KOBIK
SCOCI
CYCO

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

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

Rapport annuel 2012

AVANT-PROPOS

du conseiller d'Etat Christoph Neuhaus, président du comité directeur du SCOCI

On dit qu'il n'y a pas de lumière sans ombre. Cela est particulièrement vrai pour Internet, outil certes fascinant mais qui abrite aussi dans ses recoins les moins accessibles des activités criminelles méprisables. C'est le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) qui se charge d'aller éclairer ces zones d'ombre, de rester vigilant, de démasquer les coupables et de rendre possibles le dépôt de plaintes pénales. Dans sa fonction d'interlocuteur national pour toute personne souhaitant signaler des contenus suspects sur Internet, le SCOCI connaît malheureusement un véritable boom: le nombre de cas signalés en 2012 dépassait de 55 % celui de l'année précédente. Pour la première fois, le nombre d'annonces concernant la criminalité économique (37 %) a dépassé celui des annonces de cas de pornographie illicite (33 %).

Le SCOCI continue de remplir ses tâches principales avec professionnalisme, mais n'hésite pas à emprunter également de nouvelles voies. C'est dans cette idée que s'est tenu le premier "Forum Cybercrime Ministères publics – SCOCI". Cette rencontre avait entre autres pour objectif de mettre fin aux incertitudes existant au sein des ministères publics quant à la manière d'appréhender la cybercriminalité et quant aux différentes possibilités techniques.

Le travail du SCOCI ne se limite pas au traitement des annonces reçues du public. De par ses recherches actives sur Internet, non fondées sur des soupçons, le SCOCI est présent sur des terrains moins faciles d’accès et exerce de ce fait une fonction préventive. Le comité directeur du SCOCI redéfinit annuellement les axes principaux d’engagement dans ce domaine. Comme les années précédentes, la lutte contre la pédophilie sur Internet reste en 2012 l’axe principal d’intervention. Cependant, le comité directeur a également clairement affirmé que le SCOCI ne devait pas pour autant se détourner de la criminalité économique et de la cybercriminalité au sens strict du terme. Comme en témoignent les chiffres actuels, sa stratégie s'est avérée fructueuse. Le SCOCI est devenu indispensable.

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

Publié le 23 avril 2013

Table des matières

1. L’essentiel en bref

- En 2012, le SCOCI a reçu 8242 annonces par le biais de son formulaire en ligne. Cela représente une augmentation de 55 % par rapport à l’année précédente.

- 39 % des annonces concernaient des infractions contre le patrimoine. C'est ainsi que, pour la première fois, le nombre d'annonces concernant des infractions économiques dépasse celui des annonces concernant des cas d’infractions contre l’intégrité sexuelle (33 %); et ce en dépit du fait que ces dernières ont nettement augmenté par rapport à l'année précédente.

- Dans 383 cas, la pertinence pénale de l'annonce a permis de transmettre directement un dossier de soupçons à des autorités ou organisations nationales ou internationales.

- La recherche active sur les réseaux *peer-to-peer* a permis d’identifier 417 utilisateurs échangeant de la pédopornographie.

- Des investigations préliminaires secrètes menées par le SCOCI ont abouti à 33 dénonciations pénales aux autorités cantonales compétentes en 2012.

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

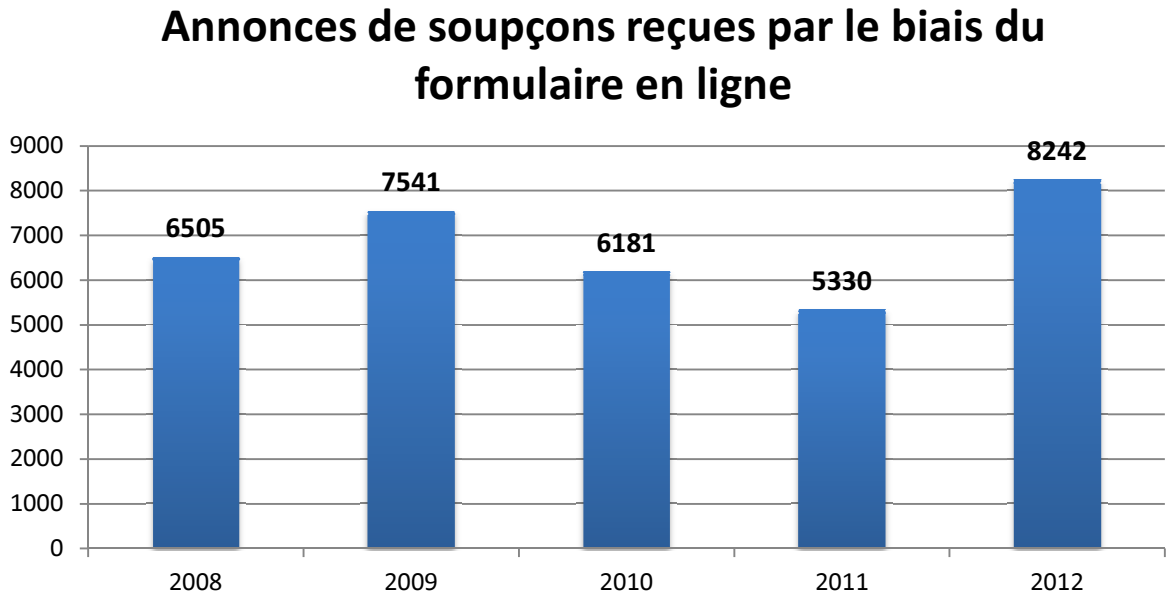
- Le 27 juin 2012, le Conseil fédéral a approuvé la stratégie nationale de protection de la Suisse contre les cyberrisques, à laquelle le SCOCI a participé activement. A travers cette stratégie, le Conseil fédéral, en collaboration avec les autorités, les milieux économiques et les exploitants d'infrastructures critiques, compte réduire les cyberrisques auxquels tous ces acteurs sont exposés quotidiennement.

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 lui parviennent par le biais du formulaire en ligne (www.cybercrime.ch) et peuvent donner lieu à des poursuites pénales, font l'objet d'un premier contrôle et d'une sauvegarde des données avant d'être transmises aux autorités de poursuite pénale compétentes en Suisse et à l'étranger.

2.1. Nombre d'annonces reçues

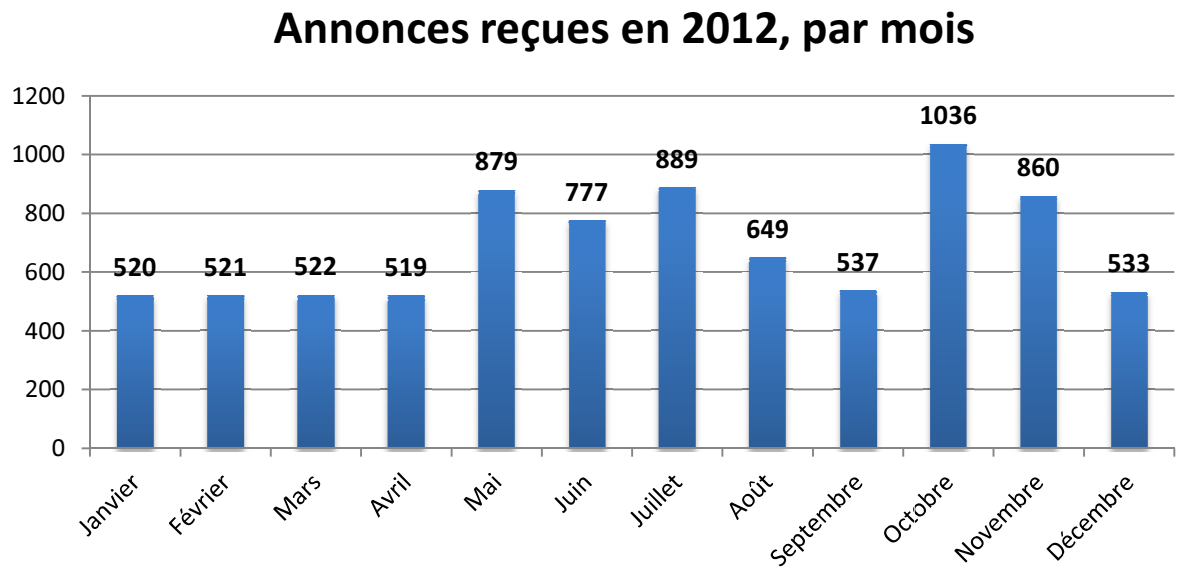
En 2012, le SCOCI a reçu **8242 annonces** par le biais de son formulaire en ligne, ce qui correspond à une augmentation de 55 % par rapport à l'année précédente (5330 annonces). Il convient de rappeler ici que ces chiffres ne permettent pas de conclusions fiables quant à l'évolution réelle de la cybercriminalité ou des contenus illégaux disponibles sur Internet. Les statistiques fournissent en revanche des indications sur la propension de la population à dénoncer les actes de cybercriminalité et sur la manière dont ces infractions sont perçues dans notre société.



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

Il y a plusieurs causes possibles à l'augmentation des annonces par le biais du formulaire en ligne: le fait que les médias aient relaté certains incidents peut avoir exercé une influence sur la population, mais les avertissements réguliers du SCOCI ont également pu jouer un rôle.

Au début de l'année 2012, le rythme d'entrée des annonces a été constant. Par la suite, divers incidents concrets et limités dans le temps ont touché de grandes parties de la population, provoquant une augmentation considérable du nombre d'annonces durant l'été et l'automne (cf. graphique 2).

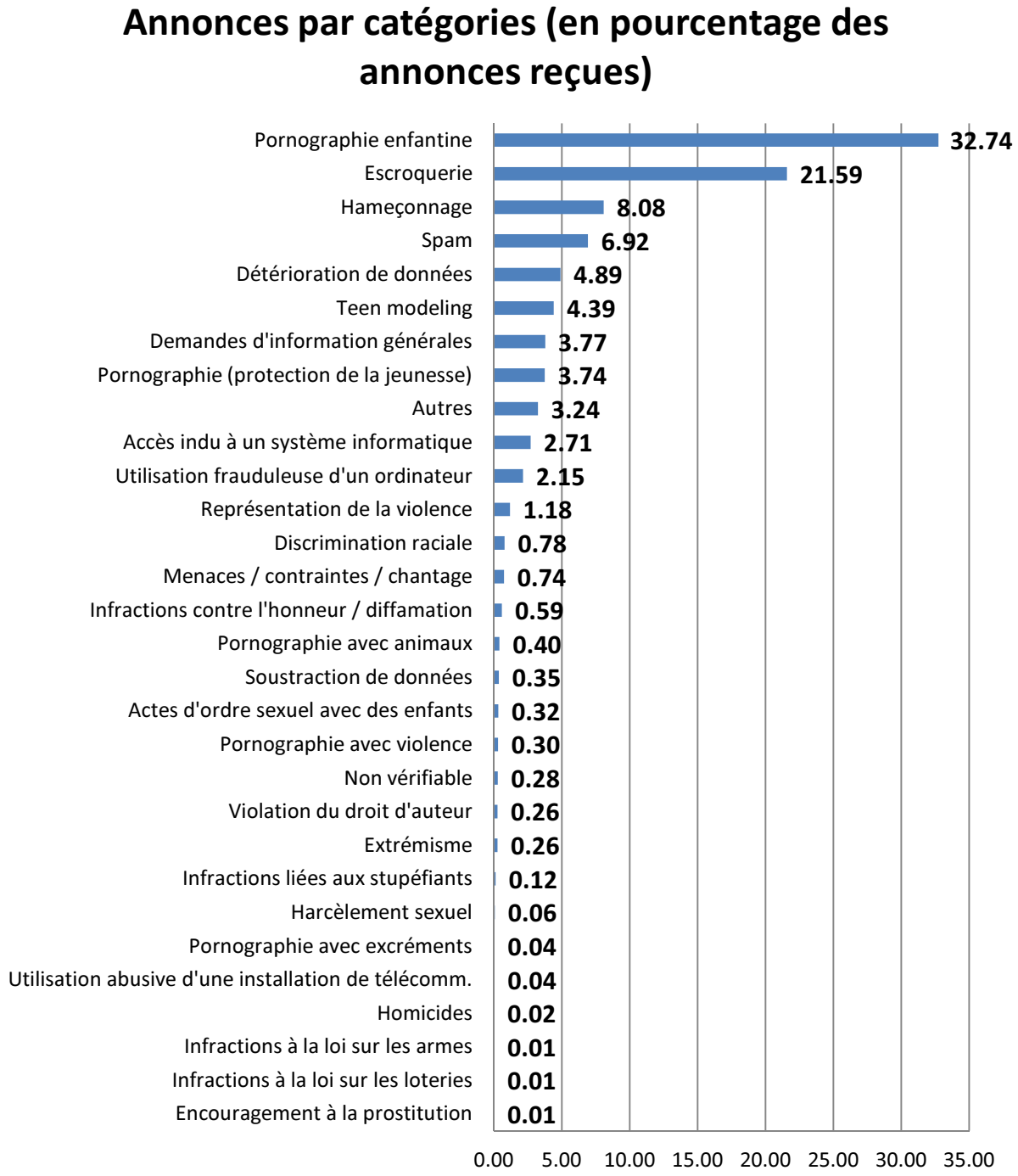


Graphique 2: annonces reçues par mois, par le biais du site www.scoci.ch (sur un total de 8242 annonces)

