Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol

Mars 2015

Rapport annuel 2014

Service de coordination de la lutte contre la criminalité sur Internet SCOCI

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

Office fédéral de la police fedpol

Service de Coordination de la lutte contre la criminalité sur Internet
Nussbaumstrasse 29
3003 Berne

www.kobik.ch
www.cybercrime.ch

Publié le : 26 Mars 2015

Photographie : Thinkstock, SCOCI

Avant-propos

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

"Ta Panta Rhei", tout passe, tout coule: comme d'habitude, le SCOCI doit aller de l'avant, s'adapter aux évolutions du monde, relever de nouveaux défis, acquérir de l'expérience, se remettre en question et toujours améliorer ses services. C'est son mot d'ordre absolu.

Au printemps dernier, les autorités allemandes ont alerté le SCOCI sur un cas d'usurpation d'identité de grande ampleur. Les malfaiteurs tentaient de se connecter à des comptes e-mail au moyen des adresses et mots de passe y afférents et de les utiliser à mauvais escient pour envoyer des pourriels. La réaction du SCOCI a été rapide et pragmatique. Les fournisseurs d'accès et plus de 38 000 citoyens ont été informés personnellement de la fraude dès le lendemain. L'écho a été plus que positif. Cette affaire a permis au SCOCI de prouver qu'il est capable de réagir dans les plus brefs délais à des situations inattendues.

Le SCOCI coopère de manière proactive avec Interpol, Europol, le FBI, le Homeland Security Investigations et bien d'autres autorités étrangères. Il représente la Suisse au sein de groupes de travail internationaux conjointement avec les partenaires suivants: les ministères publics suisses, les polices cantonales, des représentants du secteur financier, les fournisseurs d'accès à Internet, MELANI, SWITCH Noms de domaines ainsi que des ONG. Y participent aussi la Prévention suisse de la criminalité, le Service de renseignement de la Confédération, le DFAE et d'autres services fédéraux et cantonaux. Si la Suisse veut pouvoir compter sur une aide même en temps difficiles, elle doit entretenir des contacts personnels et cultiver des amitiés au niveau international, comme n'a cessé de le répéter l'ancien conseiller fédéral Adolf Ogi.

Le démantèlement des réseaux de zombies illégaux, c'est-à-dire de systèmes informatiques infectés, ainsi que la coordination d'opérations nationales pour arrêter les cybercriminels font partie des tâches relevant de cette coopération internationale. La présence dans des organes internationaux ou des alliances, comme l'Alliance mondiale, visant à lutter contre la pédocriminalité sur Internet est elle aussi capitale. Mais il s'agit avant tout d'instaurer la confiance et de la conserver par un travail de qualité. A cet égard, le SCOCI reste un partenaire apprécié et reconnu dans le combat contre le crime sur Internet.

A l'avenir non plus, le SCOCI ne pourra se plaindre de manquer de travail ou de défis à relever. Les attaques virtuelles de banques dont le butin atteint le milliard, les saisies record de matériel pédopornographique ou les dommages à hauteur de millions que l'ingénierie sociale cause à des PME suisses montrent entre autres que les dix collaborateurs du SCOCI – qui est financé aux deux tiers par les cantons et à un tiers par la Confédération – et les six autres collaborateurs de fedpol qui les soutiennent ont beaucoup à faire. Le SCOCI doit par ailleurs soumettre au Conseil fédéral d'ici fin 2016 le concept relatif à la mise en œuvre de la mesure 6 de la Stratégie nationale de protection de la Suisse contre les cyberrisques (M6 SNPC). A ce sujet, les travaux portent à ce jour sur une vue d'ensemble nationale des cas et sur la coordination de cas complexes intercantonaux.

Le SCOCI est très sollicité. Pas un jour ne passe sans que les médias ne se fassent l'écho d'un nouveau cas plus important encore de cybercriminalité. Peut-être le plus grand défi que le SCOCI doit relever est-il de faire comprendre aux décideurs l'ampleur du fléau. Ce qu'il faut, ce sont de bonnes conditions-cadres et donc des investissements dans la sécurité, même si cela a un prix.

Table des matières

1 L'essentiel en bref

- En 2014, le SCOCI a reçu au total 10 214 annonces via son formulaire en ligne, ce qui représente une augmentation de 10,9 % par rapport à 2013.
- 66,9 % des annonces concernaient des infractions contre le patrimoine, lesquelles ont continué d'augmenter par rapport aux infractions contre l'intégrité sexuelle. Ainsi, la tendance observée les années précédentes s'est poursuivie en 2014.
- Dans 50 cas, la pertinence pénale de l'annonce a conduit à la transmission directe des faits à des autorités ou organisations nationales ou internationales.
- Les recherches actives sur les réseaux *peer-to-peer* (P2P) ont permis au SCOCI d'identifier, au cours de l'année sous revue, 86 raccordements Internet utilisés pour échanger activement de la pédopornographie.
- Des investigations préliminaires secrètes en vertu de la législation sur la police du canton de Schwyz et des investigations secrètes en vertu du code de procédure pénale (CPP) menées par le SCOCI ont abouti en 2014 à 29 dénonciations aux autorités cantonales compétentes et à 281 dénonciations aux autorités de poursuite pénale étrangères.
- Plus d'un millier d'annonces concernant des sites Internet aux contenus pénalement répréhensibles ont été transmises à des autorités étrangères via Interpol/Europol ou via des organisations affiliées (par ex. INHOPE).
- Les travaux de mise en œuvre de la mesure 6 de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) sont en cours.

2 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 via un 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. Quand le SCOCI ne peut répondre directement aux demandes des citoyens, il les adresse aux services compétents ou aux autorités de poursuite pénale localement compétentes.

2.1 Nombre d'annonces reçues

Entre le 1er janvier 2014 et le 31 décembre 2014, un total de 10 214 annonces et demandes sont parvenues au SCOCI via son formulaire mis en ligne sur le site www.cybercrime.ch, ce qui constitue une augmentation de 10,9 % par rapport à l'année précédente (9208 annonces).

Le nombre d'annonces reçues ne permet pas de tirer de conclusions pertinentes sur l'ampleur réelle de la cybercriminalité et l'augmentation ou la diminution des contenus illégaux sur Internet. Il ne reflète que la manière dont la population perçoit les contenus et agissements délictueux sur Internet et la volonté de communiquer activement ces soupçons à la police et à d'autres autorités.

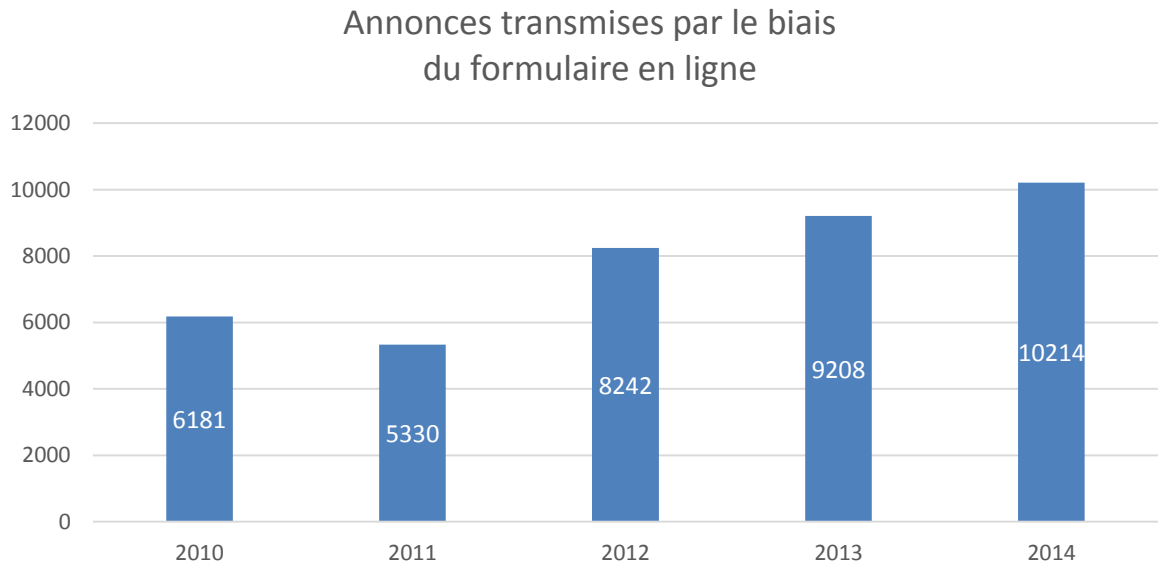

Illustration 1: annonces reçues par année via le site www.cybercrime.ch

La moyenne mensuelle du nombre d'annonces reçues se monte à 851. Les variations déjà constatées les deux années précédentes entre le mois de mai (1024 annonces) et fin septembre (837 annonces) ou début octobre (680 annonces) se sont confirmées en 2014. Comme en 2013, les annonces relatives au hameçonnage et aux tentatives d'escroquerie ont augmenté en mai et baissé en septembre et en octobre. La hausse des annonces en mai a conduit le SCOCI à publier quatre alertes sur les réseaux sociaux et sur son site. Cette augmentation pourrait s'expliquer par la fluctuation du marché de pourriels et d'e-mails de hameçonnage durant les vacances d'été aux Etats-Unis (fin mai – fin août), fluctuation qui a été constatée

par les principaux producteurs d'antivirus. Les données dont dispose le SCOCI ne permettent toutefois pas d'établir un lien de cause à effet entre cette fluctuation et le nombre d'annonces reçues.

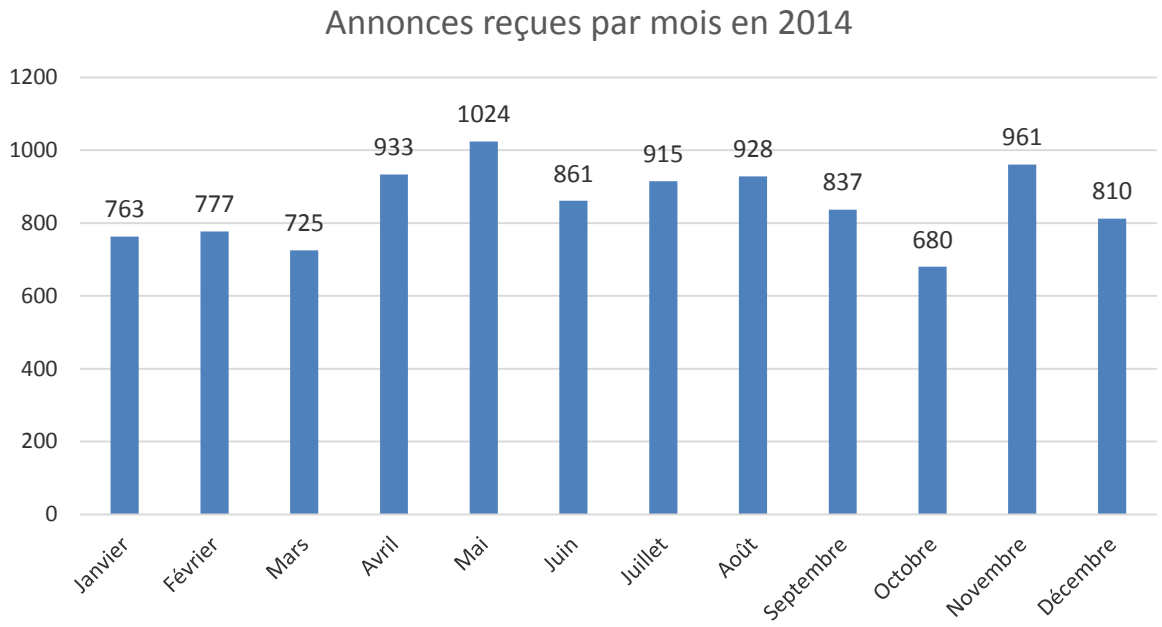

Illustration 2: annonces reçues par mois via le site www.cybercrime.ch (total: 10 214 annonces)

2.2 Types d'infractions enregistrées

Les types de criminalité signalés au SCOCI se répartissent en deux domaines qui se recoupent. Par cybercriminalité au sens strict du terme, on entend les infractions commises au moyen des technologies offertes par Internet ou qui profitent des faiblesses de ces technologies. A titre d'exemples, on peut citer des phénomènes comme le piratage informatique, l'attaque par déni de service ou la création et la mise en circuit de maliciels. Ces infractions sont apparues avec Internet et ne visent que ses technologies. La cybercriminalité au sens large, quant à elle, se sert d'Internet comme moyen de communication et fait un usage abusif des possibilités existantes que sont notamment la communication par courrier électronique ou l'échange de fichiers à des fins malhonnêtes. En font par exemple partie les arnaques sur les plates-formes de petites annonces ou la diffusion de pornographie interdite.

Quelque 87,7 % des annonces reçues en 2014 se sont avérées pertinentes du point de vue pénal, et près de 88,6 % d'entre elles ont présenté un lien avec le CP[1]. Les autres annonces concernaient entre autres des infractions à la LCD[2], à la LDA[3], à la LPM[4], à la LStup[5] et à la LBA[6] (11,4 % au total, cf. chap. 2.2.3, illustration 9).

[1] Code pénal suisse du 21 décembre 1937, RS 311.0

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

[3] Loi du 9 octobre 1992 sur le droit d'auteur, RS 231.1

[4] Loi du 28 août 1992 sur la protection des marques, RS 232.11

[5] Loi du 3 octobre 1951 sur les stupéfiants, RS 812.121

[6] Loi du 10 octobre 1997 sur le blanchiment d'argent, RS 955.0

Dans 12 % des cas environ, le SCOCI n'a pas pu constater de pertinence pénale quant aux contenus examinés. Ce pourcentage comprend également les demandes qui lui ont été soumises sans contexte délictueux.

Si les faits signalés n'étaient pas poursuivis d'office et nécessitaient par conséquent une plainte par la personne lésée pour qu'une procédure soit ouverte, le SCOCI renvoyait les auteurs de l'annonce vers les services de police cantonaux compétents en la matière.

Par rapport aux autres annonces relevant de la justice pénale, le pourcentage des annonces qui concernaient des infractions contre le patrimoine a de nouveau augmenté. Au total, 6837 annonces (66,9 %) relevaient de ce domaine (art. 137 à 172ter CP). Avec 7,4 % des annonces reçues (758), les infractions contre l'intégrité sexuelle (art. 187 à 212 CP) figurent en deuxième position. Par rapport à l'année précédente, le nombre absolu de ces annonces a de nouveau diminué massivement (de 1842 à 758 annonces, soit une baisse de 58,8 %). Il convient ici de souligner qu'avec l'entrée en vigueur de la révision du CP le 1er juillet 2014, la possession et la diffusion de pornographie dure incluant des excréments n'est plus punissable (cf. à ce sujet également le chap. 2.2.2).

