succès au cours des dernières années. La collaboration avec Action Innocence est donc fondamentale, puisque c'est grâce au logiciel fourni par cette ONG que la majorité des cas de recherche active peuvent être effectués chaque année. En outre, Action Innocence soutient le SCOCI dans le cadre de différents autres projets liés à la lutte contre la pédocriminalité.

La Fondation suisse pour la protection de l'enfant et ECPAT Suisse s'engagent notamment aussi pour la protection des enfants et la prévention des violences faites aux enfants sur Internet. Des rencontres régulières permettent de créer des synergies et d'harmoniser les efforts.

Durant l'année écoulée, une collaboration plus étroite a pu se mettre en place avec Pro Juventute suite à la participation de cet organisme à la rencontre annuelle du groupe de travail "Kindsmissbrauch" (abus sur les enfants).

7.6. Collaboration avec les fournisseurs suisses d'accès à Internet

Depuis 2007, le SCOCI collabore avec les principaux fournisseurs d'accès suisses dans le but de bloquer l'accès à des sites Internet au contenu pédopornographique. Ce blocage vise uniquement les sites hébergés à l'étranger qui proposent de télécharger de la pornographie enfantine illicite au sens de l'art. 197, ch. 3, CP. Concrètement, le SCOCI met à la disposition des fournisseurs d'accès une liste de sites Internet ayant ce type de contenu, mise à jour en continu (env. 200 à 300 sites Internet). En conformité avec leur position éthique et leurs conditions générales, ces fournisseurs bloquent l'accès à des sites pénalement punissables et redirigent leurs utilisateurs vers une page "stop".

Dans le cadre de ce projet, le SCOCI collabore étroitement avec Interpol. La liste suisse mentionnant les sites Internet contenant de la pornographie enfantine est alimentée en grande partie par la liste "worst of" d'Interpol. Le SCOCI recherche quotidiennement, de manière proactive, de nouveaux sites Internet ayant ce type de contenu et complète en permanence la liste d'Interpol, entretenue grâce à une coopération entre les polices de différents pays.

7.7. Coopération internationale

Depuis 2011, le SCOCI est membre du projet CYBORG d'Europol, dont le but est la lutte contre la cybercriminalité à l'échelle supranationale. Elle cible notamment les attaques de hameçonnage, les réseaux de machines zombies ou encore le piratage de bases de données à grande échelle. Il participe également depuis 2011 au projet TWINS, consacré à la lutte contre la pédocriminalité. Ces deux projets, classés thèmes majeurs ("Focal Points") par Europol, relèvent de l'agence *European Cybercrime Center* (EC3), qui a entamé ses activités le 1er janvier 2013.

Sis auprès d'Europol à La Haye, le centre de lutte contre la criminalité sur Internet EC3 fournit un support opérationnel aux Etats de l'UE et met à disposition ses connaissances spécialisées dans le cas d'enquêtes menées conjointement à l'échelle communautaire. Le SCOCI est en contact permanent avec l'agence EC3 et a déjà pu apporter à plusieurs reprises une contribution active à des opérations menées dans des réseaux anonymes.

Depuis 2013, le SCOCI représente également la Suisse au sein de l'EUCTF ou *European Union Cybercrime Task Force*. Ce groupe d'experts créé en 2010 se compose de représentants d'Europol, d'Eurojust et de la Commission européenne. Son objectif est de faciliter et d'optimiser la lutte contre la cybercriminalité dans l'espace de l'Union européenne en collaboration avec les responsables des unités nationales spécialisées dans la lutte contre la cybercriminalité. L'EUCTF fournit une aide visant à développer et à encourager un concept uniforme au niveau de l'Union européenne en matière de lutte contre la cybercriminalité et à résoudre les problèmes résultant de l'utilisation des cybertechnologies à des fins criminelles. L'UE a aussi attribué une très grande importance à la lutte contre la cybercriminalité dans le cadre de l'EMPACT (*European Multidisciplinary Platform against Criminal Threats*) en plaçant la cybercriminalité parmi ses huit préoccupations majeures. Le SCOCI accompagne les efforts déployés par l'Union européenne (UE) et représente activement les intérêts de la Suisse dans les discussions.

