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 2011

Service de coordination de la lutte contre la criminalité sur Internet (SCOCI)
Nussbaumstrasse 29
3003 Berne

www.scoci.ch
www.cybercrime.ch

Date de publication: 03.04.2012

Table des matières

1. L'essentiel en bref

- Le SCOCI a reçu en 2011 5'330 annonces par le biais de son formulaire en ligne. Cela représente une diminution de 14% par rapport à l'année précédente.

- Les annonces pour des cas de pornographie dure (principalement de la pornographie enfantine) sont en recul par rapport à l'année précédente mais restent la catégorie la plus fréquemment annoncée au SCOCI.

- La recherche active a permis d'identifier 214 utilisateurs échangeant de la *pédopornographie* sur les réseaux *peer-to-peer*, et de les dénoncer aux autorités compétentes. Ces consommateurs de pornographie enfantine soutiennent la production de tels contenus et sont donc eux-mêmes indirectement complices des abus commis sur des mineurs.

- Les annonces pour des cas de criminalité économique sont en nette augmentation cette année encore.

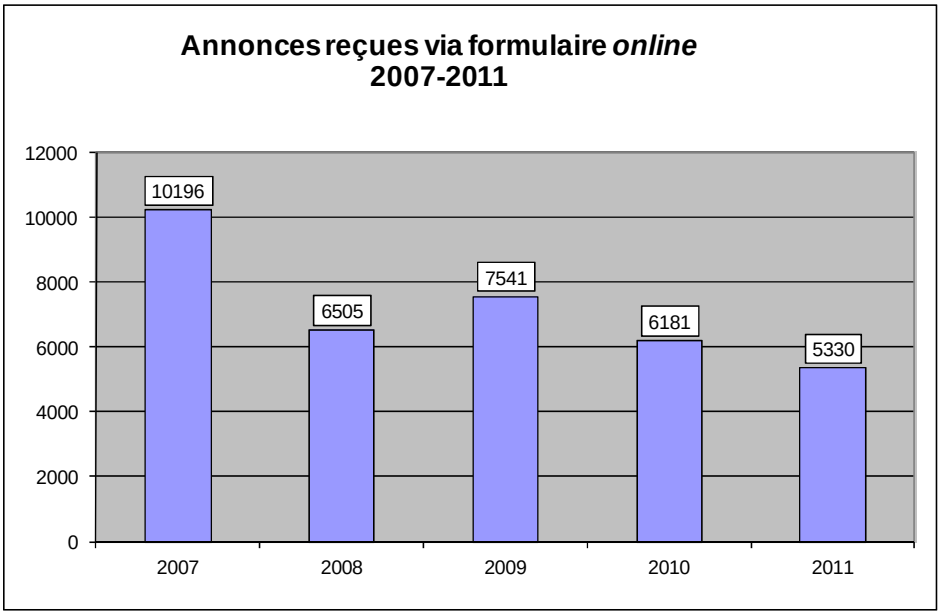
- Des avancées majeures ont eu lieu dans le projet de collection nationale de fichiers et de valeurs *hash* (CNFVH). Les représentants des cantons ont été formés et les premiers lots d'images livrés au SCOCI.

- Le SCOCI appartient depuis mai 2011 à l'équipe de projet de la stratégie nationale de *cyberdéfense* et représentera les intérêts des autorités de poursuite cantonales et fédérales lors de la mise en œuvre de la stratégie.

- La coopération avec Interpol et Europol a été intensifiée, afin de lutter contre la criminalité sur Internet au niveau international.

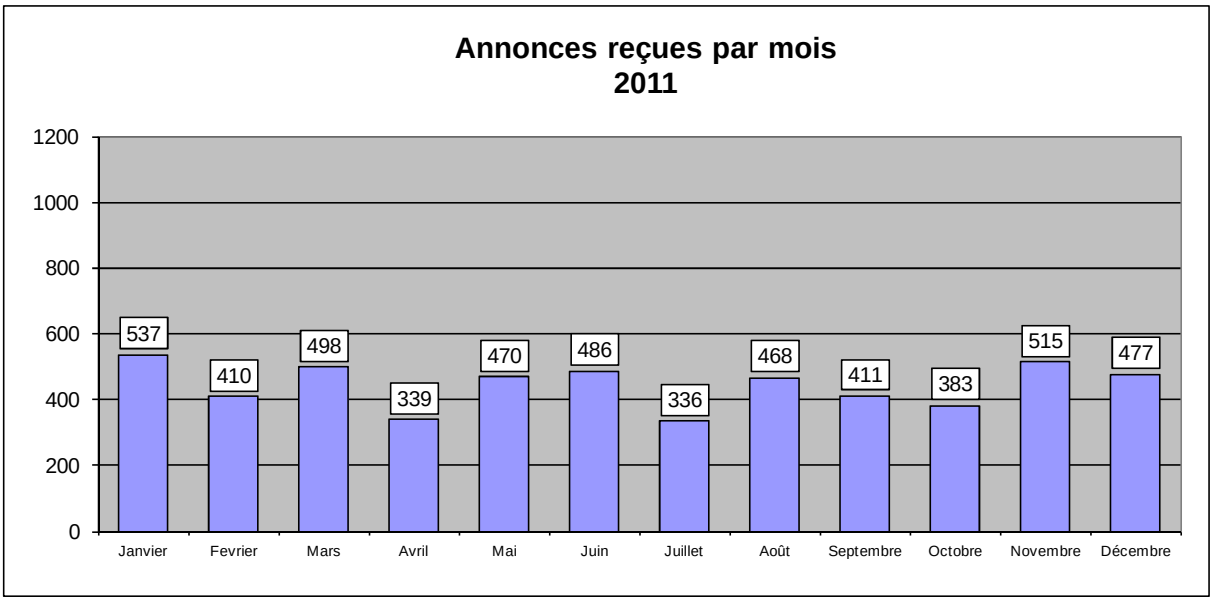
2. Nombre de communications reçues

Le SCOCI a reçu en 2011 5'330 annonces par le biais de son formulaire en ligne. Il s'agit d'un recul de 14% par rapport à l'année précédente. Jusqu'ici, et à l'exception de l'année record de 2007, le niveau d'annonces annuel s'était toujours situé entre 6'000 et 7'500. Il convient de rappeler ici que ces évolutions donnent des indications sur les comportements du public, mais que l'on ne peut pas en tirer de conclusions fiables quant à une évolution des contenus illégaux disponibles sur Internet. En clair, ces chiffres attestent uniquement d'une moindre tendance à dénoncer des actes et contenus potentiellement illégaux à l'aide du formulaire *online* du SCOCI. Il est toujours difficile d'avancer des explications valides face à ce type de phénomènes pouvant théoriquement avoir plusieurs causes. Il se peut que la criminalité sur Internet, devenant plus connue, en vienne à être banalisée, en particulier à travers ses expressions les moins graves (*spam* par exemple). En revanche, ce phénomène engendre une tendance qui s'exprime par des annonces qualitativement plus riches, et donc source de plus d'informations. Enfin, il faut encore préciser ici que l'année n'a pas vu un flot d'annonces d'un même type, qui a souvent contribué, par le passé, à gonfler les statistiques sur un court laps de temps.