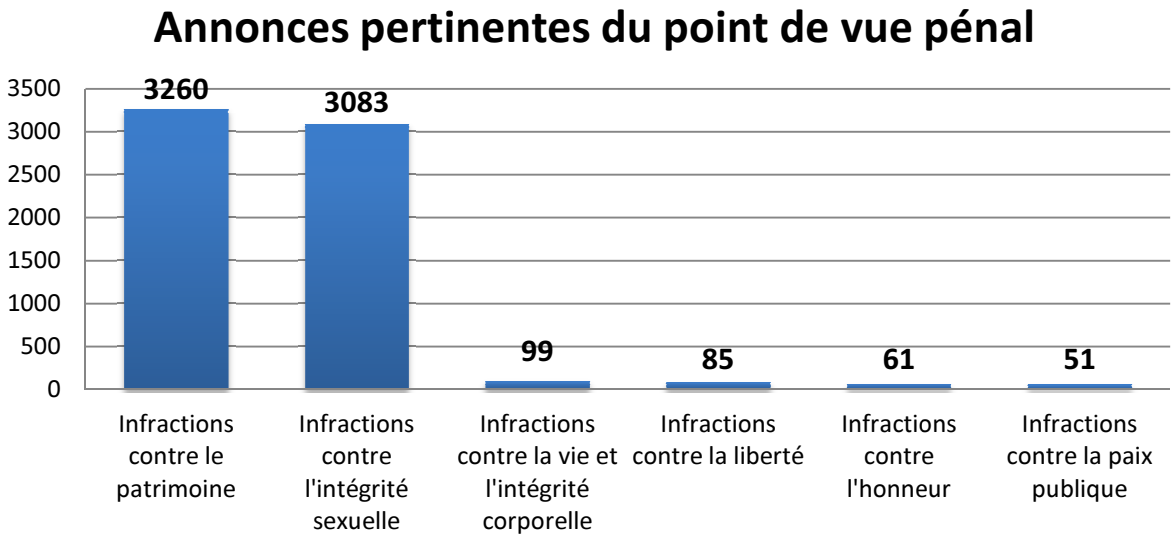
2.2 Types d'infractions enregistrées

Les annonces reçues par le biais du formulaire en ligne du SCOCI sont variées et généralement de bonne qualité. Plus de 80 % des annonces reçues en 2012 (6639) se sont avérées pertinentes du point de vue pénal. Les infractions dénoncées concernent en particulier des cas de pornographie interdite, de représentation de la violence, de racisme, d'extrémisme, de délits contre l'honneur, de menaces, de hameçonnage, d'escroquerie, d'accès indu à des systèmes informatiques, de détérioration de données et d'utilisation frauduleuse d'un ordinateur. De nombreuses annonces concernaient des infractions poursuivies sur plainte, ce qui signifie que la victime doit porter plainte pour que l'on puisse donner suite à l'affaire. Dans ce genre de cas, le SCOCI renvoie les personnes aux autorités de police locales.

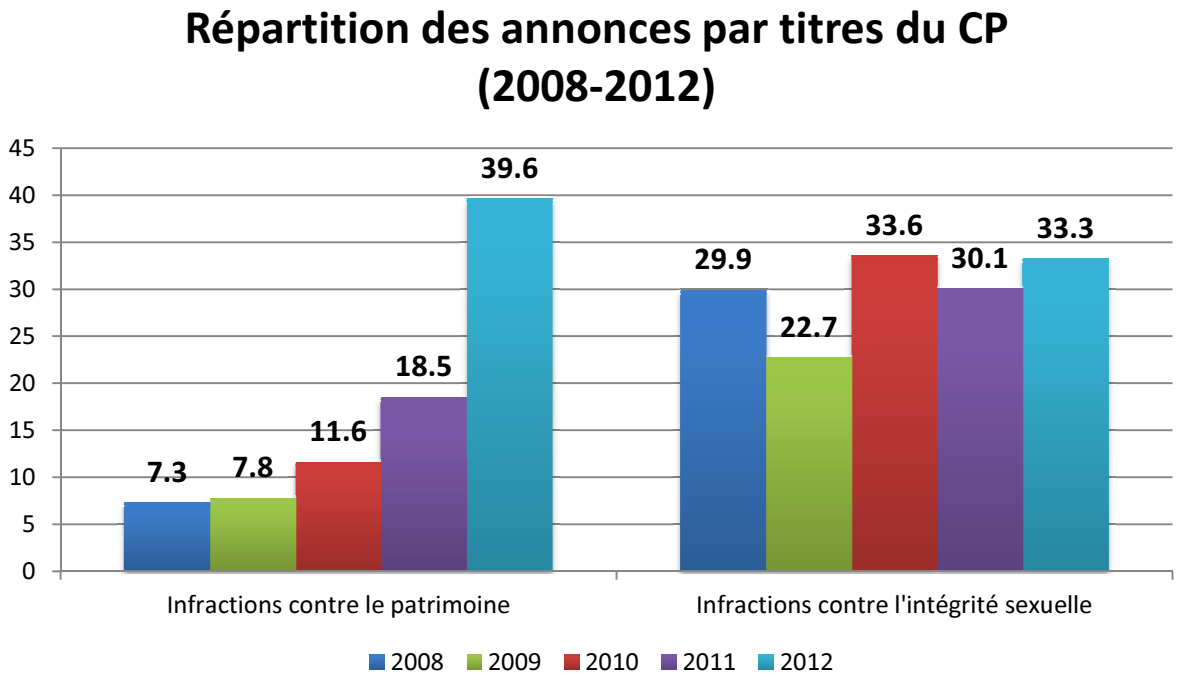
Pour la première fois depuis la création du SCOCI en 2003, la majorité des annonces concernait en 2012 des infractions contre le patrimoine (art. 137 à 172ter CP). Le nombre d'annonces de cette catégorie a connu une augmentation constante au cours des dernières années, tandis que le celui des annonces concernant des infractions contre l'intégrité sexuelle (art. 187 à 212 CP) est resté à un niveau élevé.



Graphique 3: importance des catégories sur l'ensemble des annonces reçues en 2012

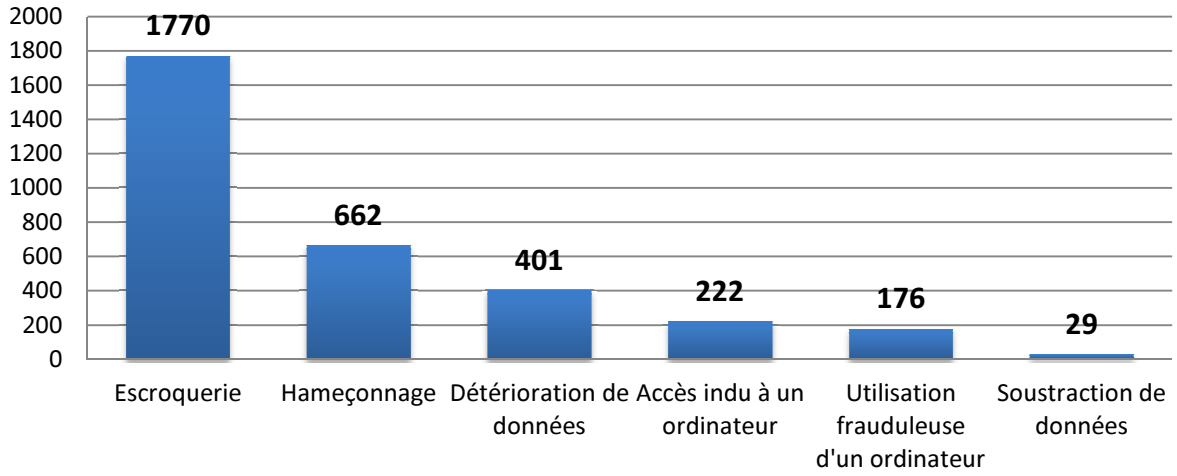


Graphique 4: annonces reçues en 2012, classées par catégorie d'infraction pénale (total: 6639)



Graphique 5: répartition des annonces de 2008 à 2012

a) Infractions contre le patrimoine



Graphique 6: annonces reçues concernant des infractions contre le patrimoine (total: 3260)

Avec un total de 1770 annonces, la catégorie "Escroquerie" comptabilise le plus grand nombre d'infractions contre le patrimoine dénoncées en 2012. Une grande partie des annonces concerne des cas d'offres frauduleuses sur des plateformes de petites annonces ou d'enchères en ligne, où le client a payé à l'avance une marchandise ou un service qu'il n'a jamais reçu. Par ailleurs, on signale de plus en plus de cas dans lesquels des personnes répondent à une annonce en prétendant être domiciliées à l'étranger. Une fois l'affaire conclue, le client exige le remboursement de taxes ou frais de douane en échange de son achat. Par la suite, il s'avère que cette personne n'a jamais eu l'intention d'acquérir le bien en question mais n'en voulait qu'à la somme du remboursement. Les plateformes immobilières sont les plus touchées par cette forme d'escroquerie.

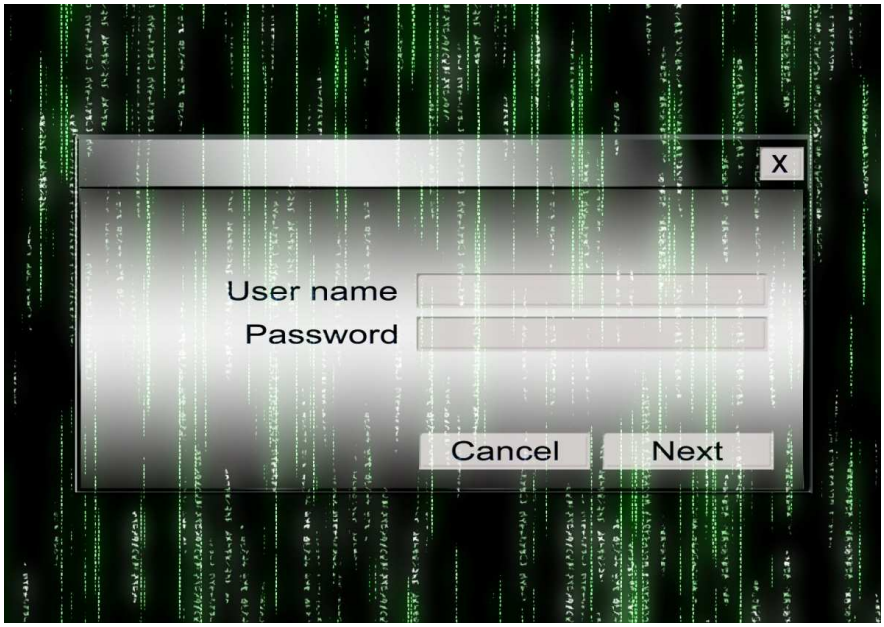
Les cas classiques de fraude à la commission ont une fois de plus été signalés en grand nombre cette année. Cette forme d'escroquerie consiste à faire miroiter des gains considérables à la victime en échange d'une petite avance. Les propositions sont en règle générale diffusées par le biais de l'envoi en masse d'e-mails (spam).

Pour la première fois cette année, les tentatives de hameçonnage (*phishing* en anglais) et le "**spam**" ont été saisis dans des catégories distinctes, étant donné que dans le domaine des e-mails envoyés en masse, le nombre d'annonces concernant de **tentatives de hameçonnage** a largement dépassé celui des messages publicitaires indésirables. En 2012, seuls 7 % des annonces reçues concernaient de la publicité indésirable. 8 % des annonces faisaient état de tentatives d'obtenir des données sensibles des internautes, généralement par le biais d'e-mails falsifiés ou d'appels téléphoniques frauduleux. Les escrocs s'intéressent particulièrement aux numéros de cartes de crédit, aux numéros de compte en banque, aux données d'accès aux comptes e-mail et aux informations d'e-banking. Les deux catégories mises ensemble comptabilisent 15 % des annonces reçues en 2012, ce qui correspond à l'importance de la catégorie générale "spams" de l'année précédente. On ne peut cependant pas en déduire une diminution réelle du nombre de spams, étant donné que les annonces reçues ne reflètent pas forcément la réalité. En effet, il faut également prendre en compte un certain effet d'habitude parmi les internautes face aux envois publicitaires, de même que l'amélioration des systèmes de filtre de spam, qui influencent fortement la propension à dénoncer un cas de spam auprès du SCOCI.

Le nombre d'infractions dénoncées relevant de la **cybercriminalité au sens strict du terme** a continué d'augmenter. Les catégories les plus touchées par cette hausse étaient "accès indu à un système informatique", "détérioration de données" et "utilisation frauduleuse d'un ordinateur".

De nombreux particuliers ont signalé que des inconnus avaient piraté leur compte e-mail ("accès indu à un système informatique") et avaient écrit aux contacts figurant dans leur carnet d'adresses pour leur soutirer de l'argent. Dans ce type d'e-mail, l'escroc se fait passer pour le titulaire du compte et demande une aide financière à ses contacts en prétendant être en voyage à l'étranger et se trouver dans une situation difficile.