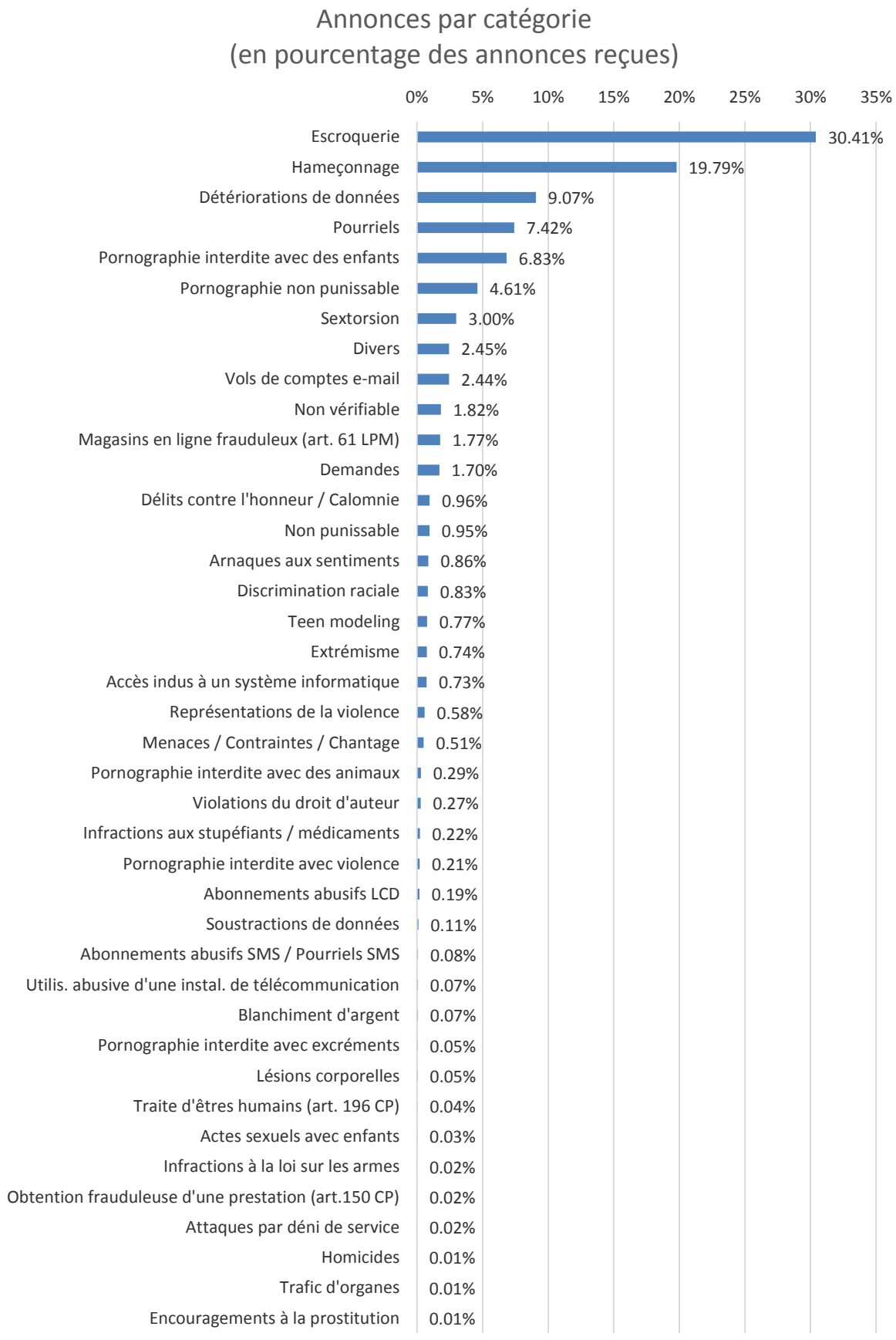

Illustration 3: importance des catégories sur l'ensemble des annonces reçues en 2014 (total: 10 214 annonces)

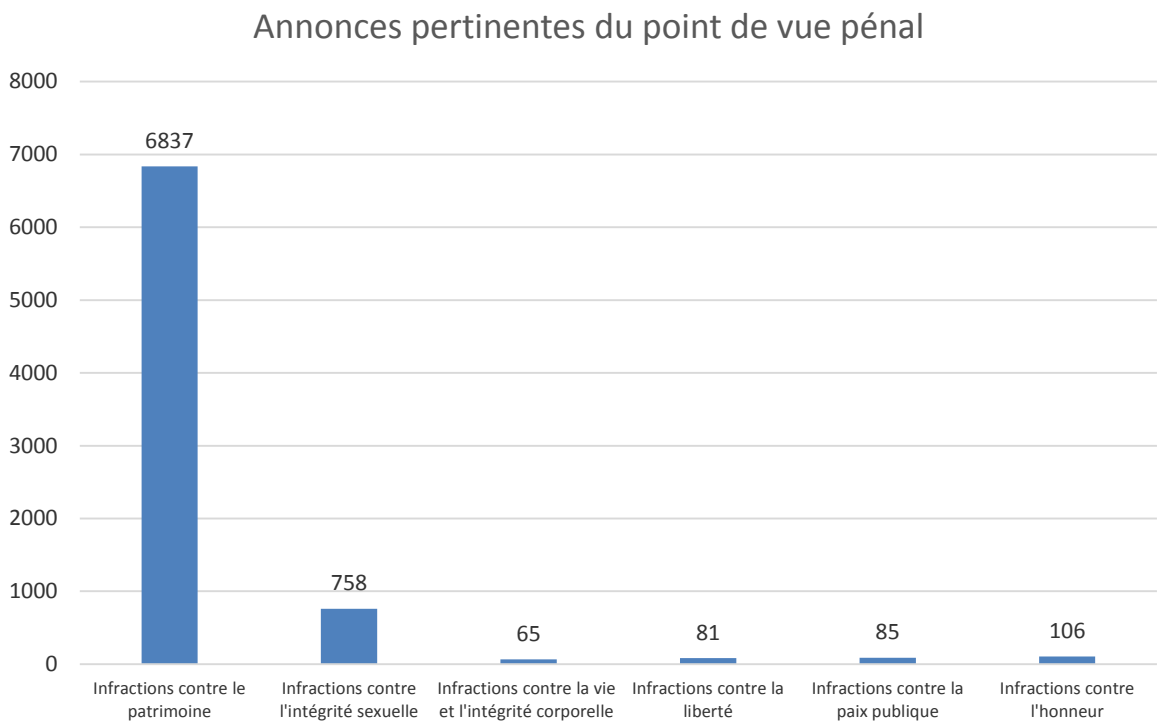

Illustration 4: annonces reçues en 2014, classées par catégorie d'infraction au CP (total: 7932 annonces)

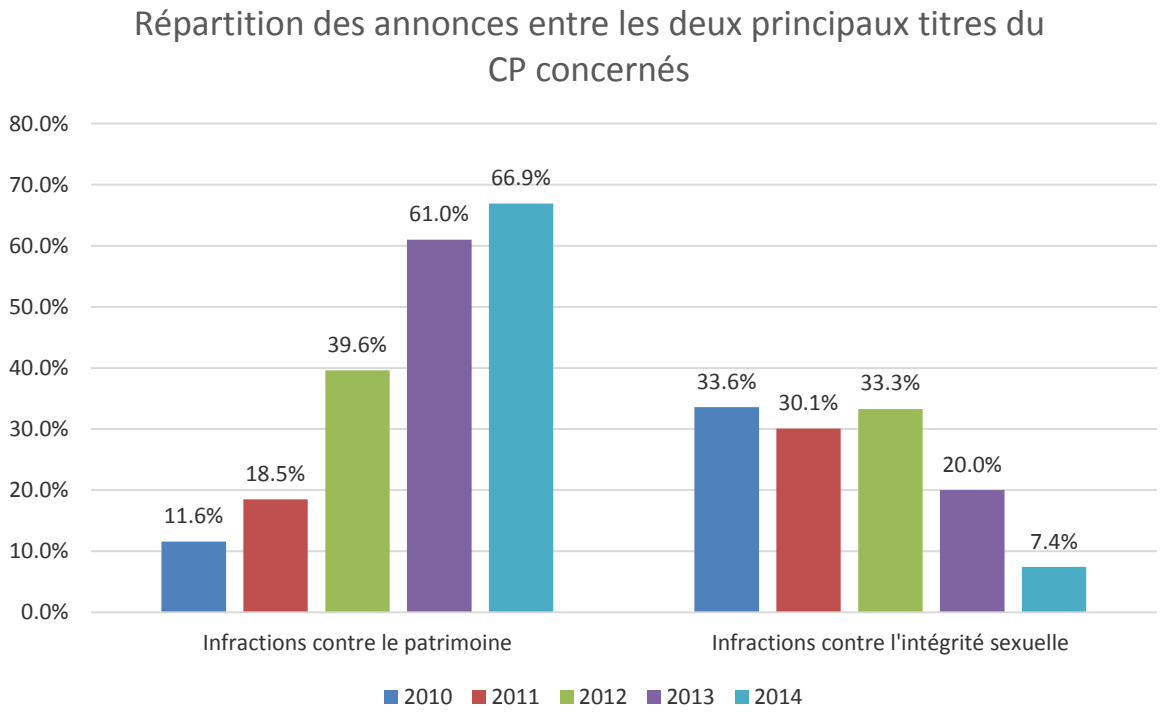

Illustration 5: évolution de la répartition des infractions selon les titres 2 et 5 du CP, 2010-2014

2.2.1 Infractions contre le patrimoine

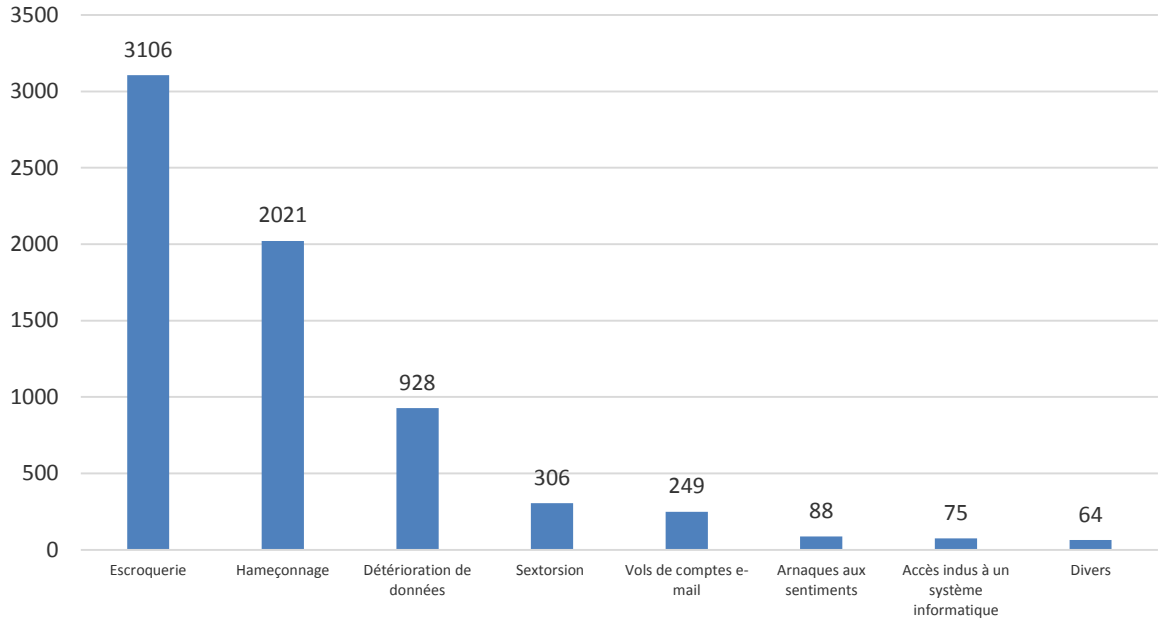

Illustration 6: annonces reçues en 2014 concernant des infractions contre le patrimoine (total: 6837 annonces)

66,9 % de l'ensemble des annonces concernaient des infractions contre le patrimoine (6837 annonces). Cette augmentation semble liée aux résultats issus de recherches de sources indépendantes telles que les rapports trimestriels de producteurs d'antivirus ou de chercheurs en sécurité Internet, qui constatent une augmentation constante dans le monde du volume de pourriels et de hameçonnages ainsi que du nombre d'infections par maliciels et de familles de maliciels nouvellement décelées. Si la liste ci-dessous des phénomènes signalés n'est pas exhaustive, elle en donne toutefois un bon aperçu.

2.2.1.1 Tentatives d'escroquerie (cybercriminalité au sens large)

Avec 30,4 % du nombre d'annonces reçues (soit 3106), les tentatives d'escroquerie représentent la majeure partie de l'ensemble des annonces. Aucune variation notable dans les modes opératoires déjà connus n'a été constatée par rapport à l'année précédente pour ce qui est de la cybercriminalité au sens large.

Au cours de l'année sous revue, de nombreuses tentatives d'escroquerie concernaient aussi de fausses annonces publiées sur des plates-formes d'enchères et de petites annonces. Les cibles visées sont d'abord les internautes qui se rendent sur ces sites. Les victimes potentielles sont attirées par des offres extrêmement alléchantes portant sur des produits généralement convoités, comme des smartphones de marque ou certains modèles de voiture. L'objectif des malfaiteurs est de les inciter à verser un acompte justifié par les conditions très avantageuses alors qu'ils ne livreront jamais la marchandise promise.

Des tentatives d'escroquerie au moyen de fausses annonces immobilières ont par ailleurs été souvent communiquées. Les criminels profitent ici de la pénurie de logements dans les grandes villes suisses comme Zurich et Bâle et mettent en ligne des biens au loyer modéré mais qui n'existent pas. Moyennant jusqu'à trois mois de loyer à titre de caution, ils promettent à la victime qu'elle pourra emménager sans délai dans le logement ou au moins que les clés lui seront envoyées pour une visite. La bonne affaire se révèle être une escroquerie au plus tard lors de la première visite à l'adresse inexistante.

Les malfaiteurs ne ciblent toutefois pas seulement les acheteurs, mais aussi les vendeurs et les personnes qui passent une annonce. Par exemple, ils répondent à des annonces pour de l'électroménager et tentent de convaincre le vendeur d'envoyer la marchandise à l'étranger en lui proposant même de payer un prix plus élevé que celui demandé initialement. Ils essaient souvent de faire croire que certains articles électroménagers disponibles en Suisse sur des sites de petites annonces ne peuvent pas être achetés à l'étranger. Ils indiquent représenter une tierce personne non domiciliée en Suisse, raison pour laquelle cette dernière ne peut elle-même se charger de la transaction. Si la victime potentielle accepte de conclure l'affaire, elle est invitée à envoyer la marchandise. Mais la somme convenue n'est généralement jamais versée. Variante de cette forme d'escroquerie : le malfaiteur tente de convaincre le vendeur de se faire payer via un service en ligne. Il envoie alors au vendeur une fausse confirmation de paiement, pour un montant souvent supérieur à celui demandé. Via un e-mail provenant en apparence du prestataire de paiement en ligne, la victime est sommée de payer des frais relatifs à des prestations y afférentes (douane, transport par bateau, etc.). Par e-mails, le malfaiteur accompagne pas à pas le vendeur dans ces opérations et, pour prévenir tout soupçon qui pourrait naître, lui promet de prendre à sa charge l'ensemble des frais. En réalité, les e-mails et créances apparemment envoyés par le prestataire de paiement en ligne provenaient de l'escroc lui-même, qui empochait toutes les sommes versées, flouant ainsi le vendeur, lequel en outre avait déjà envoyé la marchandise.

De plus en plus de petites et moyennes entreprises (PME) tombent elles aussi dans les filets des cybercriminels, qui déploient des efforts considérables pour obtenir des informations sur leurs modalités de paiement. Par exemple, les malfaiteurs se renseignent dans un premier temps sur des personnes travaillant dans des entreprises entretenant des contacts réguliers avec des fiduciaires ou des banques. Ils tentent également d'obtenir des renseignements sur les modalités de paiement et les paiements en suspens au moyen des données d'accès e-mail volées par hameçonnage. Les malfaiteurs utilisent alors ces informations et envoient de faux e-mails aux conseillers clients des banques ou des fiduciaires au nom des entreprises concernées pour leur demander de transférer ou de déclencher des paiements. Cette combine peut être extrêmement rentable; dans les cas signalés, les sommes ainsi engrangées allaient de quelques centaines à plusieurs dizaines de milliers de francs. Sur la base des annonces reçues par les autorités cantonales de police (cf. chap. 4), la somme totale du dommage en Suisse est déjà estimée à plusieurs millions de francs.