Graphique 1 : annonces reçues via www.scoci.ch (comparaison sur 5 ans)

L’analyse par mois (graphique 2) permet de voir que le niveau d’annonces est relativement stable au cours de l’année. Ceci confirme l’absence d’un flot, qui aurait pu peser de manière significative sur le total de l’année.



Graphique 2 : annonces reçues via www.scoci.ch, par mois (Total 5330 annonces)

3. Types d'infractions enregistrées

En ce qui concerne l'évolution des catégories d'annonces, le premier résultat marquant est une baisse de celles concernant la **pornographie dure,** par rapport à 2010 (cf. graphique 3). Rappelons ici que cette catégorie regroupe les différents types de pornographie illégale, mais que dans les faits, il s'agit majoritairement (dans 90% des cas) de pornographie enfantine. Cette baisse s'inscrit dans le contexte d'une diminution globale du nombre d'annonces (cf. chapitre 1). Il convient cependant d'interpréter cette tendance avec prudence. En effet, rien dans ce qu'observe le SCOCI au quotidien, ni dans les échanges qu'il entretient avec ses partenaires suisses et étrangers, ne permet de faire l'hypothèse d'une diminution de ce type de contenus illégaux sur Internet. Par ailleurs, il convient de rappeler que la pornographie dure reste le motif d'annonce le plus fréquent. Une piste explicative à ce recul, consiste en une évolution vers une moindre visibilité de ce type de contenus. De plus en plus, en effet, les pédophiles se tournent vers des plateformes fermées (forums, groupes, réseaux sociaux) leur permettant d'échanger du contenu de manière plus discrète et anonyme. Dans ce domaine, on note également le grand succès des outils rendant possible l'anonymat (*proxy* notamment), ainsi que des raccourcisseurs d'URL. Ces derniers permettent de masquer la véritable cible d'un URL (et donc d'en éliminer la connotation « pédopornographique »), mais également de modifier la cible tout en gardant le même nom. L'ensemble de ces outils permettent ainsi un échange plus efficace et un anonymat plus grand.

Les annonces pour des cas de **pornographie « légale »** sont en légère reprise après la forte baisse observée l'année dernière. Quant aux annonces pour ***spams***, elles connaissent une quatrième année de baisse consécutive. Ce résultat permet clairement de démontrer que l'évolution du nombre d'annonces faites au SCOCI n'est pas nécessairement représentative de l'évolution du phénomène en lui-même. En effet, même si certaines études attestent d'une baisse du volume de *spams* au niveau mondial en 2011, une baisse constante depuis 2008, telle qu'observée ici, n'est corroborée par aucune donnée chiffrée[1]. Une piste à suivre, face à cette baisse dans le niveau d'annonce, est celle d'une banalisation du *spam* chez les internautes, qui ne jugent plus nécessaire d'annoncer ce type de contenus. Par ailleurs, l'efficacité accrue des filtres contre les courriers indésirables a également comme conséquence, que bon nombre de *spams* ne sont plus vus par l'utilisateur, mais automatiquement mis en quarantaine, puis détruits.

En ce qui concerne la **criminalité économique**[2], la hausse des annonces pour **escroquerie** se poursuit (+53%). Nous sommes ici clairement en présence d'une tendance accentuée. Les internautes qui effectuent des achats en ligne sont tout particulièrement ciblés par des escrocs opérant depuis l'étranger sur les sites d'enchères en ligne et de petites annonces (voitures, appartements, électronique). Sur ces mêmes sites, les vendeurs sont également visés par des escroqueries, où de fausses

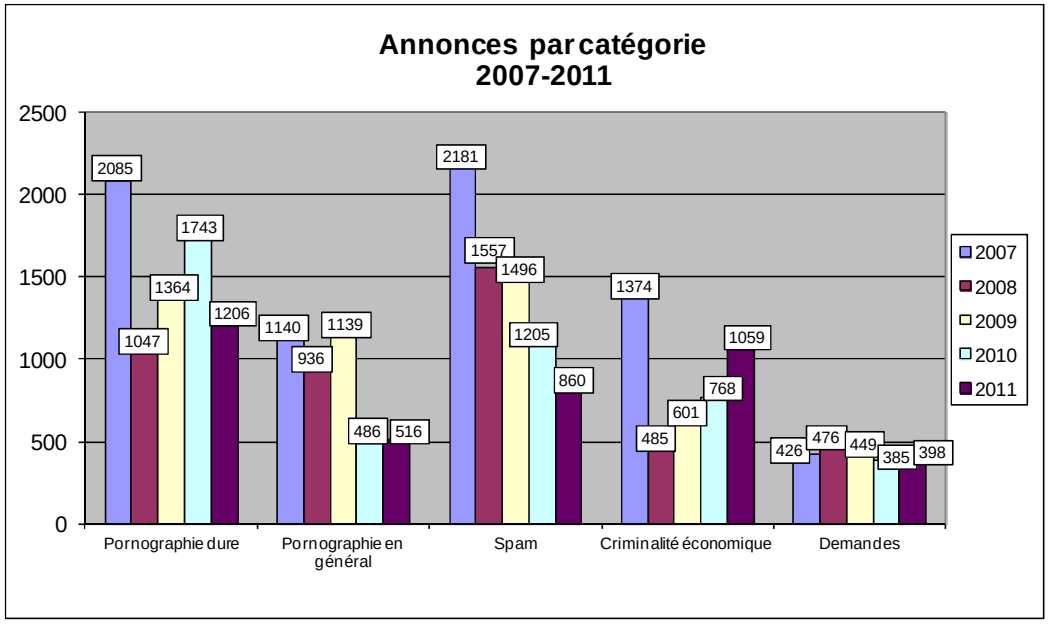
[1] Cf. par exemple McAfee Threats Reports ;
http://www.mcafee.com/apps/view-all/publications.aspx?pg=1&sz=10&tf=mcafee_labs

[2] La catégorie « criminalité économique » regroupe la catégorie « escroquerie » et les autres cas de criminalité économique (phishing et blanchiment d'argent avant tout). Ces deux catégories étaient auparavant présentées séparément dans les statistiques du SCOCI.