Un autre exemple d'"**accès indu à un système informatique**" est le piratage de la page web d'entreprises ou d'associations dans le but d'obtenir des données sensibles sur ces dernières ainsi que sur les internautes visitant ces pages. Il peut s'agir notamment d'adresses e-mail, de mots de passe de comptes en ligne, de numéros de cartes de crédit, que les voleurs s'empressent de revendre sur des marchés spécialisés. Le vol de données va souvent de pair avec des actes de vandalisme contre le site lui-même, qui peuvent aller jusqu'à l'effacement total de banques de données ou de contenus web.

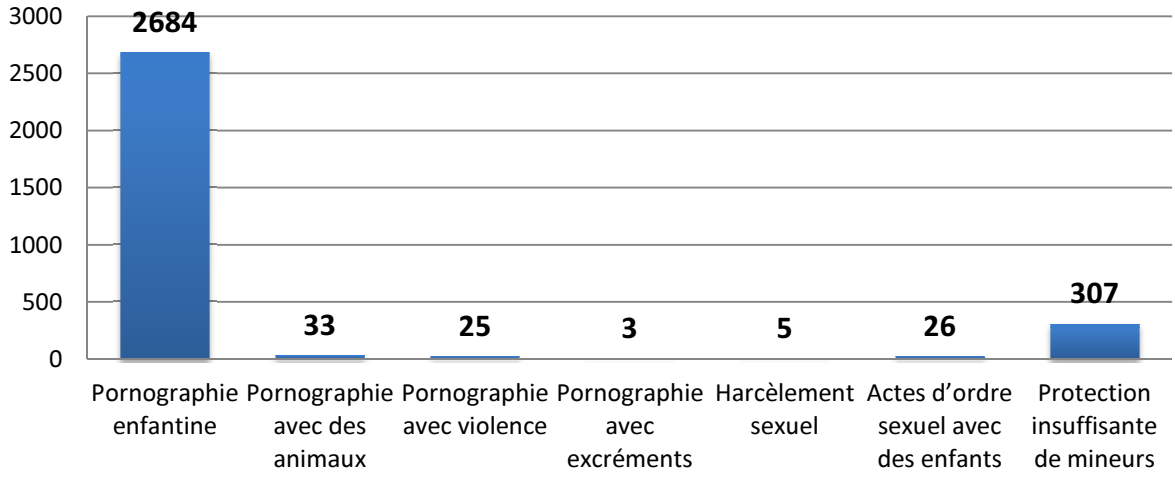


Source: Gerd Altmann / Pixelio

Le SCOCI a par ailleurs reçu des annonces concernant des menaces ou des cas réels d'attaques par déni de services (en anglais *denial of service attack*, ou DDoS) contre des exploitants de magasins en ligne. Dans leur e-mail, les pirates menaçaient de bloquer la page web concernée pendant plusieurs heures en inondant le réseau de demandes s'ils ne recevaient pas la somme exigée.

On mentionnera encore les annonces reçues concernant un logiciel malveillant envoyé au nom de l'Office fédéral de la police ou de la société de droits d'auteur SUISA, qui bloque des ordinateurs. Un message apparaît à l'écran, accusant l'utilisateur de s'être rendu coupable de téléchargements illégaux et l'enjoignant de payer une amende avoisinant les 100 francs pour faire débloquer son appareil, sous peine de poursuite pénale.

b) Infractions contre l'intégrité sexuelle

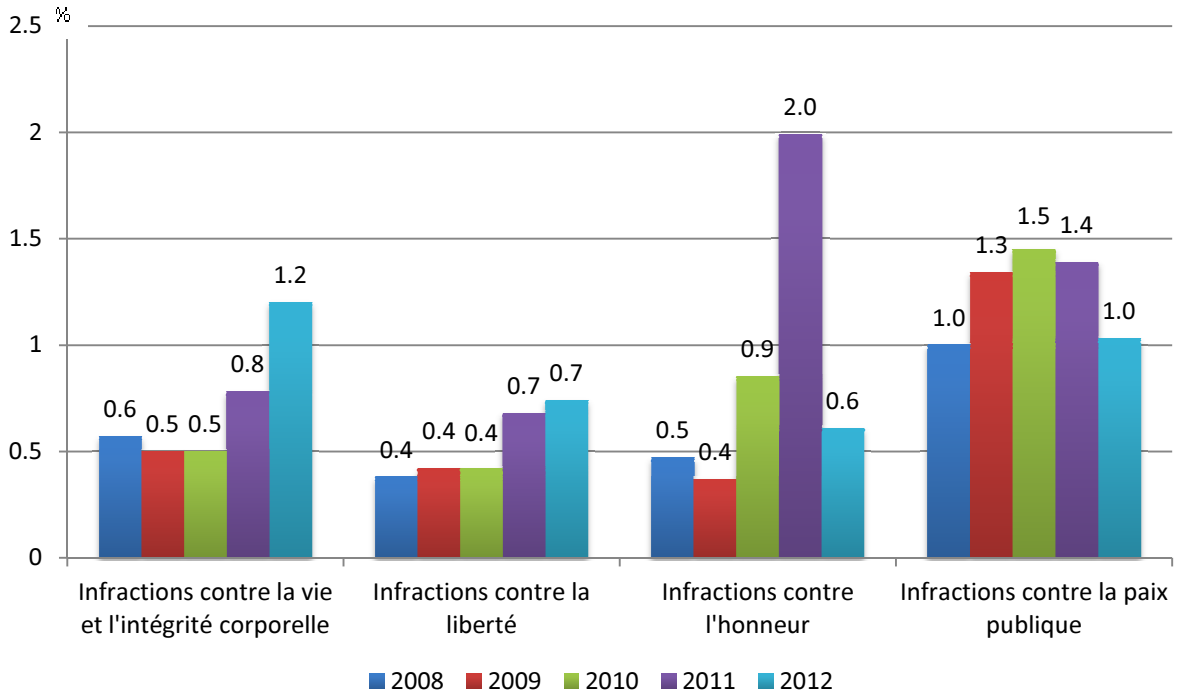


Graphique 7: annonces reçues concernant des infractions contre l'intégrité sexuelle (total: 3083)

La proportion d'annonces concernant des **"Infractions contre l'intégrité sexuelle"** a de nouveau légèrement augmenté en 2012. La grande majorité d'entre elles traitaient de diffusion de pornographie interdite impliquant des enfants. Par ailleurs, dans 307 cas, le SCOCI a été rendu attentif à des sites au contenu pornographique dont l'auteur de l'annonce pensait qu'il était trop facilement accessible à la jeunesse.

Source: S. Hofschlaeger / Pixelio

c) Autres infractions



Graphique 8: annonces reçues entre 2008 et 2012 concernant d'autres titres du CP (en pourcentage de l'ensemble des annonces)

Comme chaque année, le SCOCI a également reçu par le biais du formulaire en ligne des annonces concernant d'autres infractions. L'augmentation marquée de la catégorie "Infractions contre l'honneur" constatée en 2011 ne s'étant pas confirmée en 2012, il ne s'agit donc pas d'une nouvelle tendance. La baisse du nombre d'annonces pourrait s'expliquer par une plus grande retenue en matière d'usage des réseaux sociaux dans le sillage de la médiatisation croissante de la "cyberintimidation" (*cyberbullying* en anglais).

d) Synthèse

On constate l'émergence de deux tendances:

La première est liée à l'augmentation constante du nombre d'annonces reçues pour **infractions contre le patrimoine (infractions économiques)**, avec en tête des chiffres les tentatives d'escroquerie et de hameçonnage, suivies par les cas d'utilisation frauduleuse d'un ordinateur dans le but d'obtenir des données sensibles ou des paiements.

La deuxième met en évidence le fait que le nombre d'annonces reçues en 2012 pour **infractions contre l'intégrité sexuelle** reste élevé (3083 annonces contre 2150 en 2011). En termes de pourcentage, cette catégorie d'infraction est cependant supplantée par les infractions contre le patrimoine (cf. graphique 4).

2.3 Résultats des activités du SCOCI

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

- Chacune des 8242 annonces reçues a été examinée dans les délais impartis afin de déterminer sa pertinence du point de vue pénal et les compétences territoriales la concernant.

- Le SCOCI a répondu à 2200 de ces 8242 annonces sous la forme d'une lettre individuelle.

- 38 annonces ont, en raison de leur pertinence pénale, conduit directement à la transmission d'un dossier de soupçons à l'autorité ou au canton compétents.

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

- Des centaines d'annonces ont été transmises directement à des fournisseurs d'accès Internet (par ex. requêtes d'effacement de contenus illicites ou communication d'adresses IP).

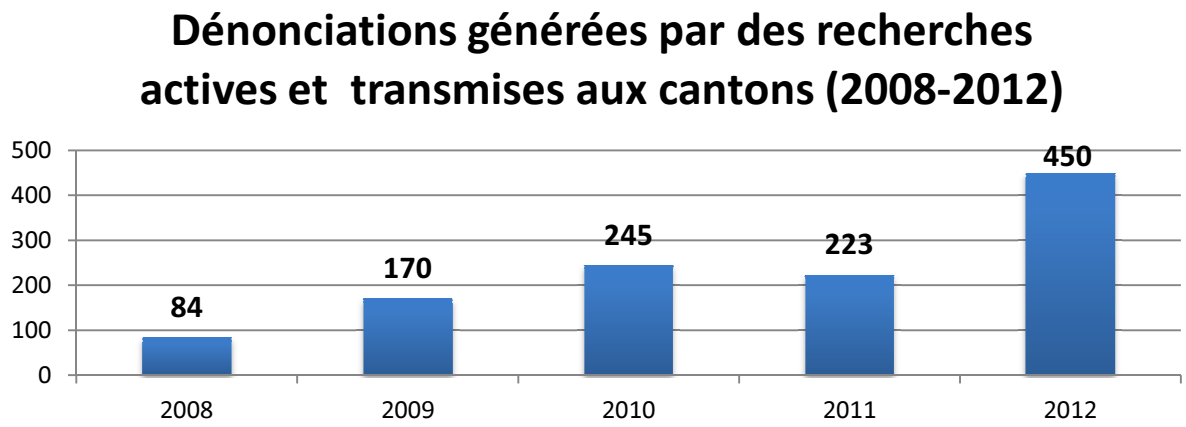
- De nombreuses annonces ont par ailleurs conduit à la transmission interne d'indices aux commissariats de la Police judiciaire fédérale (PJF) Criminalité générale, organisée et financière, Pédocriminalité et pornographie et Protection de l'Etat.

2.4 Exemple de cas

En 2012, le SCOCI a reçu plusieurs alertes concernant des annonces de suicide publiées sur Internet. Dans l'un de ces cas, une entreprise informatique française avait envoyé un formulaire d'annonce concernant un message de suicide publié sur une plateforme de jeux en ligne. L'équipe chargée de repérer les abus avait remarqué un utilisateur qui avait posté plusieurs commentaires suicidaires sur le forum d'un jeu en ligne très fréquenté. L'adresse IP de l'utilisateur indiquait qu'il se trouvait en Suisse, raison pour laquelle l'équipe a décidé de contacter immédiatement le SCOCI. Après avoir reçu l'annonce, le SCOCI a immédiatement procédé à une localisation de l'adresse IP, a trouvé l'adresse de la connexion Internet et a contacté les autorités policières compétentes. Les agents de la police cantonale ont ensuite pris contact avec les habitants du logement en question, identifié la fille de ces derniers comme étant l'auteur des messages suicidaires et pu s'entretenir directement avec cette dernière et ses parents, tout cela quelques heures à peine après la publication des commentaires. Il s'est avéré que les craintes pour sa santé n'étaient pas infondées et la jeune fille a pu bénéficier d'un soutien psychologique. Cet exemple impressionnant atteste de l'importance d'une collaboration coordonnée et centralisée entre autorités de poursuite pénale et entreprises privées.

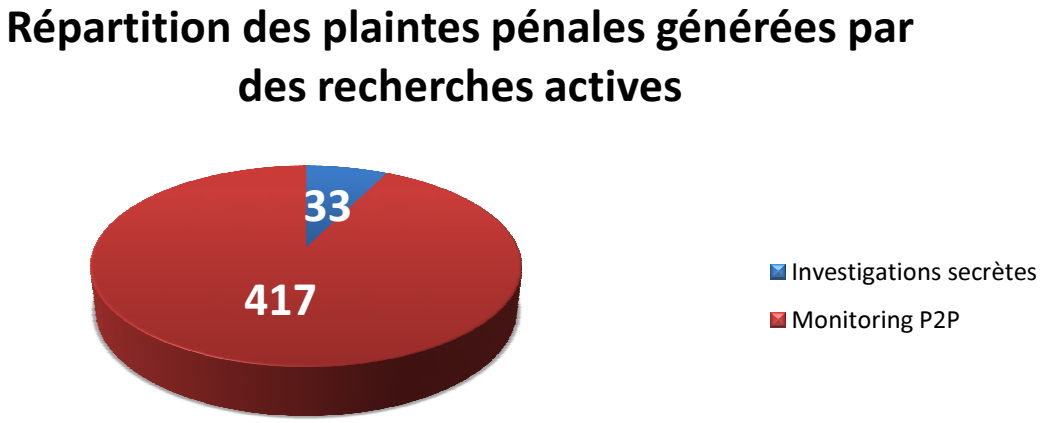
3. Recherche active (monitoring)

Le travail du SCOCI ne se limite pas au traitement des annonces reçues du public. De par ses recherches actives sur Internet et non fondées sur des soupçons, le SCOCI est présent sur des terrains moins faciles d'accès et exerce de ce fait une fonction préventive. Le comité directeur du SCOCI redéfinit annuellement les axes principaux d'engagement dans ce domaine. Comme les années précédentes, la lutte contre la pédophilie sur Internet reste en 2012 l'axe principal d'intervention. Cependant, le comité directeur a également clairement affirmé que le SCOCI ne devait pas pour autant se détourner de la criminalité économique et de la cybercriminalité au sens strict du terme.