2.2.1.2 Sextorsion (cybercriminalité au sens large)

Le SCOCI a reçu ses premières annonces de "sextorsion" (combinaison à partir des mots "sexe" et "extorsion") dès l'année 2013. Les victimes, principalement des hommes, indiquaient avoir été approchées sur des réseaux sociaux et des sites de rencontre en ligne par des escrocs inconnus, apparemment de sexe féminin. La conversation était alors déplacée vers des services de discussion par vidéo. La femme commençait à se dévêtir devant la caméra et incitait son interlocuteur à des actes d'ordre sexuel, qui étaient enregistrés à son insu. Les malfaiteurs menaçaient ensuite par e-mail de publier la vidéo compromettante si une rançon, de quelques centaines de francs en général, n'était pas payée. Dans les cas signalés, la vidéo était mise en ligne sur des plates-formes de réseaux sociaux malgré le versement de la rançon. Les malfaiteurs continuaient de faire chanter les victimes et leur demandaient de verser des rançons dont le montant ne faisait qu'augmenter.

2.2.1.3 Hameçonnage (cybercriminalité aux sens strict et large)

Avec 2021 annonces (19,8 %), le nombre de tentatives de hameçonnage signalées a légèrement reculé (-8,5 %) par rapport à l'année précédente (2208 annonces). Les tentatives de hameçonnage consistent à envoyer massivement des e-mails au plus grand nombre possible de personnes, sans ciblage particulier, et à essayer de les attirer sur des sites web s'inspirant de prestataires Internet connus, où les victimes doivent s'identifier (nom d'utilisateur, mot de passe). Les malfaiteurs ne s'intéressent pas seulement aux services d'e-banking ou aux prestataires de paiements en ligne, mais aussi aux données d'accès à des plates-formes d'achats et de ventes aux enchères, à des services de sauvegarde dans le *cloud*, à des sites de téléchargement de musique et à des marchés d'applications pour smartphones.

Au cours de l'année sous revue, les sites signalés se trouvaient sur des serveurs de personnes tierces utilisés abusivement par les criminels. Par exemple, ces derniers profitaient de lacunes de sécurité dans les systèmes de gestion de contenus pour installer sur le serveur web une page de hameçonnage. Dans certains cas, l'envoi d'e-mails de hameçonnage s'est fait de la même manière via des serveurs web utilisés abusivement ou au moyen de réseaux de zombies.

2.2.1.4 Rançongiciels de police (cybercriminalité au sens strict)

Le rançongiciel (combinaison de "rançon" et de "logiciel") de police désigne une forme de logiciel malveillant qui bloque l'ordinateur d'un utilisateur et exige de ce dernier une rançon de quelques centaines de francs, payables via un prestataire en ligne anonyme, pour débloquer le système. A la demande d'argent s'ajoute une pression psychologique, dans la mesure où des logos officiels de services de police ou d'autres organisations gouvernementales s'affichent sur la page de blocage. Les ordinateurs sont infectés par exemple lorsque l'utilisateur, machinalement, ouvre une pièce jointe à un e-mail ou se rend sur un site Internet conçu à cet effet. La diffusion de ce logiciel malveillant n'est pas ciblée, l'objectif des malfaiteurs étant surtout de maximiser le profit à partir du plus grand nombre possible d’ordinateurs infectés. Au contraire des Trojans encodeurs décrits ci-dessus, il est relativement facile pour quiconque s'y connaît de nettoyer un système infecté et d'en restaurer les données.

2.2.1.5 Crypto-rançongiciels (cybercriminalité au sens strict)

Les annonces concernant des Trojans encodeurs (crypto-rançongiciels, combinaison de "cryptographie" – en référence aux techniques de chiffrement – et de "rançongiciel") ont commencé à augmenter dès le second semestre 2013. Ce type de maliciel est diffusé sur le même mode que les rançongiciels de police via des pièces jointes à des e-mails et des sites web spécialement conçus. Si l'ordinateur de l'utilisateur s'infecte, le logiciel chiffre en arrière-plan tous les fichiers des applications ouvertes, par exemple les documents créés via des solutions Office ou des fichiers audio et vidéo. Les données sont ainsi rendues inutilisables, et, dans le pire des cas, ne peuvent pas être restaurées par des spécialistes ou seulement moyennant des efforts considérables. L'utilisateur est ensuite informé du chiffrement et sommé de payer un certain montant en monnaie virtuelle pour que les fichiers soient décryptés. Et même si la somme demandée est payée, rien ne garantit que les malfaiteurs annulent le chiffrement.

2.2.1.6 Chevaux de Troie e-banking et enregistreurs de frappes (cybercriminalité au sens strict)

Au cours de l'année sous revue, de nombreux e-mails suspects auxquels étaient joints des maliciels visant des systèmes d'e-banking ont été signalés. Les malfaiteurs rédigent les textes de ces e-mails de telle sorte que les destinataires soient incités à ouvrir la pièce jointe, permettant ainsi au logiciel malveillant de s'installer. Il est par exemple écrit dans le texte du message que la pièce jointe contient une facture en souffrance d'une grande maison de vente par correspondance. Dans d'autres cas, le texte indique que la pièce jointe contient une liste de communications mobiles à l'étranger. Une fois installé, le maliciel est en mesure de s'immiscer dans les sessions d'e-banking ouvertes par l'utilisateur et de modifier les contenus qui s'affichent sur le navigateur. L'utilisateur a simplement l'impression que des travaux de maintenance sont en cours, alors qu'en réalité, des transactions sont effectuées en arrière-plan. Les différentes variantes de maliciels peuvent en outre enregistrer les frappes sur le clavier et le trafic réseau, permettant aux malfaiteurs d'usurper les identifiants et les mots de passe.

2.2.2 Infractions contre l'intégrité sexuelle

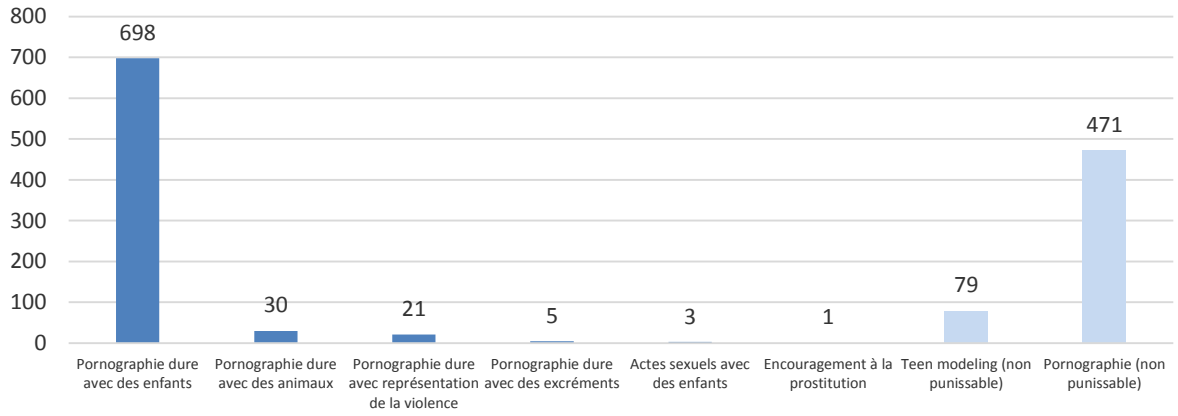

Illustration 7: annonces reçues en 2014 concernant des infractions contre l'intégrité sexuelle (total: 758 annonces)

Le nombre d'annonces relatives à des infractions contre l'intégrité sexuelle, passant de 1842 l'année précédente à 758, a de nouveau sensiblement baissé au cours de l'année sous revue (-58,8 %).

Le nombre de sites Internet signalés proposant de la pornographie interdite avec des enfants a de nouveau clairement chuté, passant de 1414 en 2013 à 698 (-50,6 %). Il convient de souligner qu'une modification de loi est entrée en vigueur le 1er juillet 2014 annulant l'interdiction de fabrication et de diffusion de pornographie avec excréments. De ce fait, des annonces reçues après cette date n'étaient plus répréhensibles pénalement et ont été classées dans la catégorie "non punissable".

Le SCOCI a en outre reçu 79 annonces portant sur des sites qui montraient des images de "teen modeling". Ces contenus ne sont pas de nature pornographique au sens du CP et ne peuvent donc donner lieu à des poursuites pénales. Ils montrent par exemple des adolescents prenant des poses suggestives ou vêtus d'habits provocants ou excitants inadaptés à leur âge. Bien que ces images ne soient pas considérées comme de la pédopornographie au sens pénal, elles sont souvent perçues comme telles par les internautes, qui les communiquent alors au SCOCI.

D'autres cas, au nombre de 471, ont été signalés au SCOCI parce qu'ils semblaient relever de la pornographie interdite, mais se sont avérés non pertinents du point de vue pénal après examen approfondi. Il s'agissait par exemple de sites web pornographiques avec excréments (qui ne sont plus pénalement punissables depuis le 1er juillet) ou de sites qui ont été perçus comme choquants du fait des pratiques sexuelles représentées. Ces cas ne sont donc pas recensés dans les statistiques des infractions relevant de la justice pénale contre l'intégrité sexuelle.

Le SCOCI explique la baisse des annonces concernant des infractions contre l'intégrité sexuelle par une plus grande efficacité dans son traitement de la liste de blocage ainsi que par la bonne coopération avec les fournisseurs d'accès à Internet (FAI) et Interpol. Il apporte à ce propos une contribution importante à l'établissement de la liste "worst of" d'Interpol (cf. chap. 6). Grâce à la collaboration de nombreux moteurs de recherche comme Google et Microsoft avec Interpol, de nombreux sites ne sont plus du tout indexés. Le SCOCI estime que cette collaboration et la meilleure efficacité de la liste de blocage dans la collaboration avec les fournisseurs pourraient être une raison de la baisse des annonces concernant de tels sites, puisque les citoyens y sont de ce fait moins confrontés. La collaboration proactive avec Interpol dans l'établissement de la liste "worst of" mais aussi avec les FAI suisses permet au SCOCI d'apporter une contribution importante au recul de la disponibilité de matériel interdit sur Internet et donc à la "revictimisation" des personnes lésées par une consommation renouvelée des abus conservés en images par les consommateurs de pornographie interdite.

La baisse des annonces pourrait également être liée à la tendance déjà constatée depuis 2012 selon laquelle les contenus pornographiques interdits sont échangés dans des domaines Internet qui ne sont pas accessibles à tous, comme les réseaux Tor ("The Onion Router") ou I2P ("Invisible Internet Project"), ou selon laquelle les criminels se tournent vers des solutions de *peer-to-peer* (cf. chap. 3.2).

2.2.3 Autres infractions

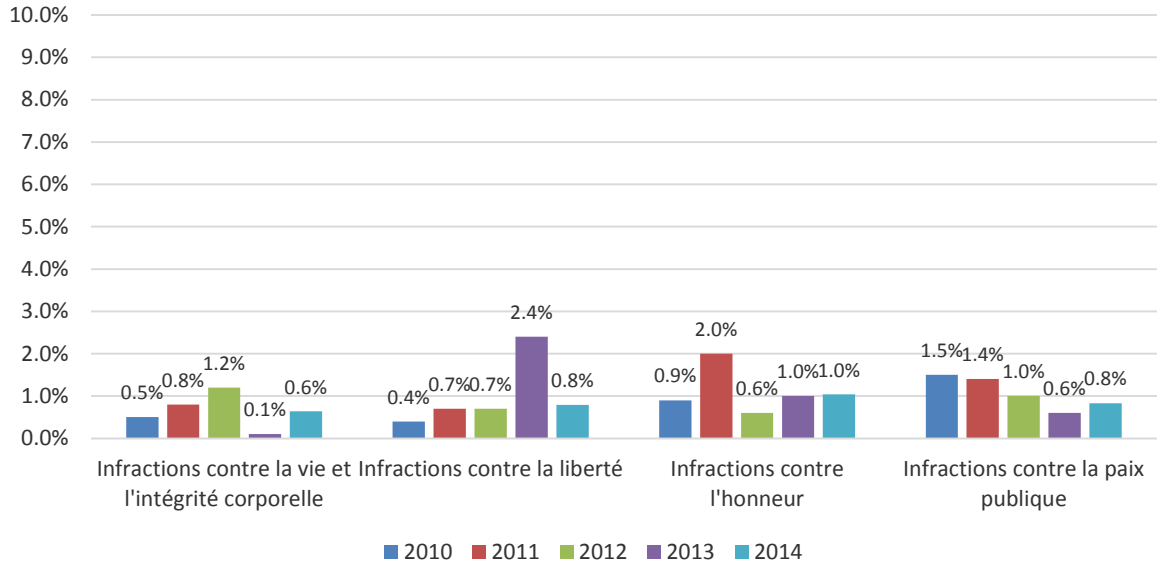

Illustration 8: annonces reçues de 2010 à 2014 concernant d'autres titres du CP (en pour cent de l'ensemble des annonces)

Quelque 4 % du volume des annonces concernaient 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. Ont été enregistrées 85 annonces portant sur des infractions pénales contre la paix publique; il s'agissait le plus souvent de propos discriminatoires ou extrémistes sur des réseaux sociaux. Si le nombre d'annonces sur ces thèmes reste au même niveau que ces dernières années, leur nombre absolu a malgré tout connu une légère augmentation.

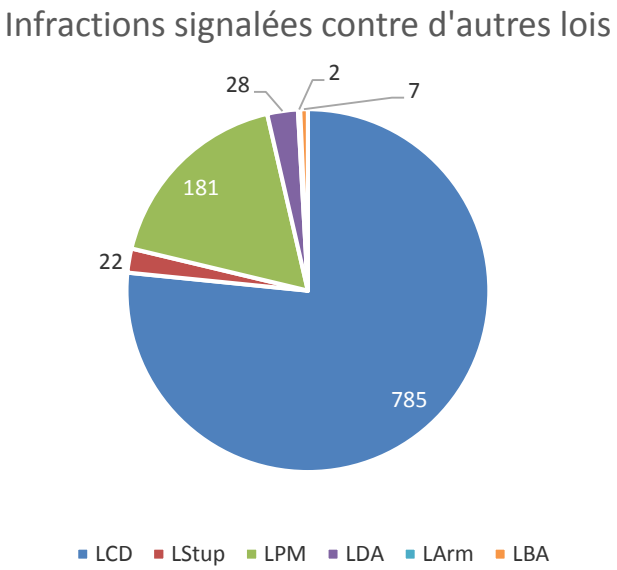

Illustration 9: répartition des infractions signalées en 2014 contre d'autres lois (au total 10 % du volume total des annonces)

Dans 10 % des annonces environ, un lien avec d'autres lois a été constaté. La LCD était de loin la plus souvent concernée, qui comprend toutes les annonces quant à des e-mails publicitaires indésirables (pourriels).

Au cours de l'année sous revue, 181 magasins en ligne potentiellement frauduleux et cas de piratage de produits sur de faux sites de fabricants d'articles de marque ont été signalés. Il s'agissait le plus souvent de magasins en ligne qui se présentaient comme vendeurs discount d'articles de luxe et de marque (articles de sport, lunettes de soleil, sacs de créateurs, etc.). Si une commande est passée sur ces sites à un prix très inférieur à celui indiqué par le fabricant, soit aucune marchandise n'est livrée, soit ce sont des contrefaçons de très mauvaise facture qui sont envoyées. Dans 76 cas, ces magasins en ligne frauduleux étaient accessibles sous un nom de domaine .ch.

Supprimer de tels contenus en dehors de toute procédure pénale prend beaucoup de temps. En cas de soupçon, le SCOCI doit alors demander au bureau d'enregistrement SWITCH une adresse suisse valable du propriétaire du domaine. C'est seulement grâce aux conditions générales de SWITCH qu'il est possible de faire supprimer le nom de domaine concerné après un délai d'attente de 30 jours, dans la mesure où les propriétaires, le plus souvent, ne donnent pas suite à ce genre de sommations.