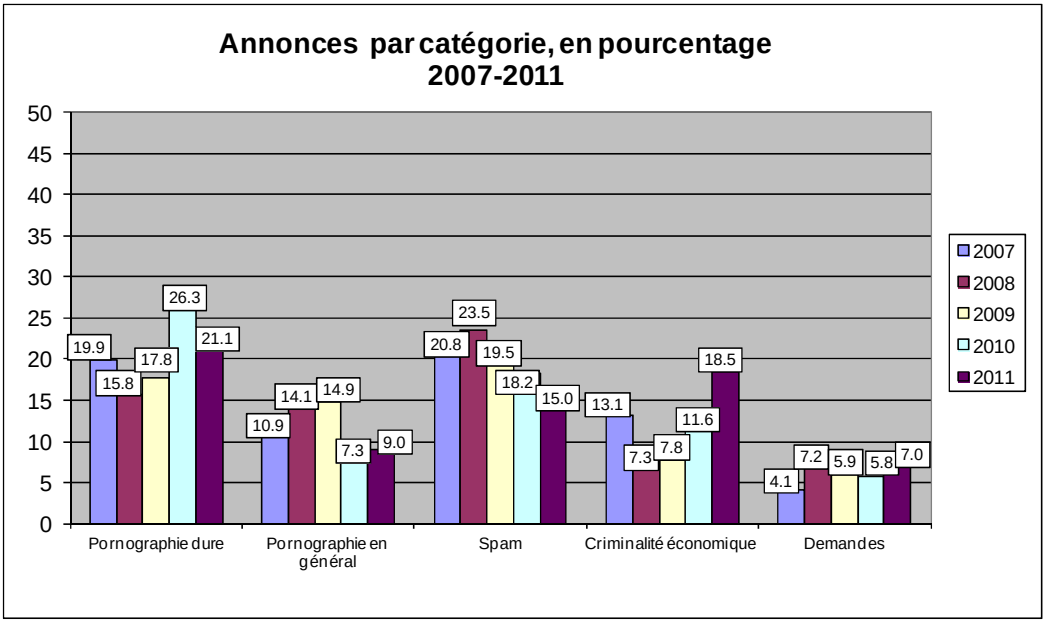
preuves de paiement leur sont délivrées, ou alors des frais réclamés. Les fraudes à la commission, pour lesquelles des frais sont demandés préalablement au versement de soi-disant gros gains (par exemple de loterie), sont toujours actuelles, et leur scénario évolue sans cesse. Par ailleurs, dans ces différents *modus operandi*, les escrocs cherchent dans un premier temps, en plus de l'argent, à obtenir des informations personnelles (copies de pièces d'identité, coordonnées bancaires, etc.) de la part des victimes. Les internautes fournissant ce type de données s'exposent par la suite à des risques d'usurpation de leur identité.

Les annonces pour des **autres cas de criminalité économique** connaissent une évolution similaire aux cas d'escroquerie, avec une hausse marquée (+28%). Les attaques de *phishing* se sont notamment multipliées au cours de l'année, ciblant tout particulièrement les services bancaires, mais également les comptes sur des sites d'enchères en ligne.

Enfin, le nombre de **demandes** adressées au SCOCI se maintient à un niveau proche de ce qui a été observé au cours des dernières années. Le SCOCI reste ainsi un centre de compétence légitime et largement utilisé par les internautes et les fournisseurs de service Internet à la recherche de soutien ou d'informations.



Graphique 3 : évolution des catégories d'annonce principales, sur 5 ans

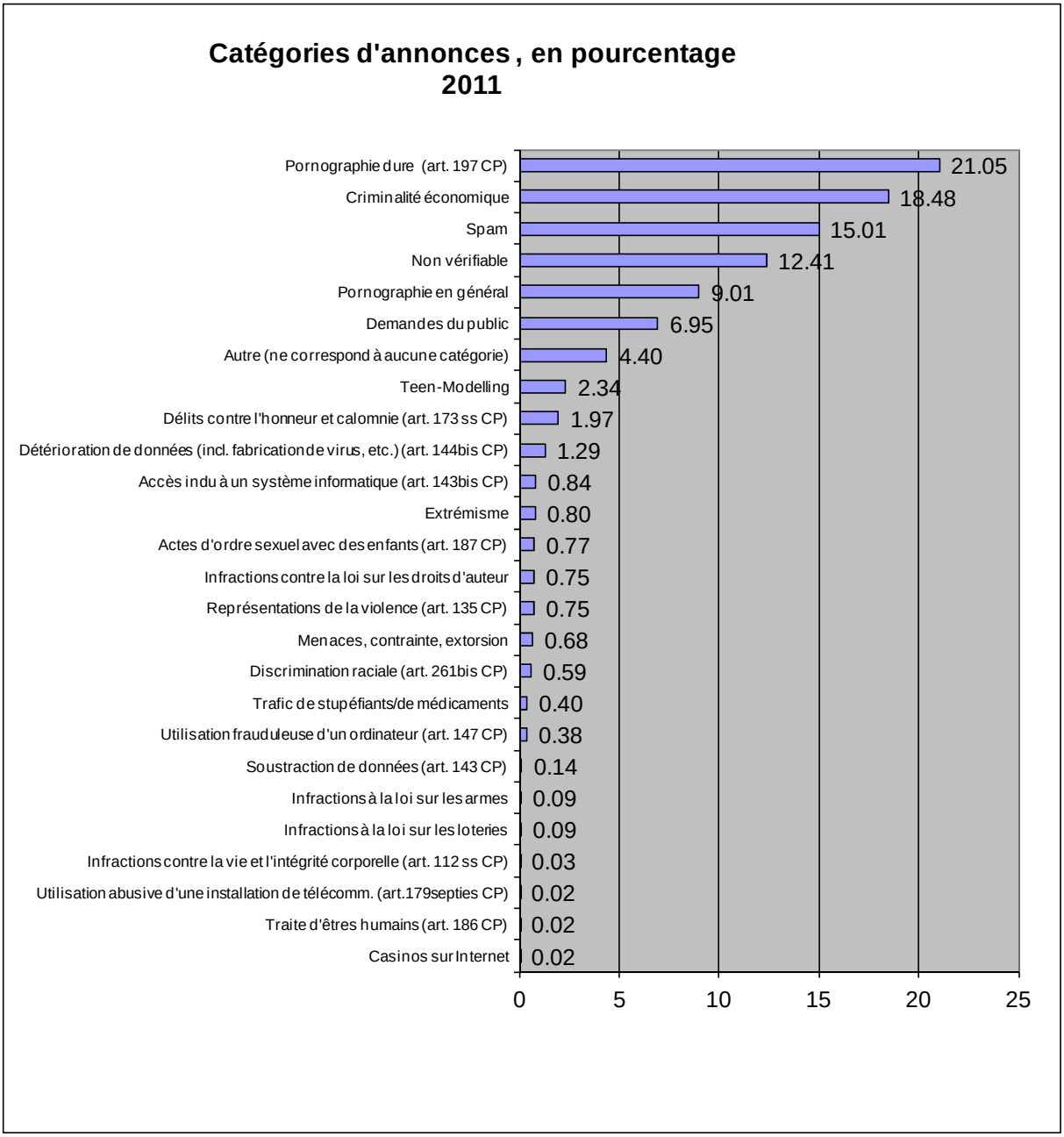


Graphique 4 : évolution des catégories d'annonce principales (en pourcentage), sur 5 ans