Par ailleurs, le SCOCI participe également au projet CIRCAMP, qui lutte contre la diffusion de la pornographie enfantine sur Internet et a été lancé par la Task force des chefs de police européens. Comme les années précédentes, il a également été en contact en 2013 avec le groupe de travail *European Financial Coalition* (EFC). Cofinancée par l'Union européenne, l'EFC rassemble les grands responsables de la poursuite pénale et les principaux acteurs du secteur privé dont l'objectif commun est de lutter contre l'exploitation sexuelle des enfants et des jeunes à des fins commerciales.

Ce sont des buts semblables que poursuit la *Global Alliance against Child Sexual Abuse Online* à laquelle la Suisse a adhéré le 6 décembre 2012 à Bruxelles. Par sa signature, la conseillère fédérale Simonetta Sommaruga a confirmé que la Suisse attache une grande importance à la coopération internationale en matière de lutte contre la pédocriminalité et que cette coopération doit continuer à être encouragée. L'un des jalons définis par le SCOCI au niveau de la collaboration avec la *Global Alliance* concerne l'adhésion de la Suisse à la *Virtual Global Taskforce* (VGT). La VGT est un partenariat international instauré entre des autorités de poursuite pénale, des organisations non gouvernementales et l'industrie privée dans le but de protéger les enfants contre les abus sexuels sur Internet. La VGT veut rendre Internet plus sûr, déceler les abus et les localiser, aider les enfants en difficulté et garantir une poursuite pénale efficace des auteurs de ces abus. La VGT compte à ce jour douze membres à part entière et divers partenaires (cf. www.virtualglobaltaskforce.com). Durant l'année écoulée, la demande d'admission de la Suisse au sein de la VGT a été acceptée à l'unanimité par le *Board of Directors*. En mai 2014, le SCOCI représentera la Suisse, en tant que nouvel Etat membre, lors de la prochaine rencontre de la VGT à Bruxelles.

8. Médias, formations et conférences

8.1. Présence médiatique

Au cours de l'exercice 2013, le SCOCI a été présent dans de nombreux médias. Par ailleurs, les mises en garde du SCOCI à l'égard des phénomènes criminels sur Internet ont été également portées à la connaissance des médias.

On mentionnera tout spécialement la participation du SCOCI à l'émission "Chronik eines Missbrauchs" (chronique d'un abus) de la série documentaire "Schweizer Verbrechen im Visier" (crimes suisses en point de mire) produite par la SRF.

8.2. Réseaux sociaux

Les échos obtenus jusqu'ici de la part des utilisateurs Facebook et Twitter quant à la nouvelle présentation du SCOCI dans les médias sociaux sont très positifs (www.facebook.com/scoci.ch et Twitter sous @KOBIK_Schweiz).

8.3. Formations et conférences

Au cours de l'année 2013, les collaborateurs du SCOCI ont eu l'occasion de participer à plusieurs cours, conférences et congrès internationaux. Ces rencontres constituent des occasions privilégiées de s'entretenir et de nouer des contacts avec différents partenaires et experts.

En outre, des collaborateurs du SCOCI ont dispensé des formations lors de diverses manifestations: par exemple par des ateliers sur la coopération policière internationale en matière de cybercriminalité organisés à l'Institut suisse de police ou encore par des exposés sur l'économie souterraine de la cybercriminalité dans le cadre de la formation continue des enquêteurs TI du Concordat de police de la Suisse du Nord-Ouest. A plus de 50 autres occasions, le SCOCI a fait des présentations ou a pris part à des tables rondes en 2013.