Graphique 9: procédures pénales ouvertes dans le cadre de recherches actives du SCOCI (2008-2012)

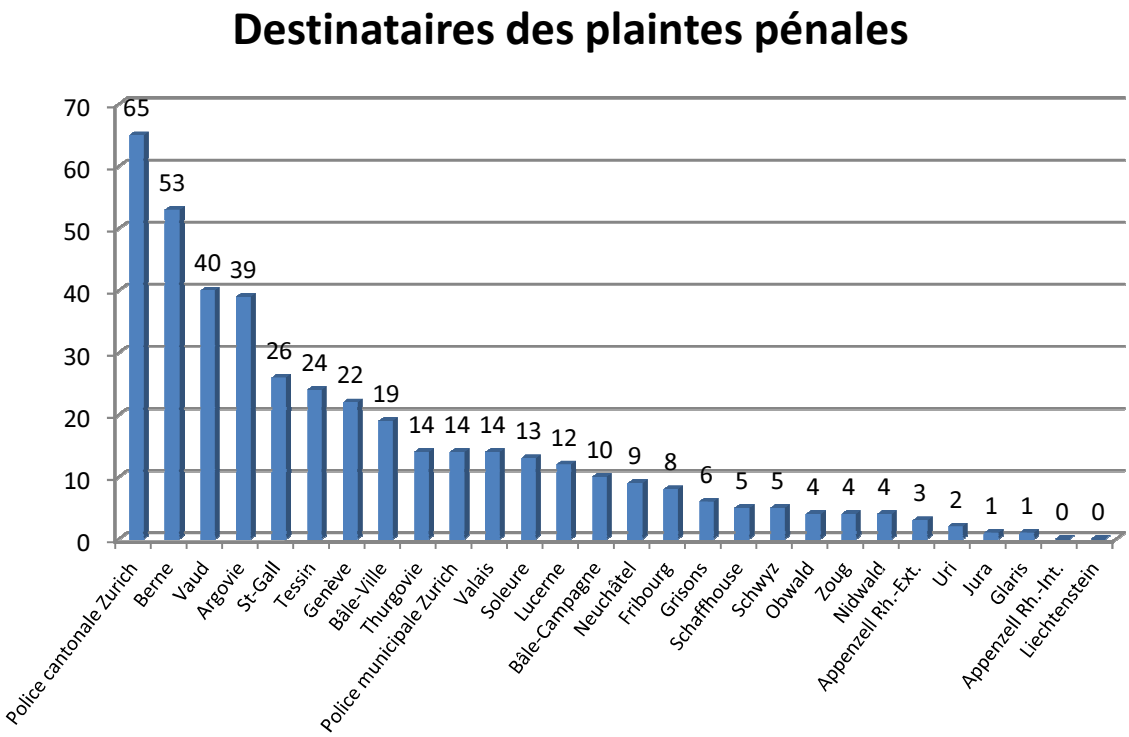
En 2012, ces recherches actives ont permis d'établir 450 dossiers de soupçons, ce qui représente le double des chiffres de l'année passée.



Graphique 10: origine des plaintes pénales générées par des recherches actives (total: 450)

3.1 Recherche active sur les réseaux *peer-to-peer* (P2P)

La grande majorité des dossiers (417 sur 450) sont issus du monitoring des réseaux *peer-to-peer* ciblant les utilisateurs échangeant de la pédopornographie en Suisse. En 2012, on a comptabilisé 214 dossiers de soupçons de plus que l'année précédente, ce qui correspond à une augmentation de 95 %. Les réseaux *peer-to-peer* restent un des moyens privilégiés utilisés pour échanger des contenus illégaux sur Internet de manière relativement anonyme. Cela dit, la nette augmentation du nombre de dossiers est surtout due au perfectionnement des logiciels utilisés pour les enquêtes et à l'optimisation des processus internes par le SCOCI.



Graphique 11: répartition des plaintes pénales selon la compétence cantonale (total: 417)

En ce qui concerne les destinataires de ces dossiers, on remarque que, comme lors des derniers exercices, ce sont les cantons les plus peuplés (comme Zurich, Berne et Vaud) qui se sont vus transmettre le plus de dossiers (cf. graphique 11).

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

3.2 Investigations préliminaires secrètes non ciblées

Source: Alexander Klaus / Pixelio

L'accord sur la collaboration lors d'investigations préliminaires sur Internet visant à lutter contre la pédocriminalité (monitoring des forums de discussion en ligne), conclu entre fedpol, le SCOCI et le Département de la sécurité du canton de Schwyz, règle les modalités de l'engagement de collaborateurs du SCOCI en tant qu'agents infiltrés pour lutter contre la pédocriminalité sur Internet[1]. Conformément audit accord, les collaborateurs du SCOCI mènent des investigations préliminaires secrètes exclusivement sous mandat et contrôle de la police cantonale schwyzoise. Il garantit que la surveillance préventive en matière de pédocriminalité sur Internet puisse continuer à être effectuée non seulement par les cantons, mais aussi par un service centralisé à l'échelon national.

Les investigations préliminaires secrètes menées par le SCOCI en 2012 ont conduit dans 33 cas à une dénonciation pénale aux cantons compétents. 13 de ces dénonciations reposaient sur des investigations menées sur des forums de discussion en ligne pour enfants. L'ensemble de ces 13 dénonciations avaient pour objet des tentatives d'actes d'ordre sexuel avec des enfants ou l'envoi de matériel pornographique à des mineurs.

En ce qui concerne les 20 autres cas, les investigations préliminaires secrètes ont eu lieu sur des bourses d'échange privées de type "peer-to-peer" (ou P2P). Dans ces cas, contrairement aux sites P2P classiques (cf. point 3.1), les données ne sont pas échangées dans un espace public: l'échange a lieu directement entre deux ordinateurs, raison pour laquelle l'investigation préliminaire secrète s'avère utile. Le domaine P2P privé n'avait jusqu'ici guère été couvert par les autorités suisses de poursuite pénale car ce type d'enquête requiert de lourds investissements en termes de temps et de personnel. Sachant que parmi ces 20 cas se trouvaient plusieurs récidivistes dans le domaine de la pornographie interdite et même des personnes déjà condamnées pour des infractions contre l'intégrité sexuelle, le SCOCI considère que sa décision d'étendre les investigations préliminaires secrètes aux bourses d'échange P2P privées était justifiée.

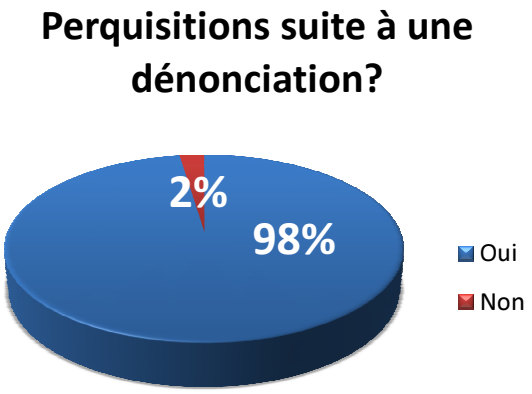
[1] Engagement au sens de l'art. 9*d* de l'ordonnance du 22 mars 2000 du canton de Schwyz concernant la Police cantonale (PolV – SRSZ 520.110).

3.3 Feed-back des cantons

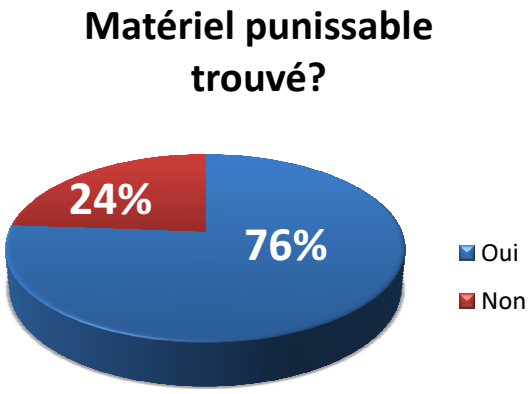
Source: Thorben Wengert / Pixelio

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

L'analyse des réponses des cantons est un outil important qui permet de vérifier l'efficacité de ces activités et la qualité des dossiers et dénonciations établis à l'intention des cantons. La grande majorité des dossiers concernant des cas suspects ont été constitués sur la base de recherches actives sur les réseaux P2P (417). Ces dossiers concernent donc des personnes qui participent activement à l'échange de contenus punissables à caractère pédopornographique.



Graphique 12: perquisitions domiciliaires en 2012



Graphique 13: matériel punissable en 2012

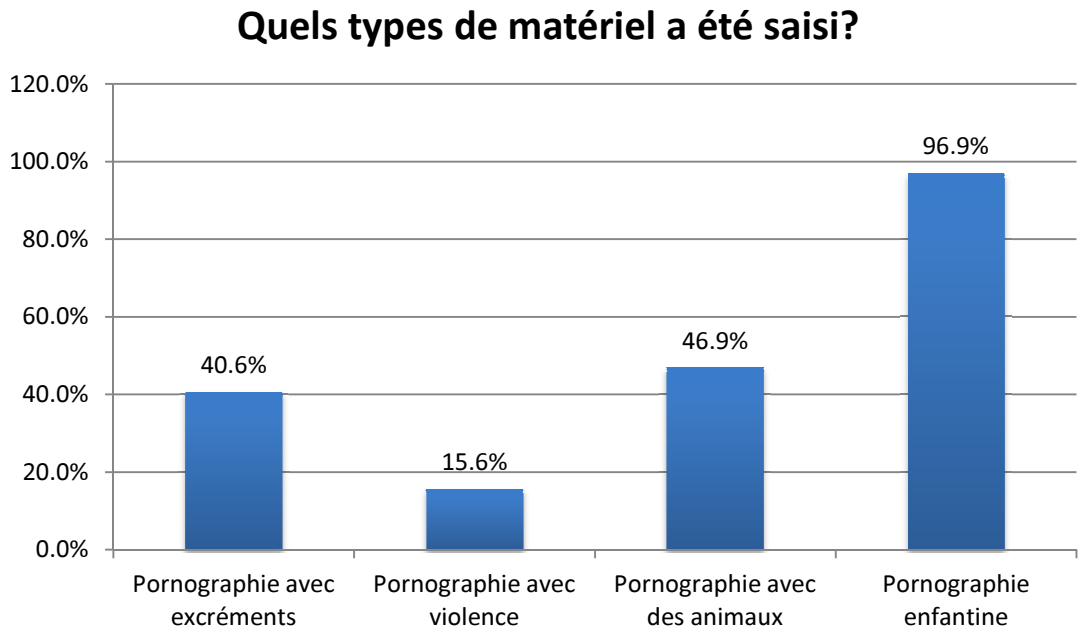
Les deux graphiques ci-dessus montrent que 98 % des dossiers transmis par le SCOCI ont été à l'origine de perquisitions domiciliaires effectuées par les autorités de police cantonales.

a) Feed-back des autorités de police cantonales

Dans 76 % des cas, ces perquisitions ont permis de saisir du matériel illégal. Les raisons des perquisitions infructueuses (24 % des cas) ne sont pas toujours faciles à déterminer. En général, un raccordement sans fil ouvert et non protégé ou le transfert de données vers des services de stockage en nuage (*cloud services*) empêchent une sauvegarde efficace des preuves et une identification certaine du suspect.