2.2.4 Synthèse

La part et le nombre total d'annonces relatives à des infractions contre le patrimoine ont continué d'augmenter en 2014 aussi, ce qui confirme la tendance des années précédentes. Dans le même temps, le nombre d'annonces concernant des infractions contre l'intégrité sexuelle est en recul, là encore dans la droite ligne des tendances observées auparavant. La part des annonces relatives à d'autres titres du CP et à d'autres contenus pertinents sur le plan pénal reste la même.

Les phénomènes observés en 2014 ne sont pas fondamentalement nouveaux, mais les modes opératoires diffèrent légèrement de ceux constatés les années précédentes. On assiste également à une augmentation de la qualité des contenus délictueux. La grammaire et l'orthographe des e-mails de hameçonnage ou des petites annonces ne cessent d'être améliorées. De même, la présentation visuelle d'annonces, de pages de hameçonnage et d'e-mails est de plus en plus professionnelle, de sorte que l'internaute a du mal à distinguer un vrai site d'un faux.

2.3 Résultats

Le SCOCI exécute différentes tâches sur la base des annonces reçues via le formulaire en ligne. Il prend des mesures visant à supprimer les contenus pénalement punissables ou transmet les annonces aux autorités de poursuite pénale compétentes.

- Au total, 10 214 annonces ont été examinées et appréciées sous l'angle de leur éventuelle pertinence du point de vue pénal.
- Dans 3218 cas sur 10 214, les personnes à l'origine de l'annonce ont reçu une réponse personnelle.
- Parce qu'elles étaient pertinentes sur le plan pénal, 50 annonces ont conduit directement à la transmission des faits à l'autorité ou au canton compétent.

- Plus d'un millier d'annonces concernant des sites Internet aux contenus pénalement répréhensibles ont été transmises à des autorités étrangères via Interpol/Europol ou des organisations affiliées (comme INHOPE).
- De nombreuses annonces ont par ailleurs conduit à la transmission en interne d'indices au Commissariat Criminalité générale, organisée et financière et au Commissariat Pédocriminalité et pornographie de la Police judiciaire fédérale (PJF) et au Bureau de communication en matière de blanchiment d'argent (MROS).
- Les faits souvent signalés ont donné lieu à la publication d'un total de 27 mises en garde sur le site www.cybercrime.ch administré par le SCOCI. Depuis fin 2013, ces alertes sont également mises en ligne par le SCOCI sur Facebook et Twitter. Les organisations partenaires que sont la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), la Prévention suisse de la criminalité (PSC) mais également les médias sont eux aussi directement informés des dangers actuels, ce qui permet d'atteindre une large frange de la population.

2.4 Exemples de cas

Le SCOCI a été informé qu'un utilisateur avait filmé à leur insu des visiteurs, de sexe féminin pour la plupart, d'un établissement de bains suisse puis avait publié les enregistrements sur une plate-forme de vidéos pornographiques. Ces vidéos montraient souvent la poitrine et le postérieur des jeunes femmes et étaient accompagnées d'un titre et de descriptions sexistes et attentatoires à l'honneur. L'une des victimes ayant recouru aux médias, plusieurs dénonciations pour infractions contre l'honneur ont été déposées auprès de la police cantonale compétente. Celle-ci, grâce au soutien du SCOCI, est parvenue à identifier l'auteur des vidéos et propriétaire du profil, en collaboration avec les exploitants du site, et à l'arrêter.

Sur la base des annonces que lui transmettent les citoyens, le SCOCI rédige des alertes qu'il publie sur son site Internet et sur les réseaux sociaux, produisant ainsi un effet préventif. Par exemple, des utilisateurs d'un réseau social se sont adressés à lui en avril parce qu'ils avaient reçu une annonce pour un concours mettant en jeu une voiture. Il était indiqué dans cette annonce que le concours était organisé par les représentations française et suisse du constructeur. Il suffisait pour participer de donner son numéro de téléphone. Cette fausse annonce cachait en réalité un abonnement piège: la saisie du numéro de mobile sur le site du concours conduisait à la conclusion d'un abonnement pour un service mobile payant. Une heure à peine après avoir reçu une plainte de la part d'un citoyen via le formulaire en ligne, le SCOCI publiait une alerte sur les réseaux sociaux, alerte qui a été reprise et diffusée par différents médias nationaux et internationaux et par la Prévention suisse de la criminalité.

3 Recherches actives par le SCOCI

Chaque année, le comité directeur du SCOCI décide sur quels domaines de la cybercriminalité les recherches actives seront axées. En 2014 aussi, comme les années précédentes, la lutte contre la pédocriminalité sur Internet a été déclarée prioritaire. Toutefois, il a également été convenu que le SCOCI entreprendrait des recherches relatives aux infractions contre le patrimoine, ces dernières étant en forte augmentation depuis 2012. Cette décision s'est notamment concrétisée dans les tâches de coordination du SCOCI (cf. chap. 4), qui portent majoritairement sur la sécurisation du flux d'informations dans les opérations entre des services suisses et étrangers.

Les recherches actives ont permis d'établir 396 dénonciations en 2014, qui ont été transmises aux autorités compétentes en Suisse et à l'étranger. Ce chiffre est en légère baisse, de 6,4 %, par rapport à l'année précédente.

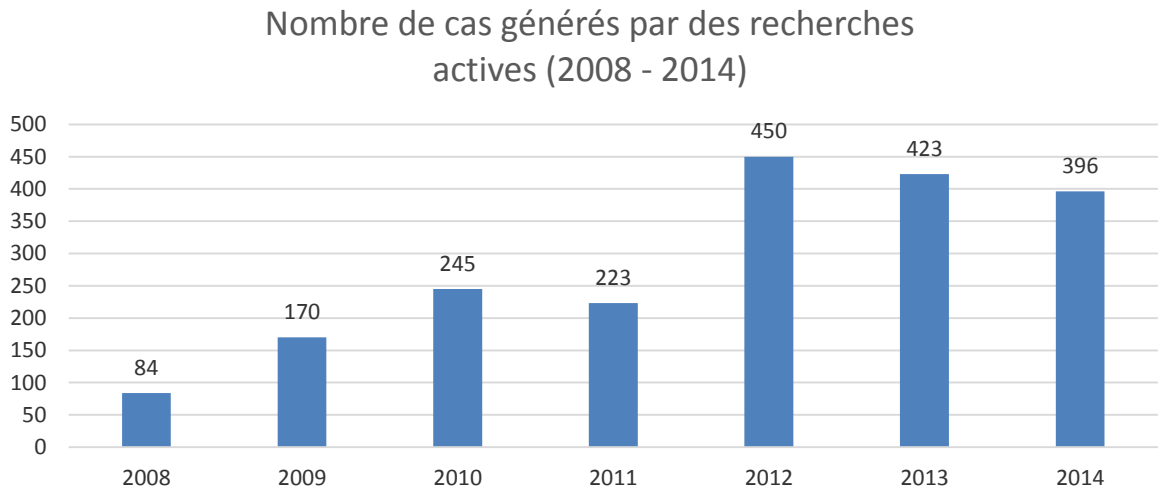

Illustration 10: dénonciations transmises dans le cadre de recherches actives (2008-2014)

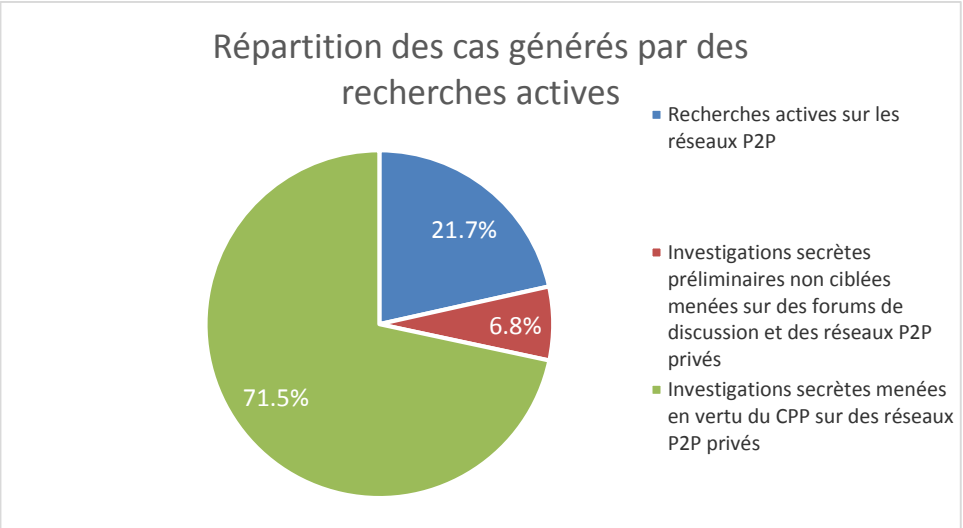

Illustration 11: origine des dénonciations pénales générées par des recherches actives en 2014 (total: 396)

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

Sur 396 dénonciations, 86 ont résulté de recherches actives menées par le SCOCI dans les bourses d'échange publiques P2P. Par rapport à 2013, ce chiffre est une nouvelle fois en légère baisse, du fait entre autres que le nombre d'utilisateurs des réseaux P2P surveillés a lui aussi reculé ces dernières années et que les activités des malfaiteurs se sont déplacées vers des domaines moins visibles d'Internet comme des réseaux P2P privés ou le web invisible (deepweb et darknet[7]).

Les dossiers visent des internautes qui échangent activement et régulièrement de la pornographie dure avec des mineurs au sens de l'art. 197, al. 4 ou 5, CP. Si le SCOCI axe spécifiquement ses recherches sur les utilisateurs en Suisse, il a aussi enregistré au cours de l'année sous revue des faits punissables concernant une personne à l'étranger (Etats-Unis). Dans ces cas-là, le SCOCI transmet les informations aux services d'Interpol compétents à l'étranger.

3.2 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 l'Office fédéral de la police (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 sous couverture pour lutter contre la pédocriminalité sur Internet[8]. Conformément audit accord, les collaborateurs du SCOCI mènent des investigations préliminaires secrètes exclusivement sur mandat et sous 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 et que les efforts de chaque canton puissent être coordonnés.

Les investigations préliminaires secrètes menées par le SCOCI en 2014 ont conduit dans 26 cas à une dénonciation pénale aux cantons compétents et dans un cas, à l'étranger. Deux dénonciations reposaient sur des investigations menées sur des forums de discussion en ligne pour enfants. Dans un autre cas, une dénonciation a été établie après que le criminel, sans y être invité, a enclenché une webcam sur un forum de discussion par vidéo pour partager ses actes d'ordre sexuel avec l'agent sous couverture, ce dernier se faisant alors passer pour une fillette mineure. Ces trois dénonciations avaient toutes pour objet des tentatives d'actes d'ordre sexuel avec des mineurs au sens de l'art. 187 CP. Le faible nombre d'enquêtes menées par le SCOCI dans des forums pour enfants est dû au fait que la plupart des cantons disposent désormais des bases légales pour intervenir eux-mêmes sur ces forums. Le SCOCI fournit aux corps de police cantonaux une plate-forme centrale de planification nationale des engagements et d'échange d'informations pour éviter que deux cantons n'évoluent en même temps sur un même forum. Les cantons disposent ainsi d'un instrument en réseau pour organiser entre eux et de manière permanente les activités d'enquête au niveau national. L'intensité de ces activités dépend des possibilités et ressources des cantons pour effectuer des investigations préventives secrètes dans des cas liés uniquement à la Suisse.

Le SCOCI, quant à lui, concentre ses ressources sur le monitoring et les investigations secrètes y afférentes dans les bourses d'échange privées de P2P, qui doivent impérativement

[7] A l'origine employé pour définir un réseau privé virtuel au sein duquel les utilisateurs ne se connectent qu'à des personnes de confiance, le darknet s'entend de nos jours davantage comme le web invisible (deepweb). Cela concerne en particulier les pages Internet qui ne sont pas indexées par les moteurs de recherche.

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

être effectués au niveau central, et sur les interventions sur le darknet, dans des domaines où il est difficile de savoir au début d'où proviennent les criminels et les victimes. La responsabilité géographique quant à la poursuite pénale est de ce fait incertaine. Pour des raisons éthico-morales, il semble primordial, dans le sens d'une aide d'urgence, que de telles investigations soient menées jusqu'à ce que les victimes et/ou les malfaiteurs soient identifiés ou localisés et que les informations obtenues soient transmises aux autorités compétentes. C'est pourquoi le SCOCI mène ces investigations de manière centralisée à la place des cantons.

Dans les 24 cas restants, les investigations préliminaires secrètes ont eu lieu dans des bourses d'échange privées P2P. Ici, contrairement aux sites P2P classiques, l'échange des fichiers se fait directement entre différents ordinateurs via des raccordements privés chiffrés, raison pour laquelle l'intervention d'un agent sous couverture est nécessaire pour entrer en contact avec les auteurs de ce type d'échange. Dans ce contexte, la plupart des dénonciations avaient pour objet la possession et la diffusion de pornographie illicite au sens de l'art. 197, al. 4 ou 5, CP, ou de l'art. 197, ch. 3 ou 3bis, CP avant l'entrée en vigueur le 1er juillet 2014 de la révision de la loi.

3.3 Investigations secrètes fondées sur le code de procédure pénale (CPP)

Comme en 2013, le SCOCI a été chargé en 2014 par différents ministères publics cantonaux de mener, au titre d'autorité directement subordonnée et dans le cadre de procédures cantonales, 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. Les injonctions reposaient sur des procédures pénales ouvertes sur la base des investigations secrètes non ciblées menées en vertu de la loi sur la police du canton de Schwyz et qui, au cours de la procédure, ont mis au jour de nouveaux cas suspects. Ces investigations ont conduit à 283 dénonciations de la part du SCOCI.

Les logiciels employés par la communauté privée P2P permettent d'établir une connexion directe entre deux ordinateurs pour échanger des fichiers, quel que soit l'endroit où se trouvent les utilisateurs. Ces particularités techniques rendent difficile le ciblage des recherches sur des auteurs d'infractions suisses. Au cours des enquêtes ordonnées, trois utilisateurs suisses ont pu être identifiés. Les 280 autres dénonciations et leurs éléments d'accusation ont toutes été transmises aux autorités étrangères de poursuite pénale compétentes dans le cadre de l'échange international d'informations de police. En traitant systématiquement les soupçons découlant des procédures suisses, peu importe l'origine des malfaiteurs et des victimes, le SCOCI, qui représente les cantons, satisfait aux obligations qui incombent à la Suisse au titre de l'Alliance mondiale ("Global Alliance"), laquelle agit dans le monde entier, de manière conjointe et solidaire, contre les abus d'enfants sur Internet. Il décharge ainsi les cantons, qui n'ont pas à utiliser des ressources pour traiter des cas où les auteurs d'infractions seront finalement dénoncés à l'étranger.

3.4 Feed-back des cantons

Afin d'avoir une vue d'ensemble des activités menées dans les cantons, le SCOCI demande à ces derniers des informations sur la suite donnée aux cas suspects qui leur avaient été signalés (mesures de police engagées et/ou résultat des procédures judiciaires).

Les feed-back des cantons reçus au cours de l'année sous revue sont listés ci-dessous. La plupart des dénonciations ont été établies sur la base des recherches actives effectuées en

2013 déjà, dans la mesure où les feed-back ont majoritairement été envoyés après la clôture des procédures concernées et l'entrée en force des jugements.

3.4.1 Feed-back des autorités de police cantonales

Pour la première fois dans l'histoire du SCOCI, il a été constaté sur la base des feed-back reçus que chaque soupçon communiqué par le SCOCI avait donné lieu à une perquisition.