9. Interventions parlementaires au niveau fédéral

Interpellation 13.3229: Ampleur de la menace et mesures de lutte contre la cyber-guerre et la cybercriminalité - Recordon Luc, 22.3.2013

Interpellation 13.3986: Pourquoi la Suisse obtient-elle aussi peu d'informations de la part des réseaux sociaux? - Vogler Karl, 27.9.2013

Motion 13.3490: Sécurité des TIC. Création d'un centre de compétences- Guhl Bernhard, 19.6.2013

Question 13.5380: Insuffisance des instruments de lutte contre la cybercriminalité - Reimann Maximilian, 18.9.2013

Question 13.5356: Commande de drogues sur le site web Silk Road - Geissbühler Andrea Martina, 16.9.2013

Question 13.5321: La Suisse fait-elle aussi l'objet d'espionnage économique par la NSA? - Leutenegger Oberholzer Susanne, 11.9.2013

Question 13.5281: Activités des services secrets américains en Suisse - Vischer Daniel, 12.6.2013

Question 13.5059: Responsabilité des fournisseurs d'hébergement et des services de blogs et de forums - Glättli Balthasar, 6.3.2013

Question 13.5224: Cyberactivités des services secrets américains en Suisse - Reimann Maximilian, 10.6.2013

Interpellation 13.4077: Espionnage de données et sécurité sur Internet - Clottu Raymond, 5.12.2013

Initiative parlementaire 13.442: Grooming avec des mineurs - Commission des affaires juridiques, 15.8.2013

Postulat 13.3707: Stratégie cybernétique globale et adaptée aux exigences futures - Guhl Bernhard, 17.9.2013

Interpellation 13.3773: Pour une loi sur les télécommunications nous permettant d'affronter l'avenir. Elaborer une stratégie globale consacrée au cyberespace - Groupe libéral-radical, 24.9.2013

Interpellation 13.3033: Comment protéger les données personnelles des citoyens suisses détenues par des entreprises américaines? - Schwaab Jean-Christophe; Groupe socialiste, 6.3.2013

Interpellation 13.3726: Usurpation d'identité. Une lacune du droit pénal à combler ? - Schwaab Jean-Christophe; Groupe socialiste, 18.9.2013

Postulat 13.3678: Evaluer les risques de la monnaie en ligne bitcoin - Schwaab Jean-Christophe; Groupe socialiste, 11.9.2013

10. Tendances et menaces potentielles en 2014

Le nombre d'annonces reçues par le SCOCI ne permet pas de tirer de conclusions directes sur l'évolution effective de la cybercriminalité ou des contenus illégaux sur Internet, ou alors seulement de manière nuancée. Les chiffres reflètent simplement le comportement de la population en matière de communication. Les statistiques fournissent tout au plus des indications sur la manière dont la cybercriminalité est perçue dans notre société. Les déclarations suivantes sont basées sur des recherches d'informations "open source" et sur l'interprétation de ces sources par le SCOCI, qui tient compte de ses propres résultats opérationnels.

Augmentation des tentatives d'escroquerie abouties sur Internet

On a constaté tout au long de l'année que les tentatives d'escroquerie rapportées étaient de plus en plus sophistiquées, tant du point de vue de leur orthographe que de leur présentation. C'est le cas de presque toutes les catégories d'escroquerie, qu'il s'agisse de l'envoi de courriels de hameçonnage, de la création d'annonces et de réponses trompeuses sur des plates-formes ou d'écrans de blocage de rançongiciels. Il faut partir du principe que ces pratiques vont se poursuivre. Les utilisateurs d'Internet devraient avoir toujours plus de difficultés à déceler une escroquerie. Etant donné que bon nombre de ces tentatives d'escroquerie proviennent de pays d'Afrique du Nord et de l'Ouest, que leurs auteurs disposent d'un réseau complet de mules[11] et qu'ils savent utiliser à leurs fins les obstacles juridiques à la poursuite pénale de leurs actes, il est extrêmement difficile de lancer une procédure pénale à leur encontre. Il appartient donc aux exploitants des sites Internet de mettre davantage l'accent sur la prévention et les mesures d'ordre technique.