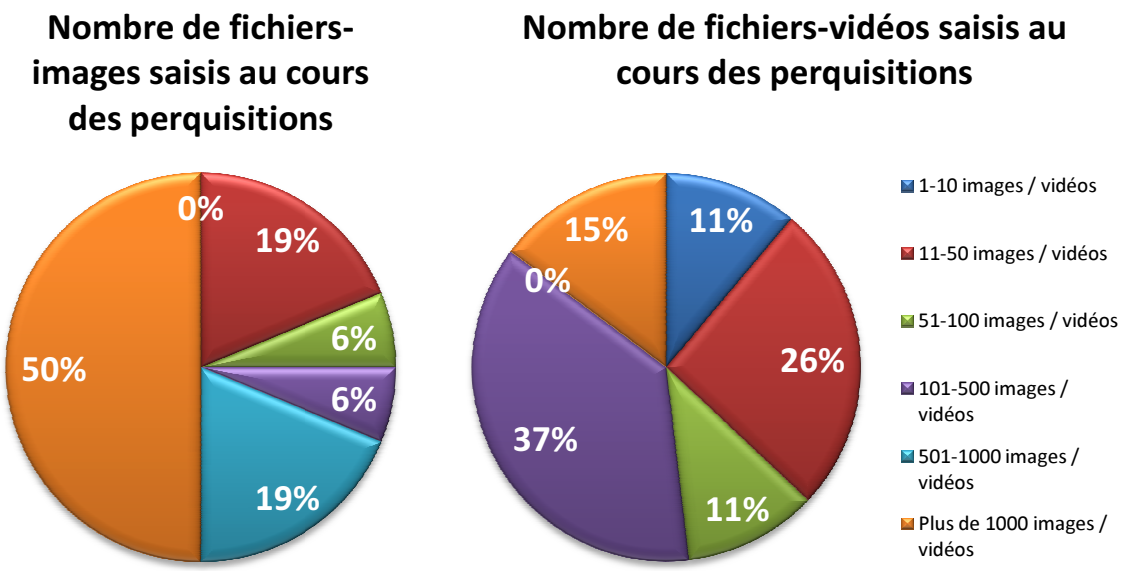
Par ailleurs, les chances de pouvoir saisir du matériel illégal dépendent aussi de la rapidité de l'intervention suivant l'annonce du SCOCI. En effet, plus les autorités tardent à intervenir, plus la probabilité que l'utilisateur ait déjà détruit les contenus illégaux ou changé d'ordinateur augmente.

97 % du matériel illégal saisi contenait du matériel pornographique impliquant des enfants. Ce haut pourcentage n'a rien d'étonnant car ce type de contenus est justement ciblé dans le monitoring des réseaux *peer-to-peer* et constitue de ce fait la grande majorité des dossiers de soupçons transmis aux cantons. Il est toutefois intéressant de relever que dans plus de la moitié des cas, un autre élément constitutif de la pornographie illégale (art. 197 CP) a été constaté (cf. graphique 14) et une perquisition sur deux a permis de saisir du matériel de pornographie impliquant des animaux.



Graphique 14: Quels types de matériel a été saisi en 2012?

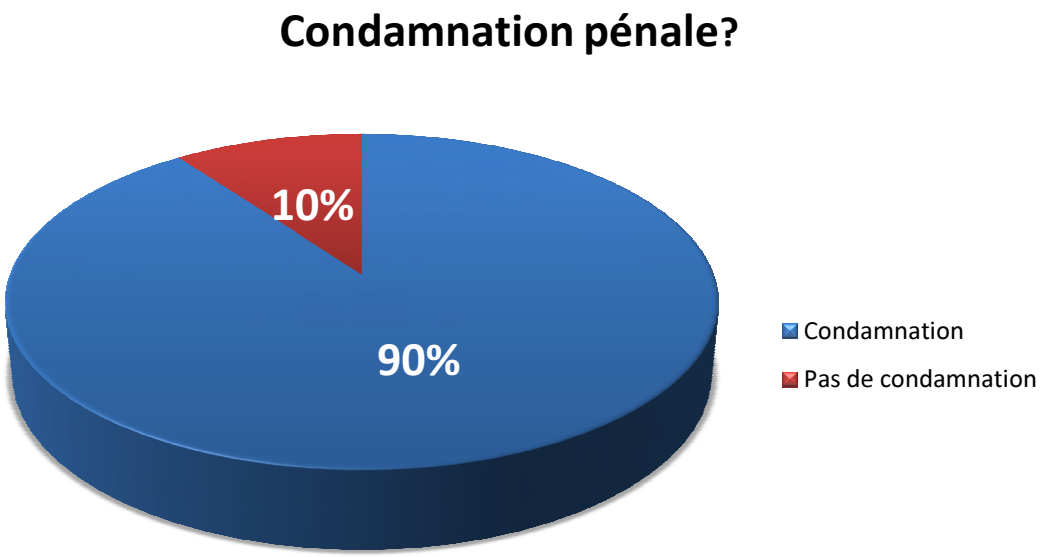
Les feed-back des autorités de police cantonales indiquent que, concernant la forme du matériel illégal saisi au cours des perquisitions, il s'agit de fichiers-vidéos (films) dans 94 % des cas et de fichiers-images (photographies) dans 66 %. Dans de nombreux cas, les deux types de fichiers sont saisis simultanément. Les quantités de matériel saisis peuvent parfois se compter en dizaines de milliers pour les films et en centaines de milliers pour les photographies.



Graphiques 15 et 16: vue d'ensemble de la quantité de fichiers-images et de fichiers-vidéos saisis

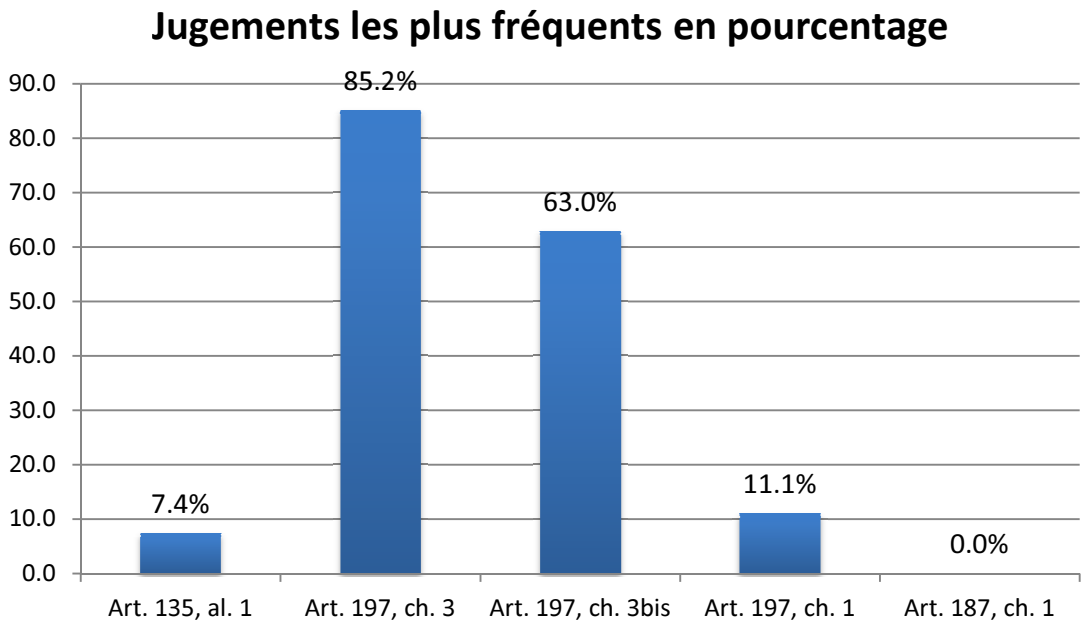
b) Feed-back des autorités judiciaires des cantons

Selon les données transmises au SCOCI par les autorités judiciaires des cantons, la procédure pénale a été suivie d'une condamnation dans 90 % des cas.



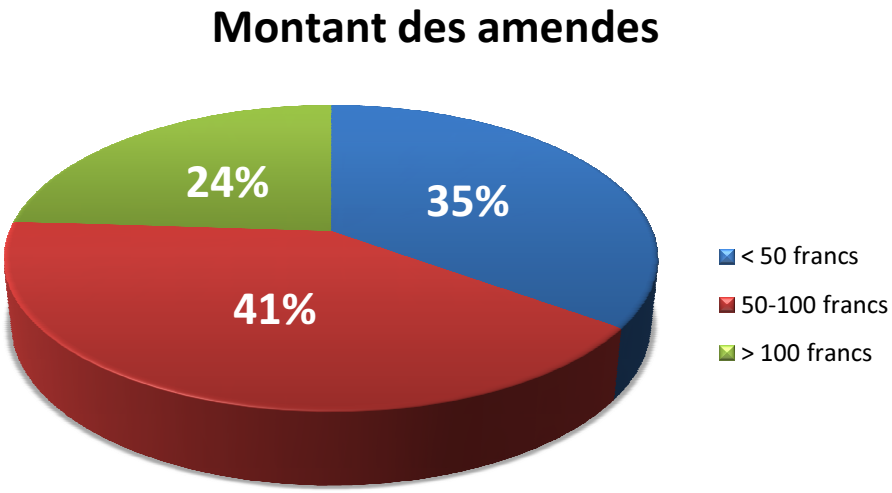
Graphique 17: condamnations pénales en 2012

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 chiffres 3 et 3bis.



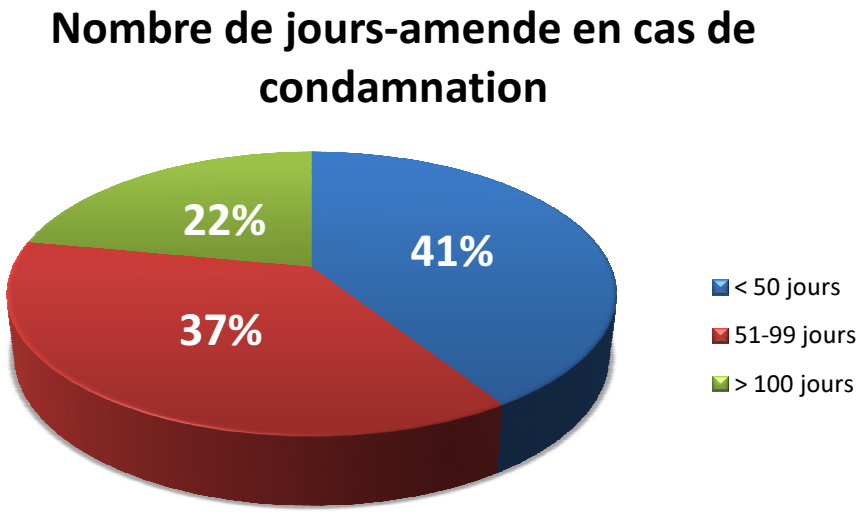
Graphique 18: jugements les plus fréquents en 2012 (en %)

La peine prononcée dans tous les cas de possession de pornographie illégale en 2012 est une **peine pécuniaire** (**jours-amende)** à laquelle s'ajoute une **amende** dans 63 % des cas. **96 % des peines pécuniaires sont assorties d'un sursis**. Aucune sanction alternative telle que le travail d'intérêt général, les mesures thérapeutiques, la peine privative de liberté (prison) et les peines pécuniaires fermes n'a été appliquée, confirmant une évolution déjà amorcée au cours des dernières années.

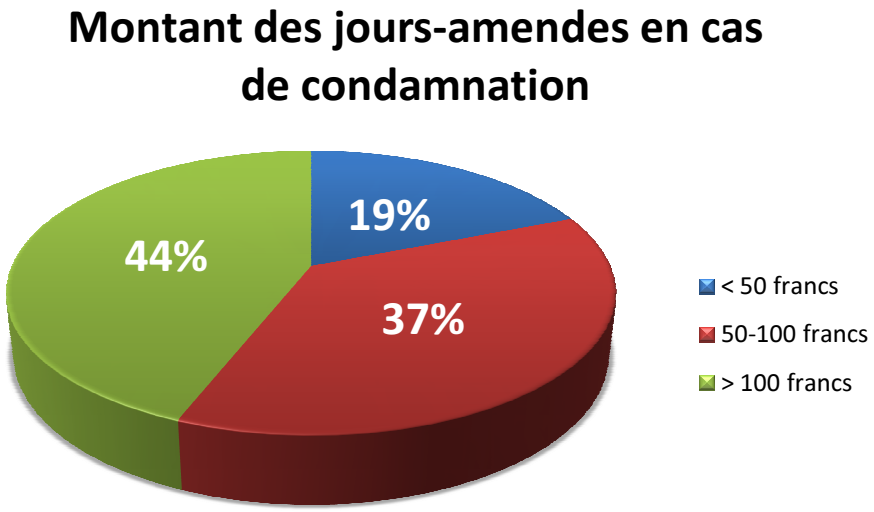


Dans 35 % des cas, les amendes sont inférieures à 1000 francs et dans 41 % des cas, elles vont de 1000 à 2000 francs. Dans 24 % des cas seulement, les amendes sont supérieures à 2000 francs.

Dans 41 % des peines pécuniaires, le nombre des jours-amendes est inférieur à 50. Dans 37 % des cas, ce nombre est compris entre 51 et 100. Ce n'est que dans 22 % des cas que 100 jours-amende ont été prononcés.



Dans 19 % des cas, des jours-amende ont été prononcés pour un montant de 1 à 50 francs, dans 37 % des cas de 51 à 100 francs et dans 44 % des cas au-delà de 100 francs.



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

3.4 Exemple de cas

L'exemple de cas qui suit illustre le cheminement des enquêtes préliminaires menées indépendamment de tout soupçon sur les réseaux *peer-to-peer.* L'enquête menée par la police cantonale sur la base du dossier transmis par le SCOCI a montré que le suspect s'était rendu à deux reprises à l'étranger où il a abusé de plusieurs enfants, devant une caméra, pour ensuite publier ces prises de vue sur Internet. Par la suite, l'enquête a permis de déterminer que le suspect avait abusé aussi de son propre enfant âgé de trois ans.