Cela ne signifie pas pour autant qu'une perquisition a été ou sera effectuée dans 100 % des dossiers transmis. Comme le SCOCI n'a pas encore reçu tous les formulaires de feed-back pour l'année 2013-2014, il n'est pas possible de déterminer le nombre réel des perquisitions entreprises. Le taux élevé de ces dernières montre toutefois que les corps de police examinent activement les dénonciations du SCOCI, qu'ils estiment prioritaires.

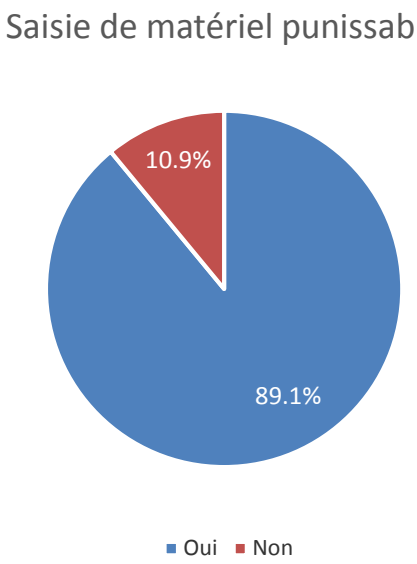

Illustration 12: pourcentage des perquisitions fructueuses en 2014 (saisie de matériel punissable pénalement après une dénonciation du SCOCI)

89,1 % des perquisitions consécutives à une dénonciation du SCOCI ont permis de saisir du matériel illégal. Les raisons des perquisitions infructueuses sont diverses et parfois difficiles à déterminer. Ces dernières années par exemple, les raccordements sans fil ouverts et non protégés empêchaient toute identification certaine des auteurs d'infraction. Grâce aux supports de stockage plus compacts, il est de plus en plus facile pour ces derniers de cacher le matériel illicite. Ils recourent par ailleurs de plus en plus à des supports chiffrés, qui rendent difficile la fourniture de preuves relatives à la possession et à l'échange de matériel interdit.

92,9 % du matériel illégal saisi contenait des données pornographiques avec des enfants. Ce haut pourcentage n'a rien d'étonnant vu que ce type de contenus est justement ciblé dans le monitoring des réseaux P2P privés ou non, et constitue de ce fait la grande majorité des dénonciations issues de ces recherches. Il est toutefois intéressant de relever que dans plus de 59,1 % des perquisitions, un autre élément constitutif de la pornographie illégale (art. 197 CP) a été constaté.

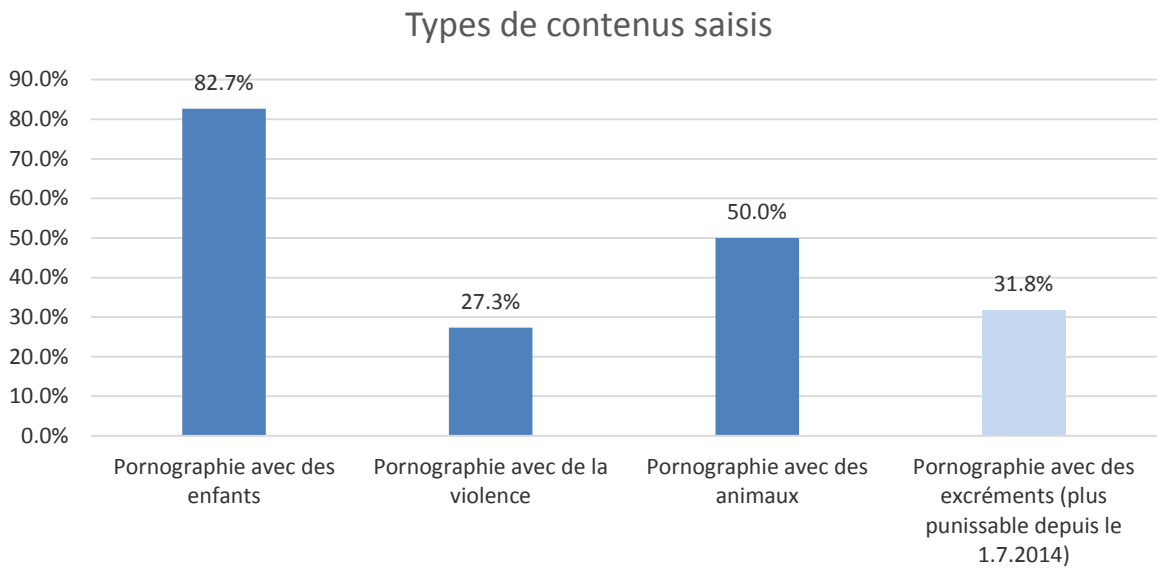

Illustration 13: pourcentages des perquisitions qui ont conduit à la saisie de matériel pornographique illicite en 2014

Il ressort en outre des feed-back des autorités de police cantonales que, concernant le type de matériel illégal saisi au cours des perquisitions, il s'agissait de fichiers vidéo dans 57,1 % des cas, de fichiers images dans 59,2 %, et d'autres supports dans 6,1 % des cas. Au total, les perquisitions ont permis de saisir près de 700 000 fichiers vidéo et images pénalement punissables.

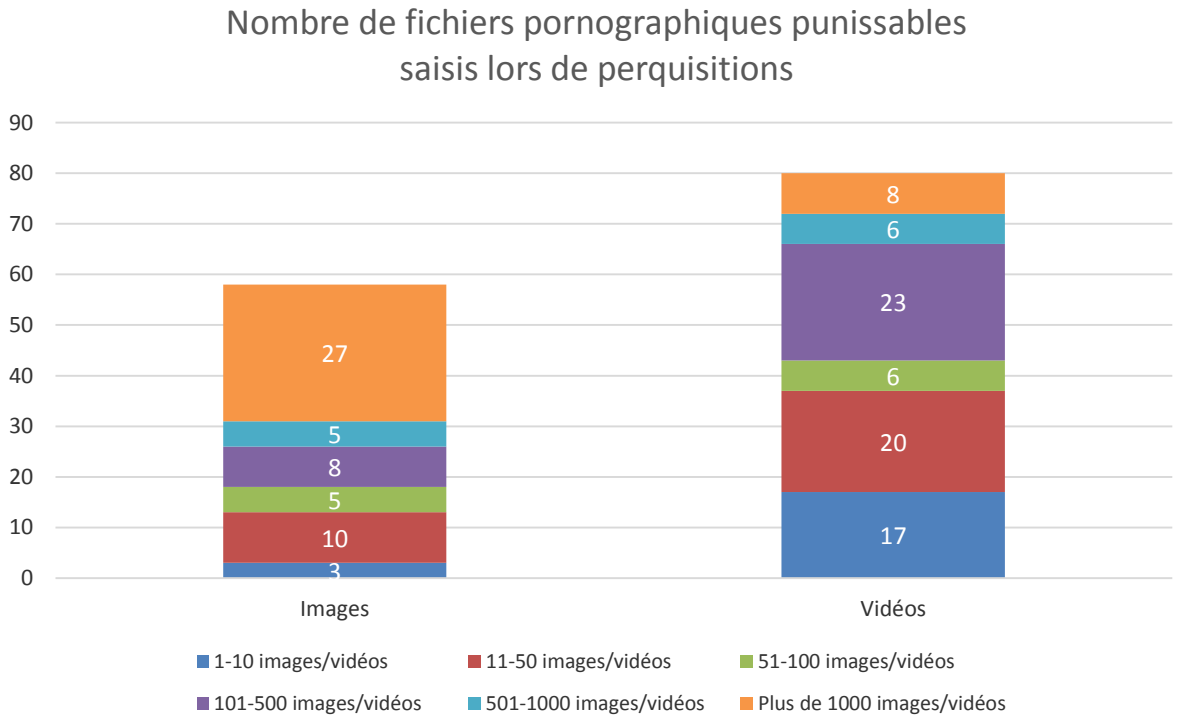

Illustration 14: répartition du matériel pornographique saisi en 2014 lors de perquisitions. Le graphique illustre le nombre de cas (nombres) et la quantité (couleur) de matériel incriminant.

3.4.2 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 89,5 % des cas.

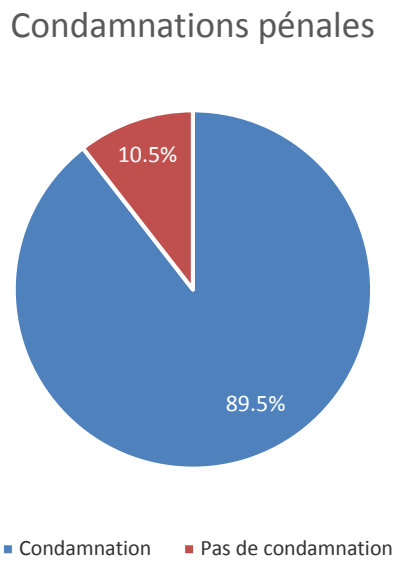

Illustration 15: condamnations pénales prononcées en 2014

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 (avant la révision du CP) et al. 4 et 5 (depuis le 1er juillet 2014).

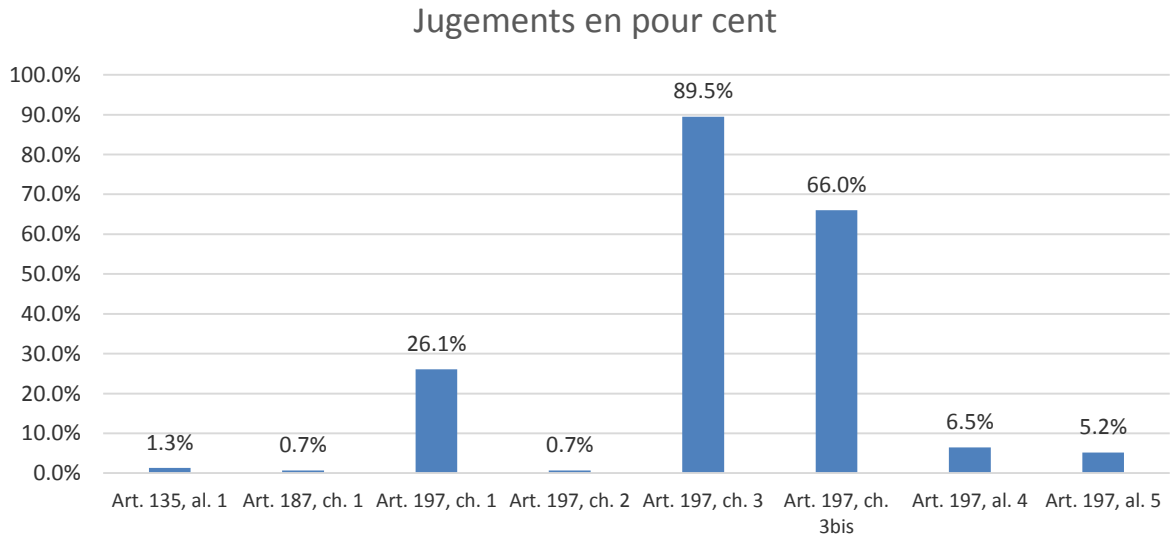

Illustration 16: jugements les plus fréquents en 2014 (en %). Le graphique montre sur la base de quel article du CP et à quelle fréquence un jugement a été rendu en comparaison avec le nombre total des jugements.

La peine prononcée dans 92,2 % des condamnations communiquées en 2014 était une peine pécuniaire (jours-amende), à laquelle s'est ajoutée une amende dans 74,5 % de ces cas. Dans 94,3 % des cas, les peines pécuniaires étaient 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 5,2 % des cas.

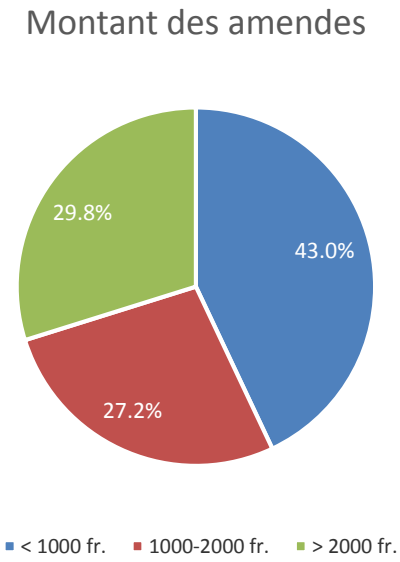

Illustration 17: nombre de jours-amende et montant de l'amende des condamnations rendues en 2014

Dans 43,0 % des cas environ, les amendes étaient inférieures à 1000 francs et dans 27,2 % des cas, elles étaient comprises entre 1000 et 2000 francs. Dans 29,8 % des cas seulement, les amendes étaient supérieures à 2000 francs.

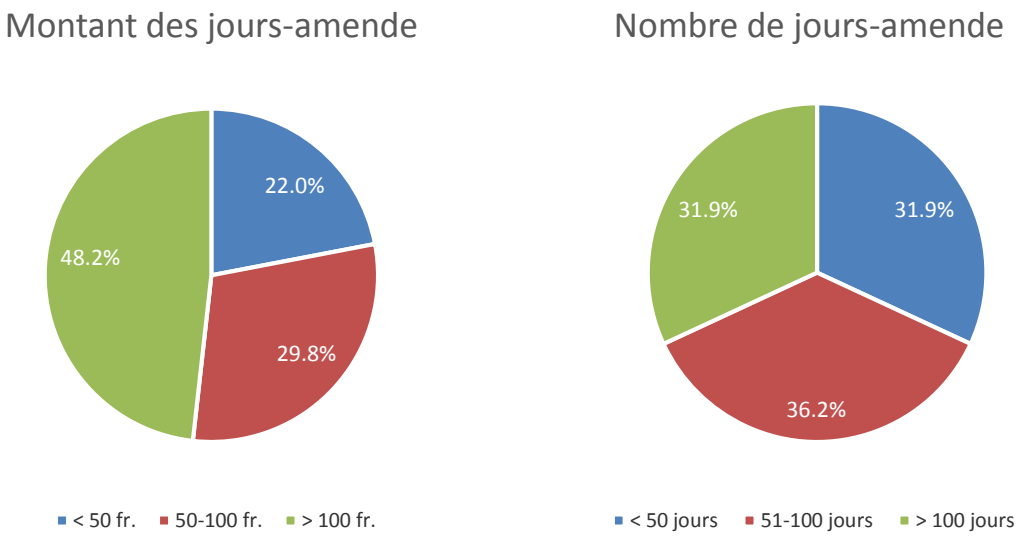

Illustration 18: répartition des montants des jours-amende fixés dans le cadre d'une condamnation en 2014

Dans 31,9 % des peines pécuniaires, le nombre des jours-amende était inférieur à 50. Dans 36,2 % des cas, il était compris entre 51 et 100. Plus de 100 jours-amende ont été prononcés dans 31,9 % des cas.

Les personnes condamnées devaient en outre s'acquitter des frais de procédure, qui excédaient souvent de beaucoup le montant effectif de l'amende.

3.5 Exemples de cas

Les investigations préliminaires secrètes menées par le SCOCI dans des bourses d'échange privées ont permis d'identifier un utilisateur en Autriche, qui avait donné à un agent sous couverture accès à sa vaste collection de pédopornographie. Les investigations qui s'en sont suivies ont mis au jour une connexion Internet en Autriche utilisée par le malfaiteur pour se rendre dans la bourse d'échange. La transmission des informations aux collègues autrichiens a permis à l'office de police du Land de Styrie d'enquêter sur le suspect ainsi que sur 51 autres se trouvant en Suède, aux Pays-Bas, en Belgique, au Danemark, au Brésil et en Iran.