Economie souterraine de la cybercriminalité en hausse

Au cours de ces dernières années, une véritable économie souterraine s'est développée autour de la cybercriminalité, au sens large comme au sens strict. Sur Internet il est facile d'acheter, de manière rapide et anonyme, des prestations telles que la fabrication ciblée de maliciels, l'envoi d'e-mails de masse, le lancement d'attaques par déni de service, la création de faux comptes sur des réseaux sociaux, etc. Le paiement se fait exclusivement par le biais de devises quasi anonymes et virtuelles comme le bitcoin ou encore par le biais de ses plates-formes d'échange. Les prestations de prestataires de services financiers établis sur le plan international sont également appréciées car elles permettent d'envoyer de l'argent à peu de frais dans des pays situés à l'extérieur de l'Europe, sans avoir à décliner une identité véritable. Dans ces conditions, il est quasi impossible de suivre ces transferts de moyens financiers.

En raison de la situation économique qui prévaut en Europe, il faut s'attendre à ce que les acteurs de cette économie augmentent. Les méthodes traditionnelles d'investigation ne permettent pas de lutter efficacement contre ce phénomène. Pour dresser un bilan de cette économie et en identifier les acteurs principaux, il faudrait plutôt miser sur les investigations secrètes effectuées dans le cadre d'une coopération internationale. Pour la Suisse, cela signifie concrètement qu'un canton à lui seul ne sera vraisemblablement pas en mesure de poursuivre les auteurs de ces agisse-

[11] Agents financiers impliqués dans le blanchiment d'argent

ments. Il s'avérerait plus efficace de mener une procédure coordonnée impliquant une vue d'ensemble au niveau national, comme le prévoit la Stratégie nationale de protection de la Suisse contre les cyberrisques. Ces procédures pourraient être conduites par des groupes de travail communs placés sous la houlette d'un canton dirigeant ou encore de la Confédération.

Toujours plus de PME dans la ligne de mire

Etant donné le savoir-faire acquis dans l'économie souterraine de la cybercriminalité ainsi que la large utilisation de logiciels d'application, il faut partir de l'idée que les PME vont se retrouver de plus en plus dans la ligne de mire pour des vols de données effectués par des tiers. Les PME constituent une cible lucrative pour des cybercriminels, car les données dont elles disposent, comme les adresses e-mail, les mots de passe, les données de leurs interlocuteurs et leurs adresses postales revêtent une grande valeur dans l'économie souterraine de la cybercriminalité; qui plus est, leurs infrastructures ne présentent souvent pas les mêmes mécanismes de sécurité que les grandes banques par exemple. Il faut aussi se préparer à l'idée que les petites entreprises connaîtront davantage de tentatives d'extorsion avec vol préalable de données et d'attaques par déni de services (DDoS) sur leurs sites web. On s'attend notamment à une augmentation des tentatives d'extorsion effectuées à l'aide de "CryptoLocker". Ces maliciels cryptent les données contenues sur l'ordinateur, les rendant ainsi inutilisables. C'est alors que les malfrats exigent le paiement d'un montant déterminé.

Vol de certificats

Durant l'année 2013, le SCOCI a déjà été avisé de la perte de certificats[12] émis par des organismes de certification éminents; les certificats volés sont alors utilisés par des cybercriminels pour signer numériquement des maliciels et échapper ainsi aux dispositifs de sécurité tels que des scanners antivirus. Dès lors, l'un des principaux piliers de la sécurité sur Internet, à savoir la "chaîne de confiance" accordée aux organismes de certification, pourrait se trouver affaibli. Cela signifierait, pour les utilisateurs finaux, que des connexions à des serveurs web considérées comme sûres seraient susceptibles d'être interceptées par des criminels sans que cela ne se remarque et que l'échange de données pourrait être lu, dévié et modifié à des fins frauduleuses. Le navigateur continuerait toutefois d'indiquer à l'utilisateur final qu'il communique avec un serveur muni d'un certificat signé en bonne et due forme. Cela pourrait avoir de graves répercussions, notamment sur l'e-banking, le transfert de données lors d'achats en ligne et d'autres applications à sécurité critique.