Le graphique 5 offre une vue d'ensemble des types d'annonces faites au SCOCI. En plus des catégories principales traitées plus haut, le SCOCI reçoit des annonces d'une grande variété. Les annonces concernant les **délits contre l'honneur et calomnies**, de même que les **menaces, contraintes et extorsions** connaissent une forte hausse par rapport à l'année dernière, respectivement de 0,70% à 1,97% et de 0,42% à 0,68%. Les réseaux sociaux sont tout particulièrement utilisés dans le cadre de ce type de délits. Parmi ces catégories, 30 cas (dont au moins 5 concernant des mineurs) peuvent par ailleurs être considérés comme relevant du ***cyberbullying*****,** tel qu'il est défini dans le cadre du rapport du Conseil fédéral publié en 2010[3].

En ce qui concerne la *cybercriminalité* au sens strict du terme, on note également des hausses par rapport à 2010 dans les catégories **« détérioration de données »** (de 0,57% à 1,29%) et **« accès indu à un système de données »** (de 0,44% à 0,84%). Des attaques ayant ciblé des utilisateurs suisses ont notamment été signalées au SCOCI. On pense ici par exemple à un *malware* ayant infecté de nombreux utilisateurs suisses, bloquant leur ordinateur pour ensuite tenter de leur soutirer de l'argent (cf. chapitre 5). Il conviendra de suivre ces évolutions au plus près, durant les prochaines années.

[3] On parle de cyberintimidation lorsque des textes, des images ou des films diffamatoires sont publiés par le biais de moyens de communication modernes dans le but de dénigrer, de compromettre ou de harceler une personne.

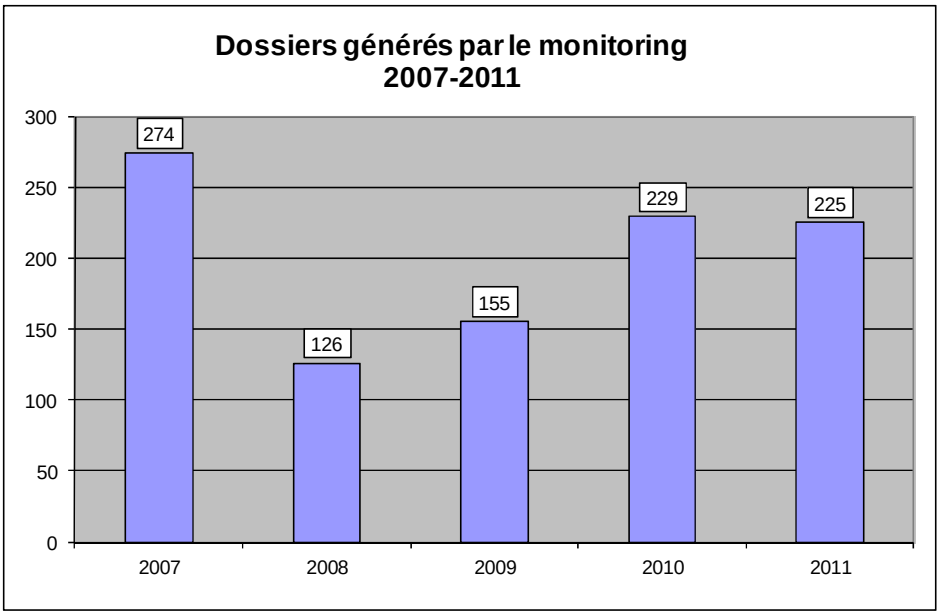


Graphique 5 : annonces 2011, en pourcentage du total des annonces

4. 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, le SCOCI est présent sur des terrains moins faciles d'accès. 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 2011 l'axe principal d'intervention. Cependant, le comité directeur a également clairement affirmé que le SCOCI ne devait pas pour autant se détourner complètement de la criminalité économique et de la *cyber-criminalité* au sens strict du terme.

Les dossiers générés par la recherche active du SCOCI (225) se situent à un niveau similaire à celui de 2010, ce qui confirme la reprise qui avait alors été constatée.



Graphique 6: dossiers créés à la suite de recherches actives du SCOCI

4.1 Recherche active sur les réseaux *peer-to-peer*

La grande majorité des dossiers (214 sur 225) sont issus du monitoring des réseaux *peer-to-peer* ciblant les utilisateurs échangeant de la *pédopornographie*. Les réseaux *peer-to-peer* restent un des moyens privilégiés utilisés pour échanger des contenus sur Internet.

Il convient de noter que deux dossiers parmi ces 214 ont été envoyés à des autorités de poursuite à l'étranger, puisqu'ils concernaient un ressortissant de leur pays.

4.2 Enquêtes sous couverture sur les *chats* et réseaux sociaux

Le nouveau code de procédure pénale (CPP) est entré en vigueur le 1er janvier 2011. Depuis cette date, les autorités fédérales ne sont plus autorisées à mener des enquêtes sous couverture à titre préventif. Cette compétence est celle des cantons, et il leur appartient de réglementer ce type d'intervention à travers leurs lois sur la

police cantonale. Puisque peu de cantons bénéficiaient d'une telle règlementation au premier janvier 2011, la crainte d'un vide juridique s'est alors fait sentir.

Afin d'éviter une telle situation, l'Office fédéral de la police (fedpol) a cherché une solution avec le canton de Schwytz. Cette démarche a abouti à la signature d'un accord de durée indéterminée le 23.12.2010. Celui-ci porte sur la collaboration entre fedpol, le SCOCI et le Département de la sécurité du canton de Schwytz, lors d'enquêtes préliminaires sur Internet, visant à lutter contre la *pédocriminalité* (recherche active sur les sites de dialogue en direct)[4]. Conformément audit accord, les collaborateurs du SCOCI mènent des enquêtes sous couverture exclusivement sous mandat et contrôle de la police cantonale schwytzoise. Il garantit que la lutte contre la *pédocriminalité* sur Internet puisse continuer à se faire sous la forme d'enquêtes sous couverture à des fins préventives. En date du 14 janvier 2011, le tribunal des mesures de contrainte du canton de Schwytz a autorisé la nomination de 6 collaborateurs du SCOCI en tant qu'enquêteurs sous couverture. Le 11 janvier 2012, le tribunal a prolongé la nomination de ces 6 personnes jusqu'au 14 juillet 2012, et a également autorisé la nomination de 2 collaborateurs supplémentaires.