Dans un autre cas, la police cantonale compétente a saisi du matériel pédopornographique lors d'une perquisition consécutive à une dénonciation du SCOCI. Comme l'accusé était le mari d'une maman de jour, la commune concernée a publié un communiqué de presse pour informer la population. La famille de jour s'occupait déjà de trois enfants depuis 2012. Par bonheur, les enquêtes des autorités cantonales compétentes n'ont pas révélé d'indices d'actes de violence sur d'autres enfants.

4 Echange d'informations de police judiciaire

4.1 Annonces entrantes et sortantes

Depuis son rattachement à la Police judiciaire fédérale (PJF) en 2009, le SCOCI est chargé de coordonner l'échange d'informations de police judiciaire au niveau international dans le domaine de la cybercriminalité. A ce titre, et en tant que centre de compétences, il soutient les cantons dans leurs enquêtes. Depuis l'entrée en vigueur de la Convention du Conseil de l'Europe sur la cybercriminalité (CCC) le 1er janvier 2012, la Suisse est de plus en plus considérée sur le plan international comme un partenaire actif dans la lutte contre la criminalité sur Internet. Pour accomplir ses tâches, le SCOCI peut compter sur un important réseau en Suisse et à l'étranger, tant dans le secteur public que privé. Il fait en outre office d'intermédiaire entre les cantons et les organisations internationales Interpol et Europol pour ce qui a trait à la cybercriminalité. Le Centre européen de lutte contre la cybercriminalité (EC3) d'Europol est devenu l'un de ses principaux partenaires.

Un total de 1314 annonces ont été réceptionnées via les différents canaux, ce qui correspond à une hausse de 77,8 % par rapport à l'année précédente. Les annonces sortantes ont elles aussi augmenté de 35,8 %, passant à 1285. Ces annonces comprennent l'échange d'informations avec des autorités suisses et étrangères.

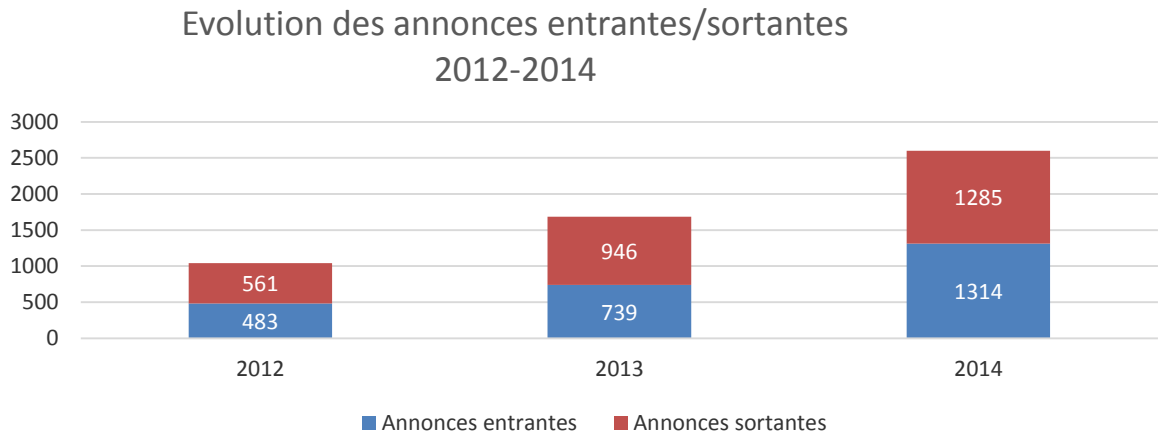

Illustration 19: évolution du nombre d'annonces dans le cadre de l'échange d'informations de police judiciaire 2012-2014

Une particularité de la CCC est la possibilité de procéder à la conservation immédiate de données dans les pays signataires par voie policière, la partie requérante s'engageant à soumettre ultérieurement une demande d'entraide judiciaire (art. 29 ss). Dans ce contexte, le SCOCI a reçu quinze demandes de cantons à des autorités étrangères, qui ont été immédiatement transmises. Dans le sens inverse, onze demandes d'autorités étrangères ont été soumises.

4.2 Coordination de procédures nationale et internationale

Sur la base des annonces entrantes et sortantes, le SCOCI entreprend régulièrement des mesures de coordination dans le cadre de l'échange d'informations international. En 2014, c'était le cas dans quelque 146 dossiers. La nature du soutien fourni dépend de la situation

initiale. Le SCOCI fait office d'interlocuteur central pour les autorités de police étrangères notamment dans le cadre de procédures d'enquête internationales. Il endosse également un rôle de conseil auprès des autorités de police et de justice en Suisse. Dans d'autres cas, surtout lorsque la compétence cantonale est avérée, le SCOCI apporte son expertise, que ce soit aux niveaux analytique, technique et juridique, ou lors de l'engagement d'agents sous couverture.

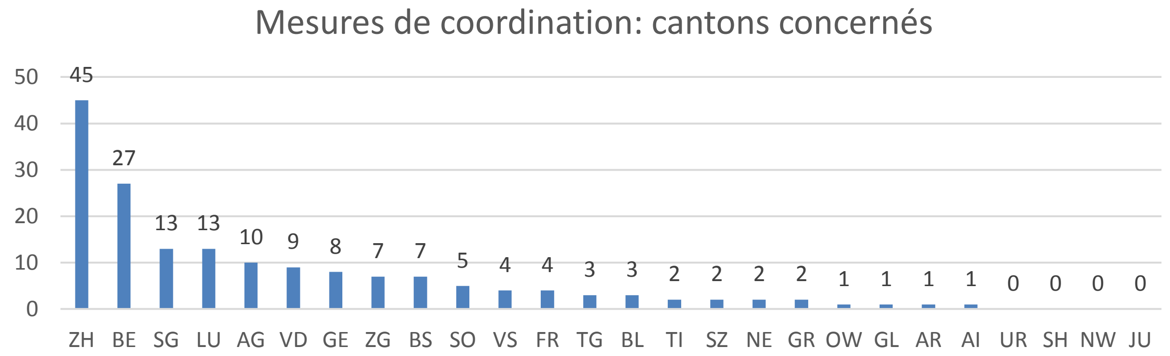

Illustration 20: cantons concernés en 2014 par des mesures de coordination. Une mesure de coordination pouvant concerner plusieurs cantons, le total du graphique ne correspond pas au total indiqué plus haut.

Les mesures prises par le SCOCI visent à garantir l'utilisation optimale des ressources disponibles auprès des services de police cantonaux et à éviter les doublons dans les enquêtes nationales. Dans ce contexte, le SCOCI a organisé dans deux cas des séances de coordination avec des représentants de polices cantonales enquêtant sur les mêmes cas complexes.

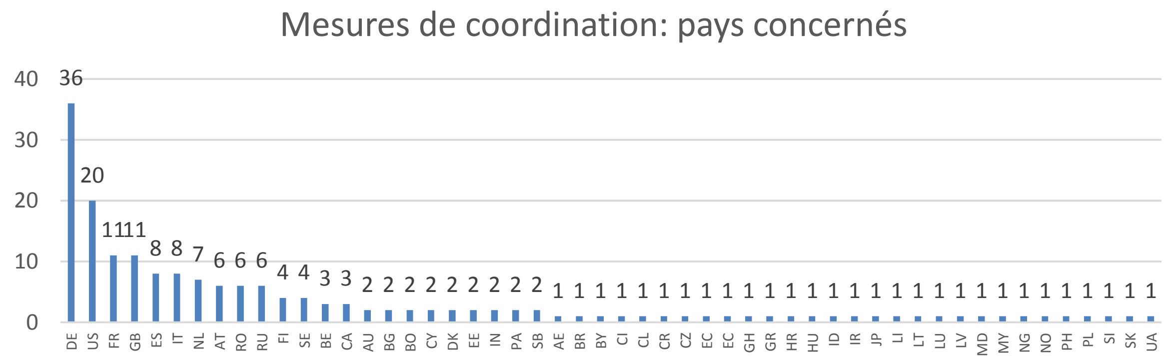

Illustration 21: pays concernés en 2014 par des mesures de coordination. Une mesure de coordination pouvant concerner plusieurs pays, le total des mesures listées dans le graphique ne coïncide pas avec les chiffres indiqués en haut.

La poursuite pénale de criminels organisés de manière informelle et opérant depuis l'étranger nécessite de nombreuses ressources et un savoir-faire technique important. La poursuite d'une infraction isolée dans un cas complexe, par exemple un dommage isolé dans une vaste campagne d'infection par maliciels, est généralement vouée à l'échec en raison du manque patent de traces exploitables. L'expérience acquise dans un cas complexe impliquant l'utilisation d'un maliciel contre des clients de banques suisses montre l'importance et l'investissement que représente la conduite d'une vue d'ensemble nationale des cas (cf. mesure 6 de la Stratégie nationale de protection de la Suisse contre les cyberrisques). Une vue d'ensemble centralisée des cas est essentielle à la reconnaissance de liens entre l'attaque effective par maliciel, la diffusion du maliciel par e-mails ou sites web conçus à cet effet, et le versement et le

transfert des sommes d'argent ainsi volées. Seule l'analyse des renseignements acquis grâce à la collecte systématique de dénonciations sur le phénomène dans son ensemble permet aux enquêtes d'aboutir à d'autres indices. Comme ce genre de cas complexes touche rarement uniquement la Suisse mais tout l'espace francophone et germanophone, une collaboration internationale et un échange des informations avec les services compétents, par exemple l'EC3 d'Europol, sont indispensables et permettent d'économiser des ressources.

4.3 Exemples de cas

En mai 2014, une opération policière coordonnée par le FBI américain et menée dans seize pays a conduit à l'arrestation d'une centaine d'utilisateurs du logiciel malveillant Blackshades. En amont de cette opération, le SCOCI, grâce aux données recueillies par le FBI dans le cadre de l'échange d'informations de police judiciaire sur le plan international, avait mené des enquêtes préliminaires sur de possibles utilisateurs suisses du maliciel. Sur la base de ces enquêtes, et après une réunion de coordination convoquée par le SCOCI avec les ministères publics compétents et les autorités de police concernées, des procédures pénales ont été ouvertes dans onze cantons contre les acheteurs présumés pour importation de logiciels malveillants au sens de l'art. 144bis, ch. 2, CP. Lors d'une autre réunion de coordination, et à la suite d'enquêtes complémentaires, des premiers résultats ont été présentés par les autorités de poursuite pénale cantonales, et la marche à suivre pour le jour de l'opération a été discutée. Le jour convenu, les polices cantonales ont effectué simultanément seize perquisitions suivies d'interrogatoires. Les personnes arrêtées avaient en moyenne 24 ans, la plus jeune étant âgée de 16 ans à peine. Le matériel saisi lors des perquisitions et les interrogatoires ont d'ores et déjà donné lieu à de premiers jugements.

Dans un autre cas, une demande est parvenue au SCOCI dans le cadre des art. 29 et 30 de la Convention du Conseil de l'Europe sur la cybercriminalité (CCC). Lors d'une enquête, les autorités étrangères avaient constaté que dans une affaire de chantage, un service Internet sis en Suisse avait été utilisé abusivement pour perpétrer des actes de chantage par e-mail. Les autorités étrangères demandaient que soient conservées les informations pouvant conduire à l'identification de l'auteur de l'e-mail. Le service concerné était administré par un particulier, inconnu dans un premier temps, via un site hébergé par un fournisseur d'accès suisse. Le domicile de cette personne et le lieu où se trouvaient les données étaient cependant dans deux cantons différents, raison pour laquelle une coordination des mesures aux niveaux policier comme juridique s'imposait. En collaboration avec les services de police concernés, les ministères publics cantonaux compétents et la Division de l'entraide judiciaire internationale auprès de l'Office fédéral de la justice (OFJ), l'exploitant privé du service a pu être identifié en peu de temps, et une ordonnance de production de pièces a pu être établie pour que les données demandées soient fournies. Suite à l'obtention d'une copie numérique de la demande d'entraide judiciaire des autorités requérantes, les données demandées ont pu d'ores et déjà être transmises dès le lendemain par voie policière, en application de l'art. 30 de la CCC.

5 Projets

5.1 SNPC

Le Conseil fédéral a adopté la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) le 27 juin 2012. La lutte contre la cybercriminalité est un facteur important de protection des infrastructures critiques, un constat que prend en considération la mesure 6 de la SNPC, dont la mise en œuvre a été confiée au Département fédéral de justice et police (DFJP) pour des raisons de compétences. Il s'agit à cet effet d'élaborer un concept conjointement avec les cantons pour obtenir une vue d'ensemble actuelle des cas de cybercriminalité en Suisse et ainsi mieux coordonner les cas complexes intercantonaux. Les informations obtenues grâce à la poursuite pénale doivent être intégrées dans une présentation globale de la situation par MELANI.

Ce concept doit être présenté au Conseil fédéral fin 2016. En plus de décrire les mesures, il définit les interfaces avec d'autres acteurs visant à la réduction des cyberrisques, la coordination avec la présentation de la situation et les ressources et adaptations juridiques – tant au niveau fédéral que cantonal – qui sont nécessaires pour le concrétiser.

L'élaboration du concept en lien avec la mesure 6 de la SNPC a pu être initiée, et début mai 2014, le SCOCI a lancé un sondage national auprès de toutes les autorités de poursuite pénale de la Confédération et des cantons. Le point de la situation qui en est ressorti ainsi que les faiblesses et les besoins des services œuvrant à la lutte contre la cybercriminalité ont été intégrés dans le concept.

Le projet s'étant avéré plus vaste que prévu du fait de la complexité du mandat, la consultation auprès des cantons a dû être reportée au premier trimestre 2015.

La révision finale du concept devrait avoir lieu à compter de septembre 2015. Le projet sera ensuite soumis au Conseil fédéral.

6 Groupes de travail, partenariats et contacts

6.1 Collection nationale de fichiers et de valeurs de hash (CNFVH)

Conjointement avec les cantons, le SCOCI gère une collection nationale de fichiers et de valeurs de hash (CNFVH) portant sur des images relevant clairement de la pornographie interdite. Cette collection de valeurs de hash (aussi appelés "codes hash") vise à réduire le fardeau psychique et la charge de travail des enquêteurs investis dans des cas de diffusion de pédopornographie. Les images dont la valeur de hash est déjà enregistrée dans la CNFVH sont automatiquement catégorisées. La CNFVH, opérationnelle depuis octobre 2012, est à la disposition des services de corps de police cantonaux et municipaux.

L'entrée en vigueur le 1er juillet 2014 des modifications de l'art. 197 CP a conduit à la suppression de l'interdiction de pornographie avec excréments. La CNFVH a dû être adaptée en conséquence, et les valeurs de hash d'images de cette catégorie qui y étaient enregistrées ont été effacées.

Les cantons ne disposent que des valeurs de hash dont les images afférentes ont été clairement jugées interdites à trois reprises. Cette classification demande un peu de temps. En outre, l'échange international visé nécessite certes une catégorisation uniforme mais aussi des normes de qualité fiables. Ces mesures ont également pour objectif de faire en sorte que les valeurs de hash portant sur du matériel clairement interdit puissent être versées dans des dossiers judiciaires.

Jusqu'à la fin 2014, quelque 4 millions de fichiers ont été fournis tandis que leurs valeurs de hash étaient enregistrées dans la CNFVH. La classification du matériel photo est chronophage et ne peut être menée à bien que grâce au soutien solidaire des cantons. Pour qu'une image soit classée interdite, il faut que des collaborateurs des services de police cantonaux ou du SCOCI émettent trois mêmes évaluations. A ce jour, 138 000 images environ ont été évaluées à trois reprises et donc saisies dans la CNFVH comme pornographie interdite.