Jusqu'à la communication de soupçons transmise par le SCOCI, l'individu n'était pas connu des services de police. Grâce à la collaboration entre le SCOCI et la police cantonale chargée de l'affaire et aux enquêtes très poussées de la police, l'auteur de l'infraction a pu être démasqué et son enfant, ainsi que d'autres enfants probablement, seront désormais protégés des abus.

Ce cas souligne de manière exemplaire l'importance du traitement systématique des cas suspects sur les réseaux *peer-to-peer* par les autorités cantonales. Du fait du manque de ressources, certains cantons sont fortement mis sous pression face à l'augmentation du nombre de dossiers transmis par le SCOCI. L'énorme surplus de travail que ces dossiers représentent les place parfois face à de grandes difficultés quant aux délais à respecter.

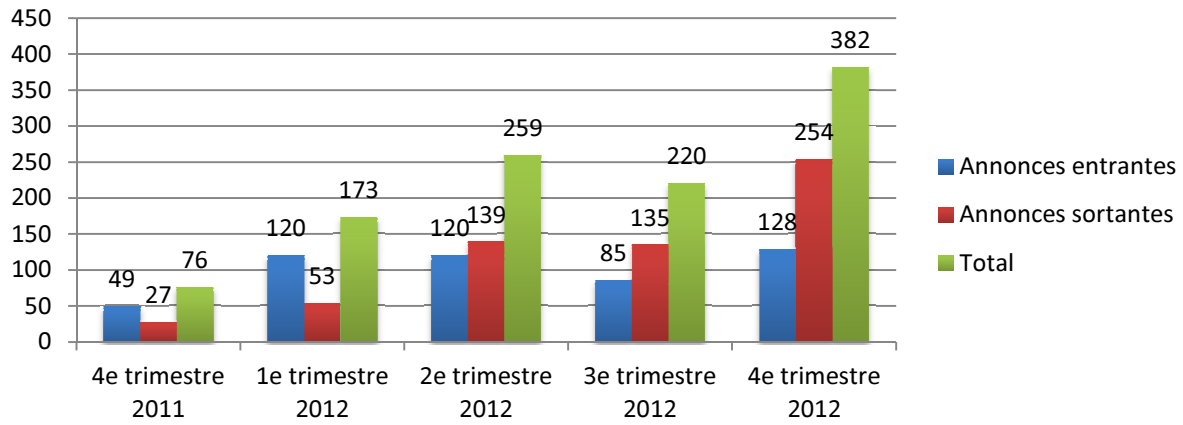
4. Echange d'informations de police judiciaire

Depuis l'entrée en vigueur de la Convention du Conseil de l'Europe sur la cybercriminalité (CCC) le 1er janvier 2012, la Suisse participe davantage de manière active à la lutte contre la criminalité sur Internet. Cela se traduit en premier lieu par une forte augmentation de l'échange d'informations de police judiciaire avec les autorités étrangères sur des cas entrant dans le champ d'application de la convention. Par ailleurs, la décision du comité directeur du SCOCI de ne pas éloigner totalement le SCOCI de la criminalité économique et de la cybercriminalité au sens strict du terme, ainsi que son association au domaine policier de fedpol n'ont pas été sans influence. En effet, l'échange d'informations de police judiciaire et les activités de coordination ont augmenté depuis l'intégration du SCOCI en 2009 dans la Police judiciaire fédérale. C'est ce que montrent les chiffres ci-dessus.

Echange d'informations de police judiciaire avec des autorités étrangères en 2012

Les statistiques montrent qu'en 2012, 483 annonces relevant du champ d'application de la CCC ont été reçues. Au cours du seul quatrième trimestre 2012, 128 annonces ont été adressées au SCOCI en provenance de l'étranger, ce qui représente une augmentation de 161 % par rapport à l'année précédente (49 annonces au 4e trimestre 2011). Le même phénomène est à relever à propos des annonces sortantes que le SCOCI a rédigées à l'intention des autorités étrangères de poursuite pénale, en corrélation directe avec l'augmentation du nombre des annonces entrantes. Au cours de l'année écoulée, le SCOCI a établi 561 annonces destinées à l'étranger (Interpol et Europol). Si l'on compare les annonces du 4e trimestre 2012 (254 annonces) à celles du 4e trimestre 2011 (27), on constate une augmentation considérable.

Evolution des annonces entrantes/sortantes 2011-2012



4.1 Exemple de cas

Les deux cas présentés ci-dessous illustrent la rapidité et l'efficacité qui caractérisent l'échange d'informations de police judiciaire conformément à la CCC:

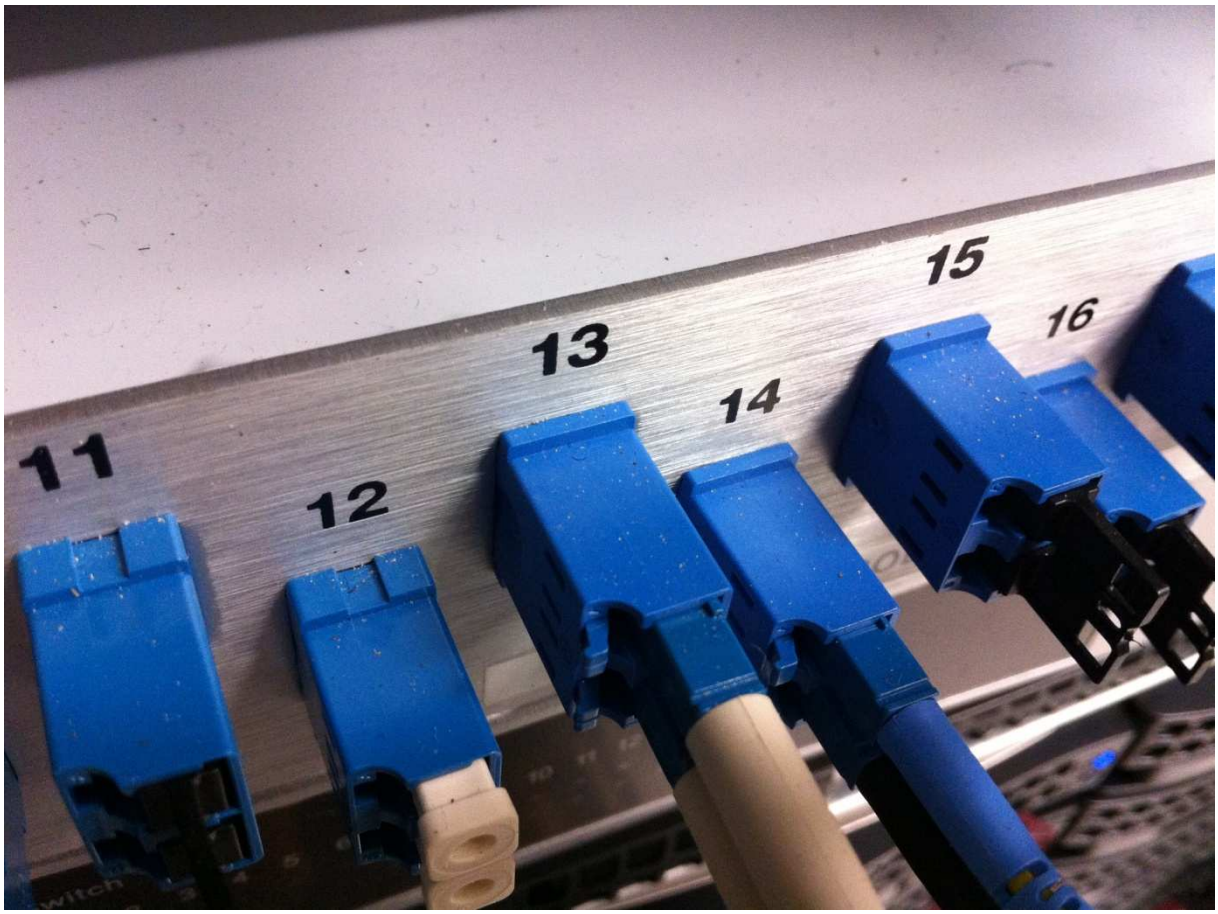
Un bureau Interpol a envoyé au SCOCI une annonce selon laquelle plusieurs membres de partis politiques du pays requérant avaient reçu par courrier électronique des menaces de mort. Les données concernant le courriel de menaces présentaient un lien avec la Suisse et ont été communiquées au SCOCI. Grâce au processus de coopération déjà défini du SCOCI avec le fournisseur d'accès concerné, il a été possible dans les 24 heures de sécuriser toutes les données et d'obtenir des indices complémentaires permettant d'identifier le propriétaire du raccordement, ainsi que d'informer les services de police du canton concerné. Le bureau Interpol a été immédiatement informé de toutes les informations nécessaires dans la perspective d'une éventuelle demande d'entraide judiciaire.

Par l'intermédiaire d'un bureau Interpol étranger, le SCOCI a été informé de plusieurs cas de chantage par courriels. Tous ces messages avaient le même contenu et le même expéditeur. Leurs auteurs demandaient des sommes d'argent considérables et menaçaient un grand distributeur international d'attentats à la bombe dans ses filiales en cas de refus. L'un des courriels avait été envoyé à partir d'un compte de courrier électronique suisse et était directement adressé au directeur d'une filiale de ce grand distributeur. Le SCOCI a immédiatement demandé aux autorités de police compétentes de sauvegarder les données auprès du fournisseur d'accès suisse. Cette mesure a représenté un soutien rapide et considérable pour le bureau Interpol qui avait transmis la demande dans son enquête visant à identifier l'auteur présumé.

5. Projets

5.1 Collection nationale de fichiers et de valeurs de hash

Ce projet a pour but de transmettre au SCOCI les fichiers (images et vidéos) saisis dans le cadre d'enquêtes en matière de pornographie enfantine, après un premier classement opéré par les autorités cantonales compétentes. Le SCOCI calcule une valeur de hash pour chaque fichier[2] et l'enregistre dans la collection nationale de fichiers et de valeurs de hash (CNFVH) ensuite mise à la disposition des cantons. Les autorités cantonales compétentes calculent aussi les valeurs de hash pour tous les nouveaux fichiers qu'elles saisissent. Elles peuvent ensuite comparer leurs propres stocks cantonaux de valeurs de hash avec la liste des valeurs de hash du SCOCI. Cette comparaison permet de vérifier d'énormes quantités de données sans devoir visualiser le contenu lui-même. Il est ainsi possible d'identifier automatiquement les duplicatas ainsi que les fichiers-images et les fichiers-vidéos déjà connus. Cette méthode permet aux enquêteurs de gagner du temps et leur épargne l'épreuve psychique de la visualisation des images saisies.



Source: Gerd Altmann / Pixelio

[2] Valeur unique permettant d'identifier une donnée, notamment une image (empreinte digitale numérique)

La CNFVH a été conçue et élaborée sous l'égide du SCOCI avec la participation des autorités de police cantonales. Pour la première fois, une liste nationale uniforme des valeurs de hash a été élaborée conformément à des critères applicables de manière générale.

La réalisation technique visait principalement le développement d'une solution performante pour l'élaboration et la comparaison de grandes quantités de données dans les systèmes de banques de données.