Probable augmentation des maliciels visant les téléphones mobiles

Etant donné que l'utilisation d'Internet s'est déplacée majoritairement vers des appareils mobiles, l'augmentation du nombre de maliciels conçus pour infecter les téléphones portables, les smartphones et les tablettes pourrait s'en trouver accélérée. On ne peut exclure que la diffusion plus large de mécanismes d'authentification destinés aux systèmes d'e-banking qui exigent la présence d'un appareil de communica-

[12] Les certificats sont des identités numériques attribuées et certifiées par des services autorisés (organismes de certification). La signature de certificats destinés à des entités électroniques, notamment de serveurs web, par des services de certification, équivaut à l'établissement d'un passeport pour une personne réelle.

tion supplémentaire, comme les téléphones portables ou les smartphones, ne fasse également augmenter le nombre d'attaques contre ce type de systèmes, par le biais de maliciels. La multitude d'appareils de conceptions différentes, dont le maniement nécessite un savoir-faire particulier et un nombre croissant de spécialistes, constituera un défi d'ordre forensique croissant pour les corps de police cantonaux dont les services informatiques sont restreints, mais également un défi d'ordre financier.

11. Glossaire

Adult check	Procédé de vérification permettant de limiter l'accès d'un site *web* à un public majeur uniquement
Chat	Dialogue (sous forme écrite) en ligne.
Cloud computing	L'informatique en nuage permet d'accéder à la mémoire et aux capacités de calcul d'ordinateurs et de serveurs répartis dans le monde entier et liés par un réseau, tel Internet. Les applications et les données ne se trouvent plus sur l'ordinateur local, mais – par métaphore – dans un nuage (cloud), composé d'un certain nombre de serveurs distants, interconnectés au moyen d'une excellente bande passante, indispensable à la fluidité du système.
Peer-to-Peer	De l'anglais *peer-to-peer*, abrév. "P2P", pair à pair: modèle de réseau informatique permettant l'échange de fichiers entre utilisateurs (les pairs).
Pornographie dure	Actes d'ordre sexuel impliquant des enfants (pédophilie, pédopornographie), des animaux, des excréments humains, ou comprenant des actes de violence (art. 197, ch. 3, CP).
Valeurs de hash	Valeur unique permettant d'identifier une donnée, notamment une image (empreinte digitale numérique).
Hameçonnage (phishing)	De l'argot anglais *phreaking*, utilisation de fausses données d'accès et *fishing*, pêche. Désigne l'acquisition illicite sur Internet de données d'accès à des services en ligne, typiquement par le biais de l'envoi en masse d'e-mails provenant d'expéditeurs fictifs exigeant la "vérification" de données clients.
Proxy	De l'anglais *proxy*, mandataire: serveur informatique dont le rôle est de servir de relais entre un client (vous) et un serveur (le site web que vous souhaitez consulter).
Spam	Communication électronique non sollicitée, principalement effectuée en masse et à des fins publicitaires, ou parfois dans le but d'installer un logiciel malveillant.
Streaming	Mode de transmission de données audio et vidéo, transmises en flux continu, plutôt qu'après téléchargement complet (permet la lecture de contenu "en direct").
URL	De l'anglais *uniform ressource locator*, localisateur uniforme de ressources: chaîne de caractères combinant les informations nécessaires pour indiquer à un logiciel comment accéder à une ressource Internet.