Le SCOCI met en outre à la disposition des cantons quelque 3 millions de valeurs de hash étrangères à des fins d'analyse forensique. Ces valeurs ont été calculées par des autorités de poursuite pénale étrangères avant d'être fournies au SCOCI. Comme toutefois le matériel photo y relatif n'est pas disponible, ces valeurs de hash ne peuvent faire l'objet d'un contrôle qualité. C'est pourquoi il s'agit ici, au contraire des valeurs confirmées de la CNFVH, de "valeurs de hash suspectes". Le SCOCI met également à disposition des "listes blanches" de 78 millions de valeurs de hash portant sur des contenus non punissables (par ex. icônes de services d'exploitation ou applications). Ces listes blanches permettent de réduire automatiquement le nombre de fichiers que les enquêteurs doivent analyser. Le SCOCI se procure systématiquement ces listes et les met à la disposition des cantons en même temps que les listes noires.

Le SCOCI, en collaboration avec les cantons, élabore actuellement un concept visant à élargir cette collection de données en vue d'une identification systématique des victimes et d'une comparaison avec la banque de données ICSE[9] d'Interpol. Ces travaux sont liés aux objectifs de l'Alliance mondiale (cf. chap. 6.7.3), dont la mise en œuvre pour la Suisse prévoit entre autres l'élaboration conjointe avec les cantons d'ici 2016 d'un concept national d'identification des victimes.

[9] ICSE - International Child Sexual Exploitation image database.

Outre les valeurs de hash et leur importance pour l'analyse forensique de matériel saisi, une banque de données images centrale offre de nombreux éléments d'enquête pour identifier les criminels et leurs victimes, dont l'abus, du fait de l'endroit à l'origine indéterminé, ne s'est pas toujours produit dans le domaine de compétence géographique des autorités chargées initialement de l'enquête. Il est reconnu au niveau international que les enquêtes axées sur l'identification des victimes au moyen de matériel saisi et d'une coopération transnationale sont très prometteuses. Il apparaît en outre comme justifié d'un point de vue éthico-moral de recourir à des ressources existantes pour identifier des enfants qui peut-être étaient encore sexuellement abusés au moment de la saisie ou de l'examen des images; et ce, même s'il s'avère que les abus ont eu lieu dans un autre domaine de compétence. Les victimes peuvent ainsi compter sur le fait que les autorités de poursuite pénale s'attellent à la tâche, peu importe la compétence géographique, pour éviter que d'autres abus ne soient commis et pour arrêter les auteurs d'infraction. Il s'agit pour chacun d'endosser sa part de responsabilité dans ce phénomène mondial et d'exploiter au mieux sa propre marge de manœuvre.

En Suisse, l'identification des victimes est perfectible. La CNFVH est la pierre angulaire d'une identification systématique des victimes. Les innombrables offres en ligne d'interactions humaines – forums, bourses d'échange P2P, réseaux sociaux et réseaux anonymes – restent malheureusement trop souvent une ouverture facile pour ceux qui veulent s'en prendre à des enfants.

A travers la CNFVH, la Suisse a posé une première pierre importante dans la lutte contre la fabrication, le commerce et la diffusion d'images illicites, contre l'abus de mineurs sur Internet et contre la "revictimisation" récurrente. Le 6 décembre 2012, lors de la conférence de l'Alliance mondiale contre la pédocriminalité sur Internet, la conseillère fédérale Simonetta Sommaruga a confirmé la volonté de la Suisse de soutenir ce combat aux niveaux national et international.

6.2 Groupes de travail nationaux

Au cours de l'année sous revue, le SCOCI était représenté au sein de différents groupes de travail nationaux.

Aux côtés du Commissariat Pédocriminalité et pornographie de la PJF, le SCOCI est membre et organisateur du groupe de travail "Kindsmissbrauch" ("Abus d'enfants"), où sont représentées des autorités de poursuite pénale de la Confédération et des cantons, la Prévention suisse de la criminalité et des organisations d'utilité publique œuvrant dans la protection de l'enfant.

Comme durant les années précédentes, le SCOCI a participé en 2014 aussi au programme national "Protection de la jeunesse face aux médias et compétences médiatiques". Il siège à la fois dans le groupe de pilotage chargé d'élaborer le programme d'action et dans le groupe de projet exécutif "Monitorage de la régulation et évolution des médias". Ce programme vise à aider les enfants et les adolescents à utiliser les nouveaux médias de façon sûre, responsable et adaptée à leur âge.

6.3 Collaboration avec d'autres services de la Confédération

La cybercriminalité concernant presque tous les titres du CP, la collaboration menée par le SCOCI avec les services de la Confédération est d'autant plus variée. Au sein de fedpol, le SCOCI travaille intensivement avec le Commissariat Pédocriminalité et pornographie, le Commissariat Enquêtes TI et le Commissariat Investigations secrètes de la PJF et entretient des contacts étroits avec la Division principale Coopération policière internationale. Comme en 2013, les relations avec divers services de la Confédération ont été approfondies; il s'agit ici pour l'essentiel de MELANI, du Domaine de direction Entraide judiciaire internationale de l'Office fédéral de la justice (OFJ), de l'Autorité fédérale de surveillance des marchés financiers (FINMA), de l'Institut fédéral de la propriété intellectuelle (IPI), de la Commission fédérale des maisons de jeu (CFMJ), du Département fédéral des affaires étrangères (DFAE) et du Réseau national de sécurité (RNS).

6.4 Echange d'expériences avec les cantons

En 2014, le SCOCI a entretenu de nombreux contacts avec les représentants de divers corps de police et des ministères publics, notamment en lien avec des cas opérationnels en cours. Dans ce contexte, il faisait profiter les cantons de son savoir technique et de son réseau international, tandis que les cantons lui apportaient des connaissances sur les particularités locales, les processus bien rôdés entre police et ministère public et un savoir-faire forensique.

La fonction de coordination du SCOCI et la bonne collaboration avec les cantons ont permis dans plusieurs cas (cf. aussi chap. 5.3) d'ouvrir une procédure pénale sur la base de faits déclarés à l'étranger ou encore d'empêcher un suspect de détruire des preuves.

6.5 Collaboration avec des ONG et des associations

Depuis de nombreuses années, le SCOCI collabore étroitement avec l'organisation non gouvernementale (ONG) 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 de réseaux P2P a pu être mené et développé avec succès au cours des dernières années.

Le SCOCI entretient des contacts avec l'association Stop Piracy pour signaler aux autorités de police compétentes ou aux fournisseurs d'hébergements les magasins en ligne frauduleux qui vendent des articles de marque contrefaits.

Il envisage également une collaboration avec l'association Swiss Internet Security Alliance (SISA), qui regroupe des FAI, des prestataires Internet et des experts en sécurité de l'information pour faire du web suisse un espace exempt de logiciels malveillants.

6.6 Collaboration avec les fournisseurs d'accès à Internet suisses (FAI)

En 2007, un accord a été conclu entre le SCOCI et les principaux fournisseurs d'accès à Internet (FAI) suisses pour bloquer les sites Internet aux contenus pédopornographiques interdits. Cette mesure vise uniquement les sites hébergés à l'étranger qui proposent de télécharger de la pornographie enfantine illicite au sens de l'art. 197, al. 4 et 5, CP. S'appuyant sur

leurs conditions générales de vente et sur des principes éthiques, les FAI bloquent tout accès à des sites pénalement punissables et redirigent l'utilisateur vers une page "stop". A cette fin, le SCOCI établit et met à jour une liste de 700 à 1000 sites.

Le SCOCI travaille étroitement avec Interpol dans le cadre de ce projet. La liste élaborée en Suisse alimente en grande partie la liste "worst of" d'Interpol, qui recense les sites proposant des contenus pédopornographiques. Le SCOCI entreprend chaque jour une recherche proactive en ce sens et complète régulièrement la liste d'Interpol, qui est entretenue en collaboration avec plusieurs pays.

6.7 Coopération internationale

6.7.1 Europol

Depuis 2011, le SCOCI est membre de plusieurs groupes de travail lié à l'EC3. Sis auprès d'Europol à La Haye, ce centre de lutte contre la criminalité sur Internet fournit un appui opérationnel aux membres de l'UE et aux Etats tiers et met à disposition ses connaissances spécialisées et ses activités d'analyse dans le cadre d'enquêtes conjointes. Le SCOCI est en contact permanent avec l'EC3 et a régulièrement participé à des rencontres stratégiques et opérationnelles au cours de l'année sous revue. L'EC3 avait principalement fait porter ces rencontres sur la lutte contre la "cybercriminalité au sens strict" par le Focal Point (FP) CYBORG, l'"abus systématique de cartes de crédit" par le FP TERMINAL et la "diffusion commerciale et organisée de pédopornographie" par le FP TWINS.

Le SCOCI est membre du FP CYBORG de l'EC3, qui lutte contre la cybercriminalité transfrontalière au sens strict. L'accent est mis ici sur le hameçonnage, les attaques par déni de service, les réseaux de zombies, le piratage et d'autres phénomènes. Le SCOCI, aux côtés du Commissariat Pédocriminalité et pornographie de la PJF, est aussi membre du FP TWINS, qui se consacre à la lutte contre la pédocriminalité.

6.7.2 Adhésion de la Suisse à la Virtual Global Taskforce (VGT)

L'évolution fulgurante d'Internet offre sans cesse de nouvelles possibilités aux criminels de commettre des abus sur des enfants, tout en ayant une longueur d'avance sur les autorités de poursuite pénale. Afin d'apporter une réponse directe à cette évolution et de lutter contre les abus (sexuels) d'enfants sur Internet, la VGT regroupe, au niveau mondial, des autorités de poursuite pénale, des ONG et des entreprises du secteur privé.

Ce partenariat international permet à la VGT de rendre Internet plus sûr: les abus sont décelés et localisés plus rapidement, les enfants en détresse sont secourus et les auteurs d'infractions sont pénalement poursuivis de manière efficace.

La Suisse est membre depuis 2012 de l’Alliance mondiale contre les abus sexuels d’enfants par Internet, assumant ainsi sa part de responsabilité dans la lutte conjointe contre ce fléau. L'objectif qu'elle s'était fixé d'adhérer à la VGT a pu être réalisé en 2014.

Illustration 22: le 13 mai 2014, Thomas Walther, chef du Commissariat SCOCI, signe à Bruxelles la déclaration d'adhésion de la Suisse à la VGT, en présence d'Anthony L. Gardner (à gauche), ambassadeur des Etats-Unis auprès de l'Union européenne, de Roberto Balzaretti (à droite), ambassadeur de la Suisse auprès de l'Union européenne et d'Ian Quinn (deuxième en partant de la gauche), président de la VGT.

Font partie de la VGT aux côtés de la Suisse l'Australie, la Grande-Bretagne, l'Italie, le Canada, la Colombie, la Corée, les Pays-Bas, la Nouvelle-Zélande, les Emirats arabes unis, les Etats-Unis, Europol et Interpol.

Les membres issus du secteur privé sont les suivants: End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes network (ECPAT International), International Association of Internet Hotlines (INHOPE), National Center for Missing & Exploited Children (NCMEC), International Centre for Missing and Exploited Children (ICMEC), PayPal, Microsoft Digital Crimes Unit, World Vision, Blackberry, The Code, Kids Internet Safety Alliance (KINSA), NetClean, International Justice Mission et Telstra.

D'autres informations sur la VGT sont disponibles sur www.virtualglobaltaskforce.com.

6.7.3 Alliance mondiale contre les abus sexuels d’enfants par Internet

Sur invitation de la commissaire européenne Cecilia Malmström et du ministre américain de la Justice Eric Holder, des représentants et des experts de plus de 40 pays se sont retrouvés à Washington le 30 septembre 2014 pour la seconde conférence ministérielle de l’Alliance mondiale contre les abus sexuels d’enfants par Internet.

A cette occasion, des intervenants du milieu de la poursuite pénale, du secteur privé et des ONG ont donné un aperçu des résultats obtenus dans les quatre domaines cibles de l'Alliance (identification des victimes, identification et poursuite des auteurs d'infractions, sensibilisation,

prévention de la revictimisation). Dans son discours d'ouverture, Eric Holder s'est dit fier des objectifs et développements atteints depuis la création de l'Alliance en 2012: 54 pays déjà en sont membres et agissent de concert pour lutter contre les abus d'enfants via Internet. Eric Holder a souligné qu'il ne fallait malgré tout pas se reposer sur ses lauriers, d'autant que les risques en la matière auraient même augmenté. La pédopornographie sur Internet, notamment, poursuit son expansion sans entrave, ce qui entraîne une victimisation permanente des enfants. Eric Holder a ajouté que l'Alliance seule ne parviendra pas à y remédier et qu'elle est bien plus un complément à des structures et accords internationaux déjà en place.

L'Alliance mondiale définit des objectifs politiques et opérationnels mais laisse chaque pays membre libre de choisir comment les mettre en œuvre et les réaliser. En 2014, la Suisse a pu atteindre voire surpasser les objectifs qu'elle s'était fixés dans tous les domaines, ce qui lui a valu une reconnaissance internationale en matière de lutte contre cette forme de cybercriminalité. Ainsi, elle a été nommée lors de diverses présentations à titre d'exemple, et depuis deux ans, elle fait office de championne au niveau international dans la lutte contre les abus d'enfants via Internet.

A l'initiative du premier ministre britannique David Cameron et dans l'esprit des objectifs de l'Alliance mondiale, le #WePROTECT Children Online Global Summit a eu lieu les 10 et 11 décembre 2014 à Londres. Au contraire de l'Alliance mondiale, #WePROTECT ne cible pas avant tout les autorités de poursuite pénale mais le secteur privé. A cette occasion, les entreprises technologiques leaders se sont déclarées prêtes à apporter leur soutien en ce sens mais aussi à signer une déclaration d'action, aux côtés des représentants présents des autorités de poursuite pénale et des organisations privées[10].

6.7.4 FBI et Sécurité intérieure des Etats-Unis

La majeure partie des grands prestataires Internet se trouvant aux Etats-Unis, et les Américains visant d'ailleurs une collaboration intense avec Europol et ses pays membres en matière de cybercriminalité, le SCOCI est en contact étroit avec le bureau de l'attaché du FBI à Berne. Outre l'échange d'informations relevant de la police judiciaire, il entretient des échanges informels quant aux meilleures pratiques concernant la sauvegarde de données auprès des grands prestataires américains. En contrepartie, les demandes des Etats-Unis concernant la sauvegarde de données auprès de prestataires suisses sont directement transmises via l'attaché du FBI à la Centrale d'engagement de fedpol, puis traitées par le SCOCI.

Le SCOCI collabore également étroitement avec l'attaché américain stationné à Rome des services d'immigration et de douanes du Département de la sécurité intérieure des Etats-Unis, qui assure la liaison avec la section Cybercriminalité, dont le directeur exerce actuellement la présidence de la VGT.

[10] Cette déclaration d'action (*Statement of action*) peut être consultée en anglais sur https://www.gov.uk/government/publications/weprotect-summit

7 Médias, formations et conférences

7.1 Présence médiatique

Au cours de l'année sous revue, de nombreux articles ont rendu compte des activités du SCOCI. Dans l'ensemble, les collaborateurs ont répondu à une centaine de questions des médias.

Il convient par ailleurs de mentionner les mises en garde publiées par le SCOCI concernant des phénomènes criminels sur Internet, mises en gardes qui ont parfois été communiquées aux médias et à d'autres organisations partenaires comme MELANI et la Prévention suisse de la criminalité (PSC). Le SCOCI publie ce type d'alertes dès qu'il constate une multiplication des annonces entrantes sur un phénomène précis. Un autre facteur est celui constitué par certaines périodes du calendrier, par exemple avant des jours fériés, qui d'expérience sont marquées par une augmentation de certaines infractions. En 2014 par exemple, le SCOCI a mis en garde la population au cours de l'Avent contre des e-mails contenant des maliciels portant soi-disant sur des factures impayées de la part de sociétés de vente par correspondance, de fournisseurs de télécommunications, etc., ainsi que sur une hausse des tentatives d'escroquerie et de magasins en ligne frauduleux.