En relation avec la nomination de collaborateurs du SCOCI comme enquêteurs sous couverture en janvier 2011, le service en question a entrepris divers travaux techniques et opérationnels. L'acquisition des connaissances de base dans ce domaine, de même que la définition des procédures de travail avec fedpol et les cantons, ont nécessité un certain laps de temps.

Au cours de l'année 2011, 16 cas ont été traités selon l'ordonnance schwytzoise. Les mesures et résultats suivants ont découlé du traitement de ces cas :

- dans 5 cas, des perquisitions ont été effectuées et les suspects interrogés
- dans un cas, un suspect a été interrogé
- 4 cas sont en cours d'évaluation auprès des procureurs cantonaux compétents
- dans un cas, le ministère public a décidé de ne pas entrer en matière
- 4 cas n'ont pu être poursuivis, en raison de l'impossibilité d'identifier l'auteur, ou d'une concrétisation insuffisante du soupçon initial
- un cas est en traitement au SCOCI et des investigations supplémentaires sont en cours

L'évaluation du matériel saisi lors des perquisitions n'était pas encore terminée à fin 2011, et aucune décision d'un tribunal en relation avec ces cas n'est pour l'instant tombée.

[4] Engagement au sens de l'article 9d de l'ordonnance sur la police du canton de Schwytz du 22.03.2000 (PolV – SRSZ 520.110).

5. Quelques cas intéressants

Différents cas particulièrement révélateurs ou ayant abouti à des résultats probants ont occupé le SCOCI au cours de l'année. La présentation de ces derniers permet de compléter l'analyse purement statistique en y apportant un éclairage plus qualitatif.

Un premier cas concerne une personne ayant été identifiée à l'aide du monitoring des réseaux *peer-to-peer*, pour avoir téléchargé et mis à disposition d'autres utilisateurs des images et vidéos à caractère pédopornographique. Suite à la perquisition menée par la police cantonale, le suspect a reconnu avoir également abusé plusieurs fois de jeunes enfants. Il s'agissait d'un éducateur de la petite enfance encore inconnu des services de police et travaillant comme animateur dans une crèche. La plus jeune de ses victimes était âgée de 3 ans. Ainsi, dans ce cas précis, la surveillance des réseaux *peer-to-peer* a permis d'identifier un *pédocriminel* et d'éviter de nouveaux abus commis sur des enfants.

Dans le cadre d'une enquête sous couverture, un service de police étranger a transmis des informations au SCOCI, laissant à penser qu'un ressortissant suisse prévoyait de se rendre en Grande-Bretagne pour y rencontrer un mineur, avec un risque que des abus sexuels soient alors commis. Le travail du SCOCI a permis d'établir que le suspect était déjà connu pour des délits sexuels à répétition perpétrés sur des mineurs, et avait déjà été condamné pour des actes similaires. Grâce à une collaboration étroite entre les services des deux autres pays concernés, ainsi que le fournisseur de service Internet, la personne a pu être identifiée et arrêtée à son arrivée en Grande-Bretagne. Le contenu de sa valise laissait à penser que la personne avait bien l'intention de commettre un abus sexuel sur sa victime mineure. En plus d'une réservation d'hôtel à son nom et à celui du mineur, une caméra et une grande quantité de bande magnétique ont été saisies. Cet exemple démontre l'importance de la collaboration entre les forces de police de différents pays et l'industrie d'Internet, à travers un interlocuteur national unique. Il faut par ailleurs souligner que l'arrestation du suspect, avant que l'acte ne soit consommé, n'a été possible que grâce à l'engagement sous couverture des forces de police étrangères.

Dans un autre cas, le SCOCI a eu connaissance à travers son formulaire d'annonce, d'un forum sur lequel un utilisateur affirmait vouloir offrir sa fille de 13 ans, aux fins d'exploitation sexuelle. Le travail du SCOCI a dans un premier temps permis d'identifier le suspect. Après l'interrogatoire de ce dernier par la police cantonale compétente, il s'avéra qu'il n'avait pas de fille, et qu'il exprimait uniquement un fantasme sans lien avec la réalité. En revanche, il fut particulièrement utile de s'intéresser aux internautes ayant répondu à l'offre. A ce stade, deux collaborateurs du SCOCI furent engagés sous couverture, selon le code de procédure pénale suisse, pour soutenir les autorités cantonales dans le travail d'identification des abuseurs potentiels. Ce travail a permis d'aboutir à l'arrestation de plusieurs suspects en Suisse, au début de l'année 2012. Les suspects ont été appréhendés par la police cantonale à l'occasion de faux rendez-vous au cours desquels ils pensaient rencontrer la mineure de 13 ans.

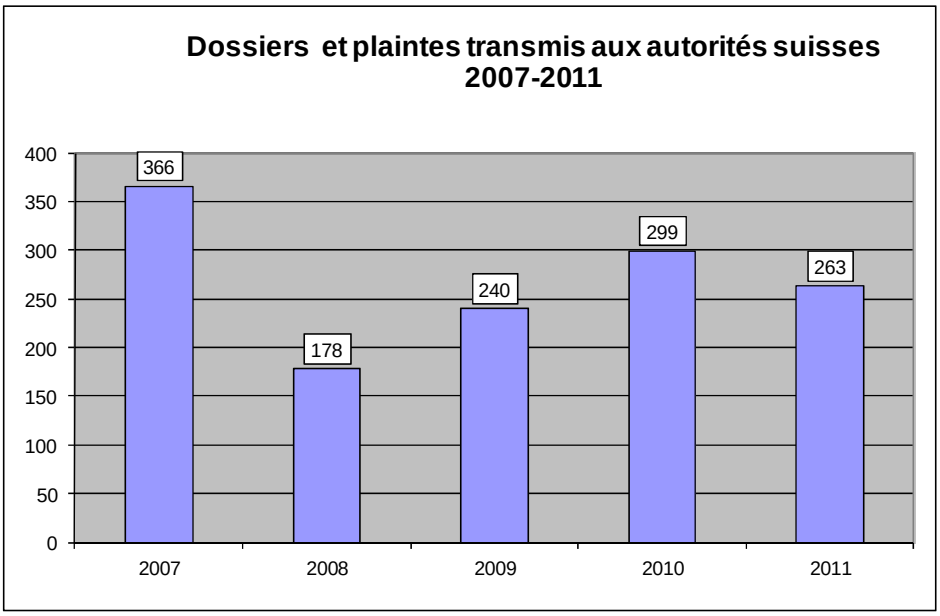
Dans le domaine de la *cybercriminalité* au sens strict du terme, de nombreux cas ont rythmé l'activité du service en cours d'année. En novembre, un *malware* particulièrement agressif a infecté les machines de nombreux utilisateurs suisses à travers des sites de vidéos en *streaming*. L'utilisateur voyait son ordinateur bloqué, et rece-