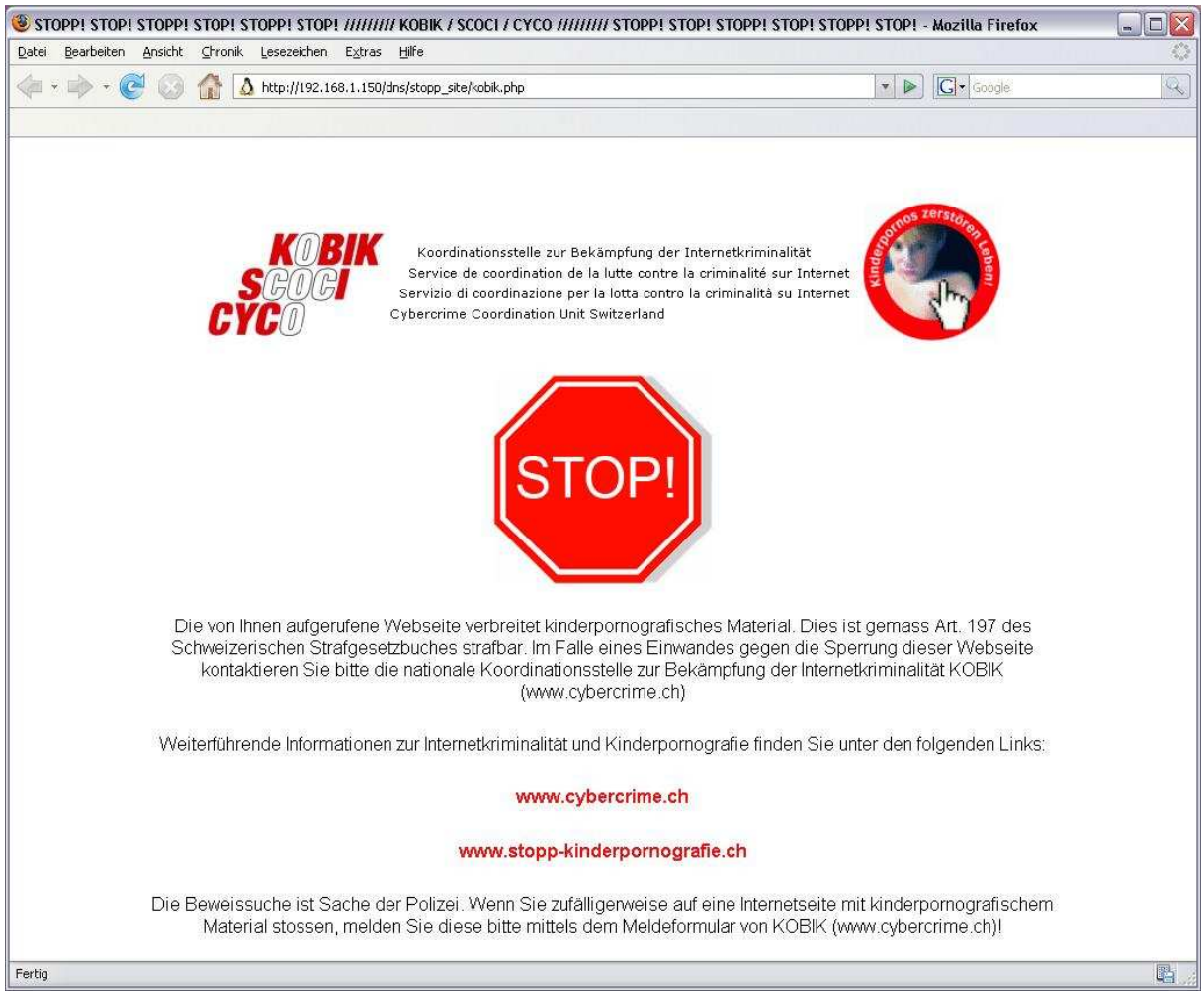
L'année 2012 constitue une étape dans la réalisation du projet-pilote de CNFVH. En février, les ordinateurs nécessaires à la CNFVH ont été mis en place. D'avril à juillet, le SCOCI a installé des programmes spécifiques et a procédé aux premiers essais. En octobre, les derniers tests ont été effectués avec succès, de même pour les adaptations de systèmes, et la CNFVH a été mise en exploitation. Les services cantonaux et municipaux peuvent maintenant soumettre les images saisies, préalablement soumises à une précatégorisation, afin que le SCOCI puisse en terminer la catégorisation (sur la base d'un double contrôle) et les transférer dans la CNFVH.

5.2 Projet de monitoring des réseaux *peer-to-peer*

Dans le cadre du monitoring effectué à titre préventif, le SCOCI a mis sur pied au cours des dernières années en collaboration avec l'ONG Action Innocence Genève (AG), un programme de surveillance des réseaux *peer-to-peer*. Ce logiciel a pour but de lutter contre l'échange de matériel pornographique mettant en scène des enfants sur les réseaux Internet *peer-to-peer*. Le développement de ce programme se poursuit en étroite coopération avec Action Innocence Genève qui en assume entièrement le financement, qui se charge de sa mise à jour et le met à la disposition des autorités de poursuite pénale.

Ce monitoring effectué sur Internet indépendamment de tout soupçon a permis en Suisse de découvrir et d'arrêter non seulement de purs "consommateurs", dont le comportement encourage la production de matériel nouveau, mais aussi des "acteurs" pédocriminels dont certains ont abusé eux-mêmes de jeunes enfants et produit à cette occasion du matériel-images.

5.3 Collaboration avec les fournisseurs d'accès à Internet



Depuis 2007, le SCOCI collabore avec les principaux fournisseurs d'accès suisses dans le but de bloquer l'accès à des sites de pédopornographie. Ce blocage vise uniquement les sites hébergés à l'étranger qui véhiculent des contenus de pornographie enfantine. Concrètement, le SCOCI met à la disposition des fournisseurs d'accès une liste de sites Internet de pornographie enfantine, mise à jour en continu (env. 200 à 300 sites Internet). En conformité avec leur position éthique et leurs conditions générales, ces fournisseurs bloquent l'accès à des sites pénalement punissables et redirige leurs utilisateurs vers une page "stop".

Dans le cadre de ce projet, le SCOCI collabore étroitement avec Interpol. Interpol tient également une liste des pages Internet sur lesquelles se trouvent des photos et des vidéos d'abus impliquant des enfants (la liste "worst of" d'Interpol). La liste utilisée en Suisse s'appuie sur cette liste d'Interpol complétée par des pages Internet propres à la Suisse. La liste "worst of" est intégrée quotidiennement à la liste du SCOCI. De son côté, le SCOCI informe Interpol de nouveaux sites Internet, lesquels seront à leur tour ajoutés à la liste d'Interpol.

6. Groupes de travail, partenariats et contacts

6.1 Groupes de travail nationaux

Au cours de l'exercice 2012, le SCOCI a été représenté au sein de différents groupes de travail nationaux.

Ainsi, le SCOCI s'est engagé cette année encore dans le groupe de travail national "Kindsmissbrauch" (abus sur les enfants), aux côtés du Commissariat Pédocriminalité et pornographie de la Police judiciaire fédérale, de plusieurs organisations d'utilité publique, de représentants des cantons et de la Prévention suisse de la criminalité.

Comme durant l'année précédente, le SCOCI a aussi poursuivi en 2012 son engagement dans le cadre du programme national "Protection de la jeunesse face aux médias et compétences médiatiques". Le SCOCI siège à la fois dans le groupe de travail chargé d'élaborer le programme d'action et dans le groupe d'accompagnement. Ce programme vise avant tout à aider les enfants et les adolescents à utiliser les médias de façon sûre, responsable et adaptée à leur âge.

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

Le SCOCI participe également aux groupes de travail "Enquêteurs TI" et "Surveillance des télécommunications", ce qui lui permet d'être au fait de l'évolution technologique et de veiller à une efficacité accrue dans le domaine de la poursuite pénale.

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

Source: Gerd Altmann / Pixelio

6.2 Collaboration avec d’autres services de la Confédération

Au cours de l'exercice 2012, le SCOCI a poursuivi sa collaboration avec différents services de la Confédération dans la lutte contre la criminalité sur Internet. Au sein de fedpol, le SCOCI collabore étroitement avec les commissariats Investigations secrètes, Protection de l’Etat, Enquêtes TI, et avec la Division principale Coopération policière internationale (CPI). En raison de la proximité des thématiques traitées, le SCOCI et le Commissariat Pédocriminalité et pornographie sont par ailleurs en contact particulièrement étroit.

Par ailleurs, les contacts ont été élargis ou intensifiés avec d’autres partenaires fédéraux. Citons notamment la Centrale d’enregistrement et d’analyse pour la sûreté de l’information (MELANI), le Domaine de direction Entraide judiciaire internationale de l’Office fédéral de la justice (OFJ), l’Office fédéral de l'informatique et de la télécommunication (OFIT), l’Office fédéral des assurances sociales (OFAS), l'Office fédéral de la communication (OFCOM), le secrétariat d'Etat à l'économie (SECO) et la Commission fédérale contre le racisme (CFR).

Divers entretiens avec le Ministère public de la Confédération ont permis de discuter de certaines actions communes majeures et d'améliorer la collaboration. Cela s'est traduit concrètement par la décision de la Police judiciaire fédérale de transmettre dans les délais au SCOCI toutes les informations émanant des procédures d'enquêtes fédérales touchant à la criminalité sur Internet au sens strict. Cela permettra au SCOCI de mieux remplir ses tâches, par exemple fournir une vue d'ensemble des cas, analyser la situation en matière de cybercriminalité en Suisse ou assurer le lien entre les autorités de police et le Service de renseignement via MELANI.

6.3 Echanges d'expériences avec les cantons

La collaboration avec les différents représentants des autorités de police et des ministères publics des cantons a été particulièrement intense au cours de l’exercice 2012. En plus des échanges d’informations habituels, plusieurs séances de travail ont eu lieu, en particulier à propos des investigations préliminaires secrètes et du projet de CNFVH.

En 2012, le premier "Forum Cybercrime Ministères publics – SCOCI" a été organisé. Cette rencontre avait entre autres pour objectif de mettre fin aux incertitudes existant au sein des ministères publics quant à la manière d'appréhender la cybercriminalité et quant aux différentes possibilités techniques. A l'occasion de ce forum, plusieurs experts ont présenté une vue d'ensemble de la lutte contre la cybercriminalité en lien avec la pratique et leurs besoins. Le vif intérêt manifesté par les ministères publics a montré que l'initiative lancée par le Ministère public de Zurich était justifiée et qu'il avait été judicieux d'élargir la rencontre au-delà des frontières cantonales.

Source: Gerd Altmann / Pixelio

6.4 Collaboration avec Action Innocence Genève

Depuis de nombreuses années, le SCOCI collabore avec l'ONG Action Innocence Genève[3] dans le cadre de la lutte contre la pornographie enfantine. C'est en particulier grâce au soutien opérationnel de cette organisation que le projet de monitoring des réseaux *peer-to-peer* a pu être mis en place et développé avec succès au cours des dernières années. La collaboration avec Action Innocence est donc fondamentale puisque c'est grâce au logiciel fourni par Action Innocence qu'une nette majorité des cas de recherche active peuvent être effectués chaque année. En outre, cette organisation soutient le SCOCI dans le cadre de différents autres projets liés à la lutte contre la pédocriminalité.

6.5 Collaboration avec le secteur privé (partenariat public-privé)

La volonté du SCOCI d'intensifier sa collaboration avec les entreprises privées actives dans le domaine d'Internet s'est traduite par de nombreuses visites et mesures concrètes de collaboration. Des contacts ont été instaurés avec plusieurs fournisseurs de services Internet. Cette collaboration est en particulier nécessaire car elle permet d'obtenir plus facilement des informations sur la connexion Internet des utilisateurs (notamment adresses IP) dans le cadre d'enquêtes ou d'enquêtes préliminaires. En outre, étant donné l'augmentation de la criminalité économique sur Internet, des pourparlers ont été entamés en 2012 avec des représentants de sites de vente en ligne.

3 Organisation non gouvernementale (ONG)

6.6 Coopération internationale

Depuis 2011, le SCOCI est membre du projet Cyborg d'Europol, dont le but est la lutte contre la cybercriminalité à l'échelle supranationale, tels que les attaques de hameçonnage, les réseaux de zombies ou encore le piratage de bases de données à grande échelle. Il participe également depuis 2012 au projet Twins, consacré à la lutte contre la pédocriminalité. Ces deux projets, classés thèmes majeurs par Europol, relèvent de l'agence *European Cybercrime Center* (EC3), qui a entamé ses activités le 1er janvier 2013.

Sis auprès d'Europol à La Haye, le centre de lutte contre la criminalité sur Internet EC3 fournit un support opérationnel aux Etats de l'UE et leur donne accès à ses données techniques dans le cas d'enquêtes menées conjointement à l'échelle communautaire. Ses collaborateurs se concentrent sur la criminalité organisée en ligne. Le centre cible tout spécialement ses activités sur la lutte contre l'exploitation sexuelle des enfants sur Internet et contre les délits financiers. En outre, les attaques contre les infrastructures critiques et les systèmes d'information font aussi partie de ses domaines d'intervention. Le rôle du centre consiste enfin à établir des analyses et des évaluations permettant de déceler les menaces à temps et de les déjouer.

Par ailleurs, le SCOCI participe également au projet CIRCAMP, qui lutte contre la diffusion de la pornographie enfantine sur Internet et a été lancé par la Task force des chefs de police européens. Comme les années précédentes, il a également été en contact en 2012 avec le groupe de travail *European Financial Coalition (EFC)*. Cofinancée par l'Union européenne, l'EFC rassemble les grands responsables de la poursuite pénale et les principaux acteurs du secteur privé dont l'objectif commun est de lutter contre l'exploitation sexuelle des enfants et des jeunes à des fins commerciales.

Le SCOCI a en outre visité et accueilli plusieurs de ses homologues étrangers. Ces contacts s'inscrivent dans une volonté d'instaurer et d'améliorer des processus de collaboration. A côté de la lutte contre la pédopornographie sur Internet, la cybercriminalité, au sens strict du terme, et la criminalité économique sont des thèmes prioritaires des rencontres internationales. Ces échanges directs avec les autorités étrangères de poursuite pénale peuvent notamment aussi être liés à des opérations en cours, dont les investigations secrètes. Là encore, le SCOCI a mis sur pied une coopération étroite et prometteuse avec différentes autorités.

7. Médias, formation et conférences

7.1 Présence médiatique

Au cours de l'exercice 2012, le SCOCI a été présent dans de nombreux médias. Les investigations (préliminaires) secrètes, mais également certaines attaques informatiques spectaculaires (notamment DDoS[4]) et infections par maliciels qui ont touché de nombreux internautes ont fait l'objet d'une couverture médiatique soutenue. L'écho dans la presse a été positif tout au long de l'année.

7.2 Conférences et formation

Au cours de l'année 2012, les collaborateurs du SCOCI ont eu l'occasion de participer à plusieurs cours et conférences. Ces rencontres constituent des occasions privilégiées de s'entretenir et nouer des contacts avec différents partenaires et experts.