Autour des plus grandes maisons d'édition suisses ont vu le jour plusieurs services numériques qui abordent des cyberthèmes et les rendent accessibles à une large partie de la population. En outre, plusieurs personnes d'intérêt public ont été victimes de cybercriminels ces dernières années. Les contenus que le SCOCI publie sur les réseaux sociaux, notamment sur Twitter, sont régulièrement suivis par des rédactions en ligne en Suisse comme à l'étranger. Les médias diffusent sur leurs propres canaux les alertes du SCOCI, en faisant souvent référence au formulaire d'annonce.

7.2 Réseaux sociaux

Depuis 2013, le SCOCI est présent sur Facebook (www.facebook.com/cybercrime.ch) et sur Twitter (@KOBIK_Schweiz). Ces plates-formes servent essentiellement à diffuser rapidement des messages d'information sur des phénomènes actuels pour mettre en garde la population contre des escroqueries souvent signalées ou des campagnes de maliciels en cours. L'écho obtenu jusqu'ici est très positif.

Après une bonne année de service, le SCOCI compte déjà un total de 3576 "J'aime" sur ses pages Facebook francophone, germanophone et italophone, et 487 *followers* sur son compte Twitter plurilingue.

7.3 Formations et conférences

En 2014, des collaborateurs du SCOCI ont assisté à plusieurs cours, conférences et congrès internationaux. Ils ont saisi ces occasions pour suivre des formations continues individuelles, mais aussi pour entretenir des contacts et échanger des informations avec des partenaires et des experts du domaine de la cybercriminalité, de la protection de l'enfant et de l'identification des victimes.

Des collaborateurs du SCOCI ont également participé à ces manifestations en tant que formateurs. Deux d'entre eux par exemple ont dispensé un cours de deux jours organisé par la

Suisse pour l'Ecole de police d'Europe centrale (EPEC) sur le sujet de l'*Open Source Intelligence* sur Internet. Des collaborateurs du SCOCI ont participé à une centaine d'autres manifestations en tant qu'experts, formateurs et intervenants spécialisés.

La troisième édition du "Forum Cybercrime Ministères publics – SCOCI" organisé par le SCOCI a eu lieu le 13 novembre 2014. Des experts internationaux de la poursuite pénale ont donné aux participants un aperçu de la lutte concrète contre la cybercriminalité dans le monde. Le laboratoire mobile d'identification des victimes sur des images pédopornographiques d'Interpol a été présenté, et des exercices pratiques ont été proposés. La table ronde qui s'en est suivie a porté sur la révision de la loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT). Une centaine de personnes étaient présentes à ce forum.

Le lendemain 14 novembre, le SCOCI, conjointement avec Interpol, a organisé à Berne une Journée d'identification des victimes pour les membres des corps de police cantonaux et municipaux. Cette journée était le résultat direct de l'adhésion de la Suisse à l'Alliance mondiale contre les abus sexuels d'enfants par Internet (cf. chap. 6.7.3) et des mesures et engagements y relatifs, qui prévoient entre autres une intensification des efforts pour identifier les victimes de pédopornographie et leur garantir protection, suivi et soutien. Cette journée était axée sur l'identification proactive et systématique des victimes sur Internet selon le modèle international. Il s'agissait en outre de vérifier s'il est possible d'exploiter des synergies entre le classement des images dans la CNFVH et l'identification des victimes dans l'ICSE mise à disposition par Interpol. Un concept de coopération et d'identification des victimes en vue d'une répartition des tâches sera ultérieurement élaboré d'ici fin 2016, en collaboration avec les cantons.

Le SCOCI, en lien avec la CNFVH, a organisé tout au long de l'année des formations sur la catégorisation de matériel photo et vidéo pour des enquêteurs de divers corps de police et représentants d'entreprises privées suisses, qui, sur mandat de ministères publics cantonaux, sont chargés de l'analyse forensique de matériel saisi et de la catégorisation y relative de matériel photo. L'objectif est que le classement de matériel pornographique illicite dans la CNFVH réponde aux mêmes critères dans toute la Suisse pour ainsi garantir la fiabilité qualitative de la banque de données. Les deux demi-journées du cours ont entre autres porté sur des questions juridiques, et les participants ont eu tout le loisir de classer eux-mêmes du matériel photo et de discuter avec les formateurs de cas litigieux.

8 Interventions parlementaires au niveau fédéral

8.1 Liste des interventions parlementaires pertinentes

Motion 14.3022: Pornographie enfantine. Interdiction des images d'enfants nus – Rickli Natalie Simone, 3.3.2014

Question 14.5175: Prendre en compte les cyberrisques liés à la plate-forme Tumblr – Schmid-Federer Barbara, 12.3.14

Postulat 14.3193: Améliorer l'efficacité des enquêtes policières dans les réseaux sociaux – Vogler Karl, 20.3.14

Interpellation 14.3204: Consensus trouvé par le groupe de travail AGUR 12. Suite des opérations – Gutzwiller Felix, 20.3.14

Interpellation 14.3250: Violence des jeunes. Que faire? – Grin Jean-Pierre, 21.3.14

Motion 14.3288: Faire de l'usurpation d'identité une infraction pénale en tant que telle – Comte Raphaël, 21.3.14

Motion 14.3367: Combattre la textopornographie – Amherd Viola, 8.5.14

Postulat 14.3655: Définir notre identité numérique et identifier les solutions pour la protéger – Derder Fathi, 20.6.14

Motion 14.3665: Compléter l'article 260bis CP (art. 187 CP, "Actes d'ordre sexuel avec des enfants") – Commission des affaires juridiques CN, 14.8.14

Motion 14.3666: Article 198 CP. Infraction poursuivie d'office dans certains cas – Commission des affaires juridiques CN, 14.8.14

Interpellation 14.3888: Lutter internationalement contre la propagande haineuse sur Internet – Naef Martin, 25.9.14

Motion 14.3905: Garantir l'identification des auteurs de messages haineux sur le Net – Schwaab Jean Christophe, 25.9.14

Postulat 14.3908: Internet. Zéro tolérance envers l'intolérance – Tornare Manuel, 25.9.14

Postulat 14.3962: Améliorer l'assistance administrative internationale en cas d'infractions contre des enfants sur Internet – Müller-Altermatt Stefan, 26.9.14

Postulat 14.3963: La législation sur la protection des données protège-t-elle également les pédophiles? – Müller-Altermatt Stefan, 26.9.14

Interpellation 14.3969: Utiliser les compétences médiatiques pour lutter contre les discours de haine – Masshardt Nadine, 26.9.14

9 Développements futurs

Le nombre d'annonces enregistrées par le SCOCI dépend notamment de la propension de la population à rapporter des contenus suspects sur Internet. Grâce à ces signalements, le SCOCI a une meilleure vision du paysage cybercriminel en Suisse. Toutefois, cela ne concerne que la partie émergée de l'iceberg, la plupart des activités illégales sur Internet demeurant bien souvent inconnues du grand public helvétique. Les paragraphes suivants se fondent sur des informations *open source*[11] et autres rapports, ainsi que sur les connaissances acquises par le SCOCI au cours de ses onze années d'activité.

Campagnes de hameçonnage et affinement des escroqueries

Depuis les premiers types d'escroqueries par e-mail, les cyberescrocs ont revu leurs techniques, faisant désormais preuve d'une grande habileté. Ils maîtrisent davantage d'outils informatiques, dont certains rendent difficile leur identification, tels que le réseau Tor, les services VPN et les hébergements *bulletproof*. Dans le prolongement de l'année 2014, la Suisse, en raison de sa richesse et de son taux de pénétration d'Internet élevé, continuera à être une cible privilégiée de campagnes de hameçonnage. Celles-ci déploient des sites de hameçonnage identiques aux sites officiels et quasi indétectables, si bien que seuls des experts avisés peuvent faire la distinction. Pour échapper à la détection des antivirus et des pare-feu, les cybercriminels hébergent ces pages sur des comptes piratés ou non, sur des services de *cloud* (par ex. Dropbox, Google Drive, etc.), en donnant ainsi une apparence légitime à la page de hameçonnage. Une alternative consiste à injecter un code malveillant dans un site de bonne réputation afin de rediriger les visiteurs vers un site de hameçonnage. Dans cette lignée, il faudra également compter à l'avenir sur une augmentation des cas d'utilisation abusive des nouveaux domaines de premier niveau (par ex. support, .email, etc.), et des certificats de sécurité échus ou volés[12].

La double tendance du tout connecté (même dans la mobilité) et du tout partage (l'emploi du temps est rythmé par la publication de statuts, de localisations, de ses humeurs…) est une aubaine pour les escrocs de la Toile. Ces derniers amassent quantité de données et de renseignements utiles à la préparation de fraudes très sophistiquées (notamment au moyen de techniques d'ingénierie sociale), ceci au détriment des citoyens tout comme des PME et grande entreprises. À la lumière de ces considérations, une augmentation des tentatives d'usurpation d'identité associée à une hausse des cas d'escroquerie est à prévoir à l'avenir.

L'économie souterraine du darknet

La vitesse croissante d'Internet, la vulgarisation et la popularité des techniques d'anonymisation encouragent les cybercriminels à utiliser davantage les services du darknet. L'opération Onymous[13] menée le 6 novembre dernier par Europol et le FBI en collaboration avec seize pays d'Europe – dont la Suisse – est révélatrice du taux de pénétration de ces techniques au sein du grand public. Beaucoup de commerces et trafics illicites migrent dans la face cachée du web, où il est possible d'acheter, de manière plus au moins anonyme, des maliciels, des données de carte de crédit, de louer un réseau de zombies ou de commettre des attaques par

[11] Les liens suivants ont été consultés pour la dernière fois le 18 mars 2015.

[12] http://www.csoonline.com/article/2687132/social-engineering/recently-introduced-tlds-create-new-opportunities-for-criminals.html

[13] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network

déni de service[14]. Ces plates-formes s'imposent également comme lieu d'échange de matériel pédopornographique ou d'achat et de vente de produits stupéfiants et de toute autre sorte de biens interdits. Ces activités sont du reste facilitées par la diffusion des monnaies virtuelles telles que les Bitcoins, ainsi que par des méthodes de paiement à distance qui permettent des transferts d'argent plus discrets et anonymes.

Certains groupes criminels ne se bornent plus à vendre leurs prestations, mais offrent désormais de véritables "services après-vente" ainsi qu'une assistance 24/7 à leurs "clients"[15]. Il est dès lors possible de louer des réseaux de zombies pour l'envoi massif de pourriels ou de chevaux de Troie tout en bénéficiant d'un support technique en cas de problèmes. Ces criminels développent un nouveau *business model,* connu sous l'appellation de *Crime-as-a-Service,* capable de garantir innovation et concurrence. Désormais, la cybercriminalité n'est plus réservée aux spécialistes, mais elle est à la portée de tout un chacun qui dispose d'un budget. Tout porte à croire que cette tendance s'accentuera encore aux cours des prochaines années.

Maliciels sur les téléphones mobiles

A l'avenir, les smartphones et autres tablettes représenteront une part de marché toujours plus considérable par rapport aux ordinateurs traditionnels[16]. Pour certains utilisateurs, les smartphones se sont même déjà imposés, offrant davantage de possibilités de rester connecté. Le smartphone représente un véritable trait d'union entre la personne qui le manipule et son identité virtuelle. Avec toutefois une différence notable: si l'individu en société a une identité intrinsèque, son pendant virtuel est composé d'éléments épars et mal contrôlés (par ex. e-mails, photos, SMS, réseaux sociaux, etc.). Or, si l'utilisateur moyen a compris l'importance de posséder une solution antivirus ainsi que des programmes à jour sur son ordinateur, il n'est cependant pas toujours sensibilisé aux risques et dangers inhérents aux dispositifs portables. Les cybercriminels tirent profit de ces négligences en développant un nombre toujours croissant d'applications malveillantes qui permettent notamment de soutirer les données entreposées de façon éparse dans le portable ou sur la Toile, ou de souscrire et d'envoyer des messages vers des services surtaxés à l'insu du propriétaire. Des maliciels jusqu'à présent circonscrits au seul ordinateur font leur apparition sur les systèmes d'exploitation des dispositifs portables. C'est le cas du rançongiciel de police Reveton, dont une version pour Android a été identifiée pour la première fois l'année passée[17]. Le monde des monnaies virtuelles est également bouleversé par les premières applications malveillantes capables par exemple de transformer un smartphone en un "mineur Bitcoin" sans que le propriétaire ne s'en rende compte[18].

Si le public suisse semble épargné à ce jour, il n'est évidemment pas exclu que cette situation évolue à l'avenir.

[14] Trend Micro, Deepweb and Cybercrime, 2013, pp. 9 et ss

[15] Europol, The Internet Organised Crime Threat Assessment (iOCTA) report, 2014, p. 11

[16] http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones

[17] http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-moves-to-mobile/

[18] https://blog.lookout.com/blog/2014/04/24/badlepricon-bitcoin/

Anciennes vulnérabilités, *cloud* et nouveaux systèmes de paiement

L'année écoulée a vu l'apparition de plusieurs vulnérabilités critiques (par ex. Heartbleed[19] et Shellschock[20]) ou de failles dans des protocoles datés (par ex. POODLE[21]) qui permettent entre autres aux criminels d'accéder à des serveurs de messagerie, pour finalement parvenir à créer et gérer des réseaux de zombies[22]. À l'avenir, il faudra compter avec ce type d'attaques et savoir réagir promptement.

En raison de l'énorme quantité d'informations qu'ils hébergent, les services de *cloud* sont des cibles privilégiées des criminels. Le scandale du piratage et du vol d'images osées dans des comptes *iCloud* de certaines stars américaines[23] montre les conséquences d'un compte mal protégé. Les cybercriminels, appâtés par la grande quantité d'informations personnelles, devraient continuer de s'attaquer aux différents *clouds* dans les prochains temps. Les utilisateurs doivent être conscients de ces faits et adopter les mesures nécessaires pour sécuriser leurs accès, comme la vérification en deux étapes et le choix de mots de passe non triviaux.

Dans un autre registre, la course aux nouveaux systèmes de paiement sans espèces a également démarré. Elle met aux prises des sociétés qui rivalisent d'ingéniosité pour créer notre porte-monnaie numérique de demain, parmi lesquelles on peut citer Apple Pay, Google Wallet et Cashcloud. Comme toute technologie nouvelle, ces systèmes de paiement vont à coup sûr susciter l'intérêt des criminels, si bien que les consommateurs devront apprendre à les utiliser de façon aussi sécurisée que possible.

The Internet of Things

Cisco estime que le nombre de dispositifs connectés à Internet atteindra les 50 milliards en 2020[24]. En plus des ordinateurs, tablettes et autres smartphones, Internet connectera toutes sortes d'objets: douches, cuisines, lampes, thermostats, voitures etc. C'est en ce sens que nous pouvons parler de l'*Internet of Things*[25]*,* ou de l'Internet des objets. Il est à parier que cette dynamique va encore susciter des vocations chez les cybercriminels… D'où la nécessité encore plus grande de sensibiliser le public aux possibilités et aux risques des nouvelles technologies, ainsi qu'à une utilisation appropriée de ces dernières.

[19] http://heartbleed.com

[20] http://www.troyhunt.com/2014/04/24/badlepricon-bitcoin/

[21] https://access.redhat.com/articles/1232123

[22] SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy, November 2014, pp. 1-2

[23] http://time.com/3247717/jennifer-lawrence-hacked-icloud-leaked/

[24] SWITCHcert Report zu aktuellen Trends im Bereich IT-Security und Privacy, Oktober 2014, pp. 4-5

[25] http://postscapes.com/internet-of-things-examples/