vait un message provenant soi-disant des autorités fédérales l'accusant de pratiques illégales - allant de la distribution de pornographie enfantine à l'envoi de courriels à des fins terroristes - ayant justifié le blocage de l'ordinateur. Seul le paiement d'une somme d'argent devait permettre de débloquer la machine. De telles activités délictueuses sont régulièrement entreprises, avec des variations relatives aux sites utilisés et aux victimes potentielles visées.

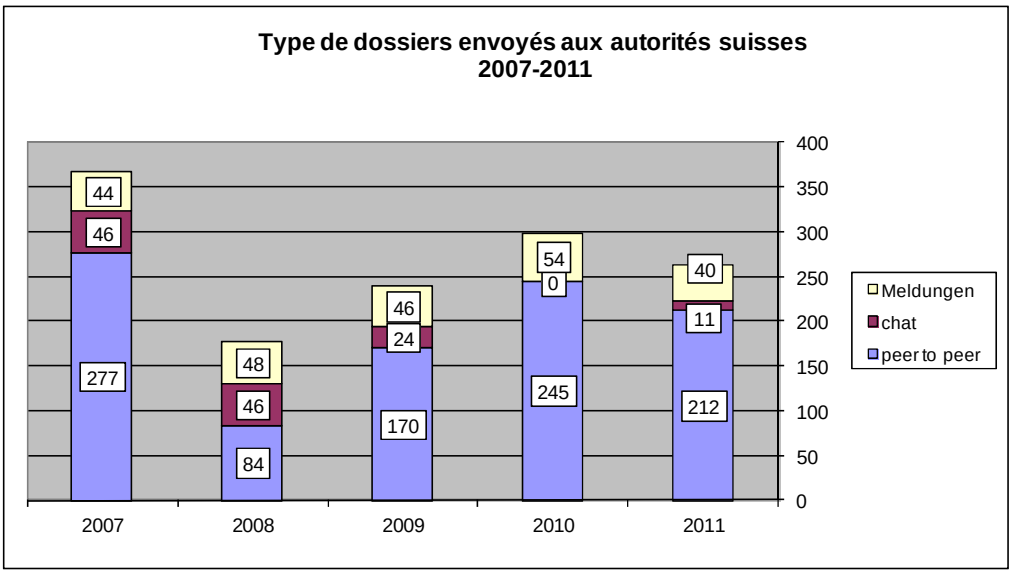
Enfin, un cas particulièrement intéressant est celui d'un utilisateur ayant fait mention sur plusieurs forums de sa volonté de transmettre le VIH, étant lui-même malade du SIDA. Ce type de comportement tombait sous le coup de la loi, selon le SCOCI, mais aucun canton ne s'estimait compétent. Suite au travail de monitoring approfondi du-service, suffisamment d'éléments ont été réunis, afin d'établir la compétence au niveau cantonal. La personne concernée a donc été dénoncée auprès des autorités cantonales.

6. Dossiers transmis aux autorités

Le nombre de dossiers envoyés par le SCOCI aux autorités suisses de poursuite pénale est en légère baisse par rapport à l'année dernière mais se situe tout de même à un niveau supérieur à celui de 2009.



Graphique 7: dossiers transmis aux autorités, en nombres absolus



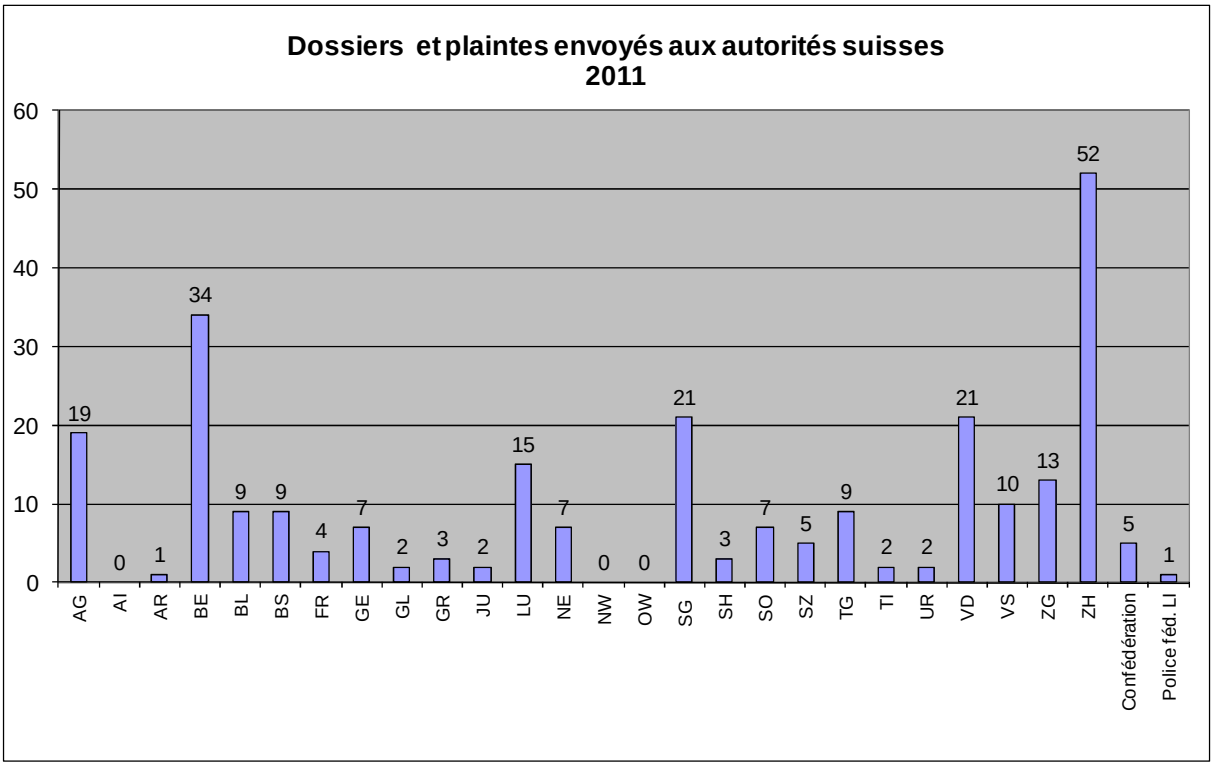
Graphique 8: type de dossiers transmis, en nombres absolus