[4] *Distributed Denial of Service attack*, attaque par déni de services

8. Interventions parlementaires au niveau fédéral

8.1 Interventions parlementaires déposées en 2012 (sélection)

- Question 12.5264: Sollicitation d'enfants à des fins sexuelles sur Internet - Amherd Viola; Groupe PDC-PEV
- Question 12.5198: Assurer la neutralité du réseau en Suisse également - Glättli Balthasar
- Question 12.5185: DFAE. Trois attaques informatiques en cinq ans - Killer Hans; Groupe de l'Union démocratique du centre
- Question 12.5005: Investigations secrètes. Etat des travaux - Schmid-Federer Barbara; Groupe PDC-PEV
- Postulat 12.4238: Utilisation d'offres illégales sur Internet. Impact sur l'économie - Fluri Kurt; Groupe libéral-radical
- Motion 12.4212: Inscrire la neutralité du réseau dans la loi sur les télécommunications - Glättli Balthasar; Groupe des Verts
- Motion 12.4161: Pour une stratégie nationale contre le cyberharcèlement - Schmid-Federer Barbara; Groupe PDC-PEV
- Interpellation 12.4086: Mesures techniques de surveillance et nouveaux outils de communication - Janiak Claude; Groupe socialiste
- Interpellation 12.3902: La Suisse, paradis du téléchargement illégal - Fluri Kurt; Groupe libéral-radical
- Interpellation 12.3898: Plus de sécurité juridique dans le commerce électronique - Amarelle Cesla; Groupe socialiste
- Motion 12.3834: Protection du droit d'auteur - Freysinger Oskar; Groupe de l'Union démocratique du centre
- Postulat 12.3545: Accès des enfants à Facebook - Amherd Viola; Groupe PDC-PEV
- Motion 12.3476: Harcèlement sexuel des mineurs. Adapter les éléments constitutifs de l'infraction - Schmid-Federer Barbara; Groupe PDC-PEV
- Postulat 12.3326: Vers un droit d'auteur équitable et compatible avec la liberté des internautes - Recordon Luc; Groupe des Verts
- Postulat 12.3289 : Atteintes à la personnalité sur Internet - Malama Peter; Groupe libéral-radical
- Postulat 12.3152 : Droit à l'oubli numérique - Schwaab Jean Christophe; Groupe socialiste

8.2 Evolution législative et politique

La lutte contre la criminalité sur Internet présente également de nouveaux enjeux en terme de jurisprudence et au niveau législatif. Les évolutions les plus marquantes au niveau national et international sont présentées ci-dessous.

Source: Gerd Altmann / Pixerio

a) Convention sur la cybercriminalité

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

La Convention du Conseil de l'Europe sur la cybercriminalité est le premier traité international destiné à combattre la criminalité informatique. Elle oblige les Etats parties à pénaliser la fraude et la falsification informatiques, le vol de données et l'accès indu à un système informatique protégé, mais aussi la pornographie enfantine et la violation des droits d'auteur sur Internet.

Cette convention règle également la façon dont sont recueillies et préservées les preuves électroniques dans les enquêtes pénales. Elle assure notamment que les autorités chargées de l'enquête puissent rapidement avoir accès aux données informatisées, afin que ces dernières ne soient pas falsifiées ou détruites pendant la pro-

cédure. Enfin, elle vise l'instauration d'une coopération étroite, rapide et efficace entre les Etats parties.

La mise en œuvre de la convention a nécessité deux modifications mineures de la législation, l'une concernant le code pénal, l'autre la loi sur l'entraide pénale internationale.

- La punissabilité de l'infraction constituée par l'accès indu à un système informatique (art. 143bis CP) est déplacée en amont: désormais sera punissable toute personne qui mettra en circulation ou rendra accessible un mot de passe, un programme ou toute autre donnée dont elle sait ou doit présumer qu'ils pourront être utilisés pour s'introduire de manière illicite dans un système informatique protégé.

- La loi sur l'entraide pénale internationale accordera aux autorités suisses en charge de ce domaine la compétence de transmettre, dans certains cas, à des fins d'enquête, des données relatives au trafic informatique, à l'autorité requérante avant la clôture de la procédure d'entraide (cf. art. 18*b* EIMP). Ces données (expéditeur et destinataire, date, durée, taille et parcours des données) ne pourront toutefois être utilisées comme preuves qu'une fois entrée en force la décision finale relative à la procédure d'entraide.

- Il a été décidé en outre que le point de contact 24/7 prévu par l'art. 35 de la convention serait assuré par la Centrale d'engagement de fedpol (SPOC, CE fedpol). Le SCOCI soutient la centrale d'engagement dans le traitement des demandes selon la convention.

b) Stratégie nationale de protection de la Suisse contre les cyberrisques

Le 27 juin 2012, le Conseil fédéral a approuvé la Stratégie nationale de protection de la Suisse contre les cyberrisques[5]. A travers cette stratégie, le Conseil fédéral, en coopération avec les autorités, les milieux économiques et les exploitants d'infrastructures critiques, compte réduire les cyberrisques auxquels tous ces acteurs sont exposés quotidiennement.

La stratégie souligne le fait que les risques informatiques sont en premier lieu liés aux tâches et responsabilités. Par conséquent, ces risques devront être traités dans le cadre des processus existants de gestion des risques. Il faut en priorité que les responsables soient mieux informés sur les cyberrisques et apprennent à mieux les percevoir.

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

---

[5] http://www.admin.ch/ch/f/ff/2013/517.pdf

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

9. Glossaire

Adult check	Procédé de vérification permettant de limiter l'accès d'un site *web* à un public majeur uniquement.
Chat	Dialogue en ligne.
Cloud computing	L'informatique en nuage permet d'accéder à la mémoire et aux capacités de calcul d'ordinateurs et de serveurs répartis dans le monde entier et liés par un réseau, tel Internet. Les applications et les données ne se trouvent plus sur l'ordinateur local, mais – par métaphore – dans un nuage (cloud), composé d'un certain nombre de serveurs distants, interconnectés au moyen d'une excellente bande passante, indispensable à la fluidité du système.
Cyberintimidation	Cyberintimidation, cyberharcèlement (de l'anglais *cyberbullying*, de *to bully*: intimider, brimer, harceler) lorsque des textes, des images ou des films diffamatoires sont publiés par le biais de moyens de communication modernes comme les téléphones portables, les *chats*, les sites Internet de réseautage social tels que Netlog ou Facebook, les portails vidéos, les forums ou les blogs, dans le but de dénigrer, de compromettre ou de harceler une personne. Ces attaques sont généralement des actes répétitifs ou commis au cours d'une période relativement longue, et les victimes se caractérisent par une grande vulnérabilité.
One-click-hosting	Les sites *one-click hosting* proposent de l'espace disponible aux utilisateurs pour y stocker des fichiers (principalement vidéo ou audio). Par la suite, un simple URL permet d'accéder à ces fichiers en vue d'un téléchargement.
Peer-to-peer	De l'anglais *peer-to-peer*, abrév. "P2P", pair à pair: modèle de réseau informatique permettant l'échange de fichiers entre utilisateurs (les pairs).
Phishing	Hameçonnage, de l'anglais *phishing* (*p*assword *h*arvesting f*ishing),* la pêche aux mots de passe: méthode permettant d'obtenir frauduleusement les données personnelles d'un utilisateur (mot de passe, nom d'utilisateur, etc.), le plus souvent par le biais de sites *web* falsifiés.
Pornographie dure	Actes d'ordre sexuel impliquant des enfants (pédophilie, pédopornographie), des animaux, des excréments humains, ou comprenant des actes de violence (art. 197, ch. 3, CP).
Proxy	De l'anglais *proxy*, mandataire: serveur informatique dont le rôle est de servir de relai entre un client (vous) et un serveur (le site *web* que vous souhaitez consulter).
Redirect service	Service de redirection: permet de bénéficier d'un URL "simplifié" (notamment un URL plus simple à retenir ou plus court) redirigeant l'utilisateur vers un contenu.
Spam	Communication électronique non sollicitée, principalement effectuée en masse et à des fins publicitaires, ou parfois dans le but d'installer un logiciel malveillant.
Streaming	De l'anglais *stream,* courant, flux: mode de transmission de données audio et vidéo, transmises en flux continu, plutôt qu'après téléchargement complet (permet la lecture de contenu "en direct").
URL	De l'anglais *uniform ressource locator*, localisateur uniforme de ressources: chaîne de caractères combinant les informations nécessaires pour indiquer à un logiciel comment accéder à une ressource Internet.
Valeurs de hash	Valeur unique permettant d'identifier une donnée, notamment une image (empreinte digitale numérique).

10. Tendances et menaces en 2013

Le nombre d'annonces reçues par le SCOCI ne permet pas de tirer de véritables conclusions sur l'évolution effective de la cybercriminalité ou des contenus illégaux sur Internet. On peut tout au plus en déduire des tendances quant à la propension de la population à dénoncer les actes de cybercriminalité et quant à la manière dont ces infractions sont perçues dans notre société.

Chevaux de Troie bancaires: il n'est pas exclu que l'opération "Guerre éclair", qui a été annoncée par des groupuscules russes et semble être dirigée surtout contre des banques américaines, aboutisse aussi à des attaques contre des banques suisses. Ces attaques consistent essentiellement à s'emparer de données d'accès à l'aide de chevaux de Troie. Du fait que la plupart des banques en Suisse possèdent des mécanismes d'authentification à plusieurs niveaux, le risque de dommages financiers directs provoqués par de fausses transactions est certes faible, mais n'est pas à exclure.

Maliciels visant les téléphones mobiles: en 2012, le nombre des variantes de logiciels malveillants infectant surtout les portables androïdes a explosé. Selon certains experts, cette augmentation devrait se poursuivre. Pour les personnes concernées, cela signifie des frais supplémentaires occasionnés, d'une part, par le transfert de volumes de données importants du fait de l'utilisation des appareils infectés pour mettre en place des attaques par déni de service et, d'autre part, par l'envoi indésirable de spams par SMS. Il faut s'attendre en outre à ce que des données personnelles comme les contenus de carnets d'adresses, les mots de passe, etc. soient lus sans autorisation et vendus à d'autres fraudeurs.

Maliciels: il s'agit aussi d'un domaine dans lequel on s'attend à une détérioration de la situation. Le but premier des maliciels demeure l'espionnage de données bancaires, de numéros de cartes de crédit et de mots de passe. Leur but secondaire porte sur les données des carnets d'adresses dans le but de créer des identités factices pour mettre en place des tentatives d'escroquerie et un réseau de zombies pour lancer des attaques par déni de service. Il faut s'attendre en outre à de nouveaux modes de contamination, par ex. les *add-ons* pour les navigateurs ou les applications *web* pour les sites de médias sociaux. Par ailleurs, les lacunes sécuritaires pourraient être exploitées dans les services en nuage afin d'installer des logiciels malveillants sur des ordinateurs-cibles.

Vols de données: plusieurs exemples ont montré que les petits sites *web* ne sont pas à l'abri des attaques. Pour les pirates, les données de clients telles que les adresses demeurent une cible précieuse car elles facilitent grandement l'ingénierie sociale et peuvent être mises en œuvre dans le cadre d'autres escroqueries. En outre, la vente d'adresses électroniques peut s'avérer fort lucrative sur les forums adéquats. Du fait que les cybercriminels se spécialisent dans certaines prestations comme l'obtention et la vente de données, les cibles de petite envergure pourraient à l'avenir être également intéressantes pour ce type d'attaques et être visées.

Escroqueries: du fait de l'expansion d'Internet en Afrique, associée à l'apparition d'une nouvelle classe moyenne, mal rémunérée à l'aune des critères occidentaux dans des pays comme le Nigéria, l'Afrique du Sud ou le Maroc, les experts redoutent que les offres frauduleuses passées sur des sites de petites annonces ou de ventes aux enchères augmentent à nouveau considérablement au cours des prochaines

années. Les estimations tablent sur un doublement du volume des annonces d'ici 2015.

Attaques par déni de services: plusieurs attaques par déni de services ont été lancées en 2012 à des fins de chantage mais aussi politiques. On estime que ce type d'attaques se poursuivra en 2013. Les grandes puissances œuvrent actuellement à la mise en place d'unités de réserve de l'armée et des renseignements pour défendre les infrastructures critiques contre ces attaques et contre les piratages. Cela montre que les attaques par déni de services de grande envergure sont perçues come un scénario de menace à prendre au sérieux.

Pour tous les types d'infractions commises sur Internet, la réponse ne peut être qu'une réponse concertée. Elle se doit d'impliquer l'ensemble des acteurs: gouvernements et autorités de poursuite pénale des différents pays impliqués, fournisseurs d'accès à Internet et autres fournisseurs de services Internet, autorités de surveillance. Différents groupes de travail auxquels participe le SCOCI, au niveau suisse et international, visent à poursuivre ce but. Dans cette optique, la collaboration entre organismes privés et publics (partenariat public-privé) jouera à l'avenir un rôle de plus en plus décisif dans la lutte contre la criminalité sur Internet.