L'analyse du type de dossiers envoyés (cf. graphique 8) permet de se rendre compte que cette baisse est tout d'abord imputable à une diminution des annonces faites par le public et transmises par la suite aux autorités suisses de poursuite pénale. Ce résultat découle donc directement de la baisse des annonces ayant été constatée (cf. graphique 1). Par ailleurs, le nombre de dossiers issus du monitoring des réseaux *peer-to-peer* et transmis aux cantons (212), présente également une baisse par rapport à l'année dernière. Une analyse plus fine de ce résultat permet de se rendre compte que cette baisse concerne les mois de juillet/août/septembre, durant lesquels

très peu de dossiers ont été envoyés. Durant ces mois, un travail d'amélioration et de modification des processus et méthodes utilisées, afin d'en augmenter l'efficacité, a été mené. Cela a eu comme conséquence de rendre l'outil non opérationnel pendant cette période.

Enfin, 11 cas concernant des actes d'ordre sexuel avec des enfants commis sur des sites de dialogue en direct (chat) ont été transmis aux cantons. Ces derniers sont issus d'enquêtes sous couvertures menées par le SCOCI.

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 ont été les plus concernés. Quelques dossiers ont par ailleurs été transmis en interne, notamment vers d'autres commissariats de la police judiciaire fédérale (notamment « protection de l'Etat », « criminalité générale, organisée et financière » et « *pédocriminalité*-pornographie »).



Graphique 9: nombre de dossiers transmis en Suisse et au Lichtenstein, par destinataire (Total= 263)

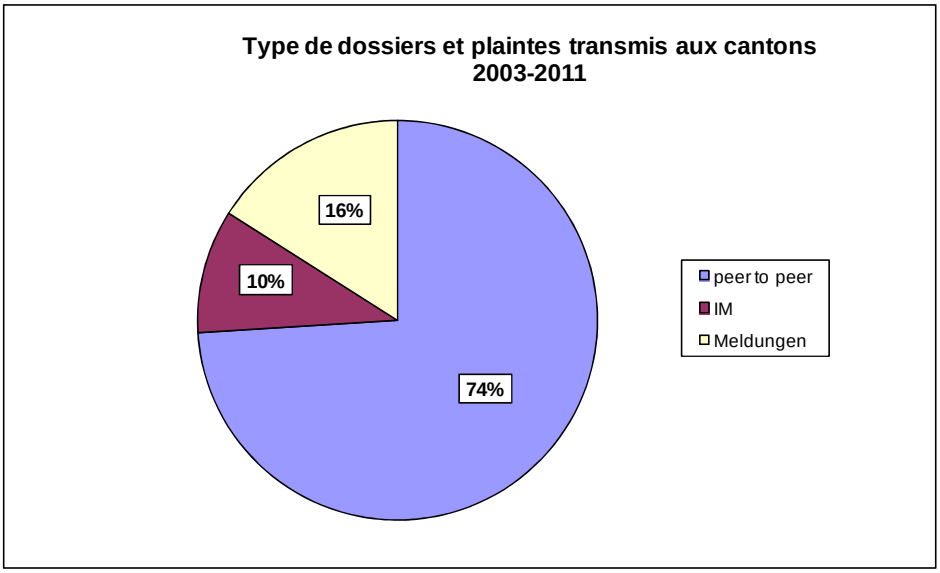
Pour être complet, il convient de préciser que plus de 50 signalements ont été faits vers des services de police à l'étranger, via Interpol et Europol. Il s'agit principalement de sites hébergés dans les pays concernés, et qui présentent un contenu potentiellement illégal (pornographie enfantine ou *cybercriminalité* au sens strict du terme notamment). La plupart du temps, ce type de sites est signalé au SCOCI par le biais de son formulaire d'annonce. En plus de ces signalements effectués par le canal officiel d'Interpol, le SCOCI a par ailleurs souvent été amené, au cours de l'année, à communiquer des contenus potentiellement illégaux à d'autres acteurs. On pense notamment ici aux hébergeurs de sites *web* ou aux sites eux-mêmes.

7. Feedback des cantons

En parallèle à l'envoi de dossiers de suspicion d'infraction et de plaintes aux cantons (cf. graphique 7), le SCOCI demande à ces derniers de lui fournir un feedback sur le suivi du cas au niveau de la police et des autorités judiciaires cantonales, sous forme d'un questionnaire. Les résultats de cette procédure sont présentés dans ce chapitre.

Ces résultats constituent pour le SCOCI un outil important, lui permettant notamment de vérifier l'efficacité de son outil de monitoring des réseaux *peer-to-peer*, et de la solidité des dossiers transmis aux cantons en général.

Comme le graphique 10 en atteste, la grande majorité des dossiers envoyés aux cantons sont issus du monitoring des réseaux *peer-to-peer*, et ciblent donc les utilisateurs qui échangent des contenus *pédopornographiques* illégaux.

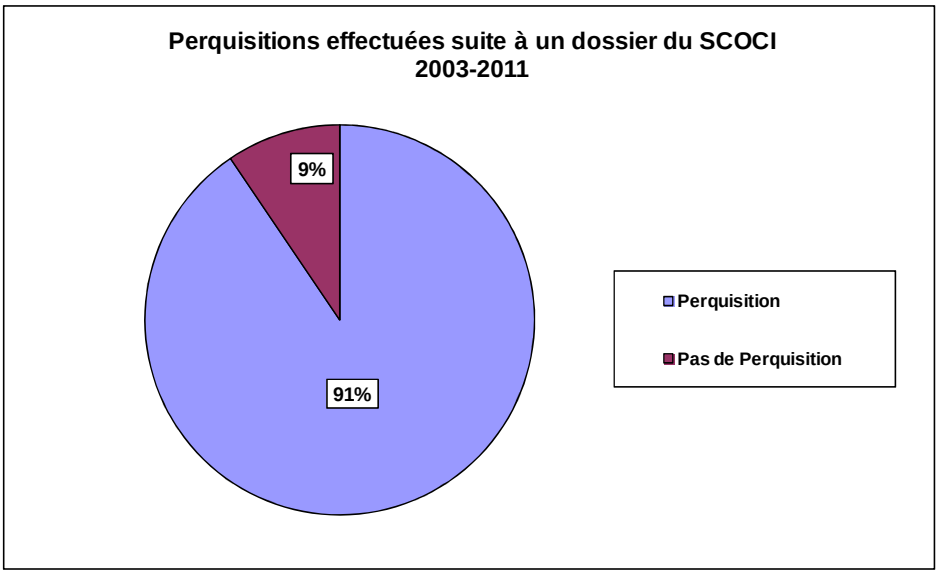


Graphique 10 : type de dossiers transmis aux cantons (depuis 2003, N=2437 dossiers)[5]

[5] IM= Instant Messaging ; un moyen de communication permettant à deux ou plusieurs personnes d'échanger des messages textuels en temps réel (chat).

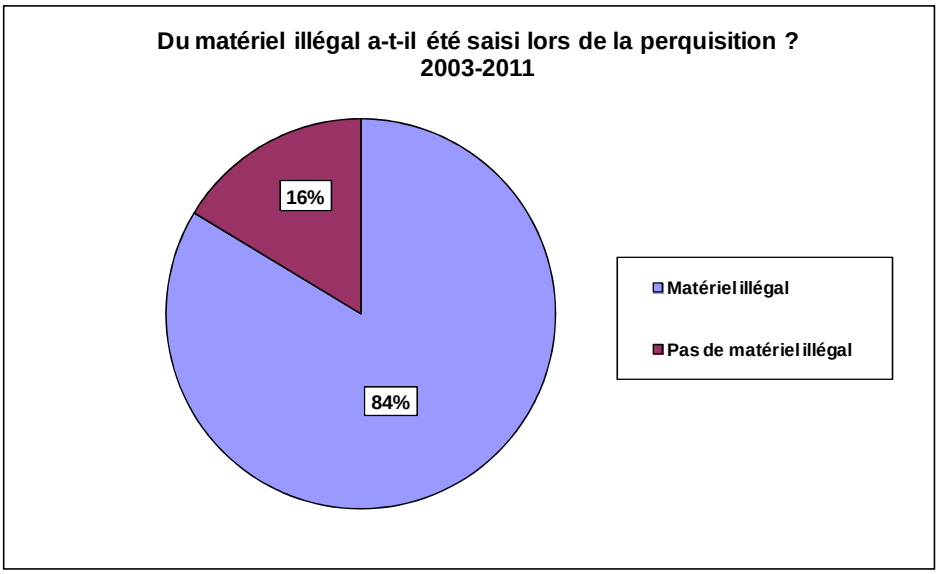
7.1 Feedback des polices cantonales

Sur l'ensemble des dossiers envoyés par le SCOCI, 91% ont été à l'origine d'une perquisition de la police cantonale. Bien entendu, ce pourcentage dépend fortement du type de dossier envoyé, tous les cas ne justifiant pas toujours qu'une perquisition soit menée. Ainsi, les dossiers émanant du monitoring des réseaux *peer-to-peer* et ciblant les consommateurs de *pédopornographie* ont été suivis d'une perquisition dans plus de 98% des cas. Si l'on considère cette relation en sens inverse, on note que 95% des perquisitions effectuées et reportées au SCOCI l'ont à la suite d'un dossier *peer-to-peer*.



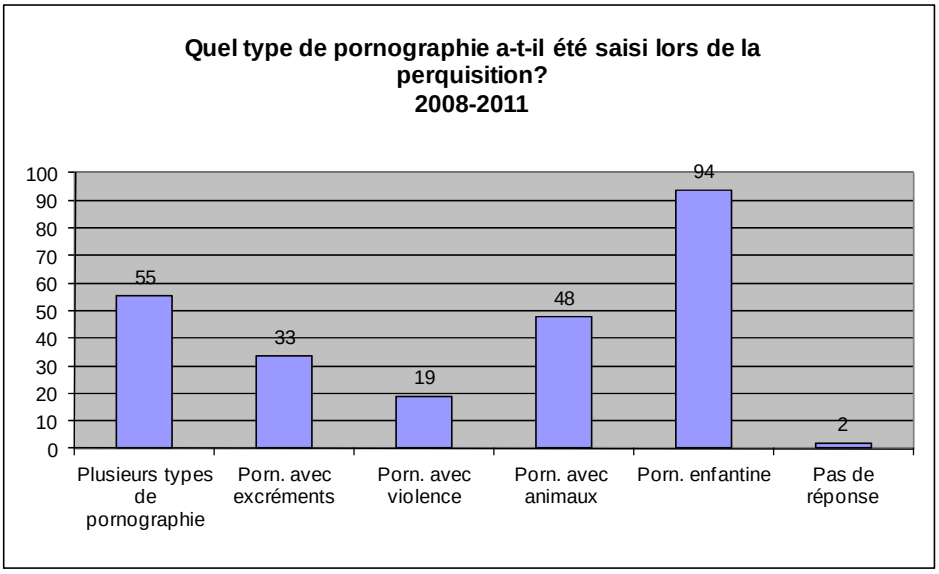
Graphique 11 : perquisitions effectuées (N=791 Feedback)

Dans 84% des cas, les perquisitions effectuées sur la base des dossiers fournis par le SCOCI permettent de saisir du matériel illégal, seules 16% de celles-ci se révélant infructueuses. Il n'est pas toujours possible de savoir avec certitude pourquoi une perquisition ne permet pas de saisir du matériel illégal, les explications possibles étant potentiellement nombreuses. Néanmoins, les situations dans lesquelles le raccordement sans fil identifié par le SCOCI est ouvert et non protégé sont fréquentes (20% des perquisitions infructueuses). Dans ce type de cas, il n'est pas toujours possible d'identifier l'auteur, le raccordement pouvant avoir été utilisé par de nombreuses personnes. Ainsi l'auteur de l'infraction n'est apparemment pas le propriétaire du raccordement. Par ailleurs, les chances de pouvoir saisir du matériel illégal dépendent aussi de la rapidité de l'intervention suite à l'annonce du SCOCI. En effet, plus ce laps de temps est élevé, plus les chances que l'utilisateur ait détruit les contenus illégaux augmentent. La rapidité de la perquisition est ainsi un critère de réussite important.



Graphique 12 : saisie de matériel illégal suite à la perquisition (N=716 perquisitions)

Dans la quasi totalité des perquisitions où du matériel illégal a été trouvé, des fichiers contenant de la pornographie enfantine on été saisis (94%). Ce résultat est logique étant donné que c'est justement ce type de contenu qui est ciblé dans le monitoring des réseaux *peer-to-peer*, qui constitue comme nous l'avons vu plus haut, la grande majorité des dossiers transmis aux cantons. Un aspect intéressant est de noter que dans plus de la moitié des cas, un autre type de pornographie illégale a également été découvert (cf. graphique 13). De même, dans un cas sur deux environ, la personne possédait également de la pornographie illégale avec des animaux.



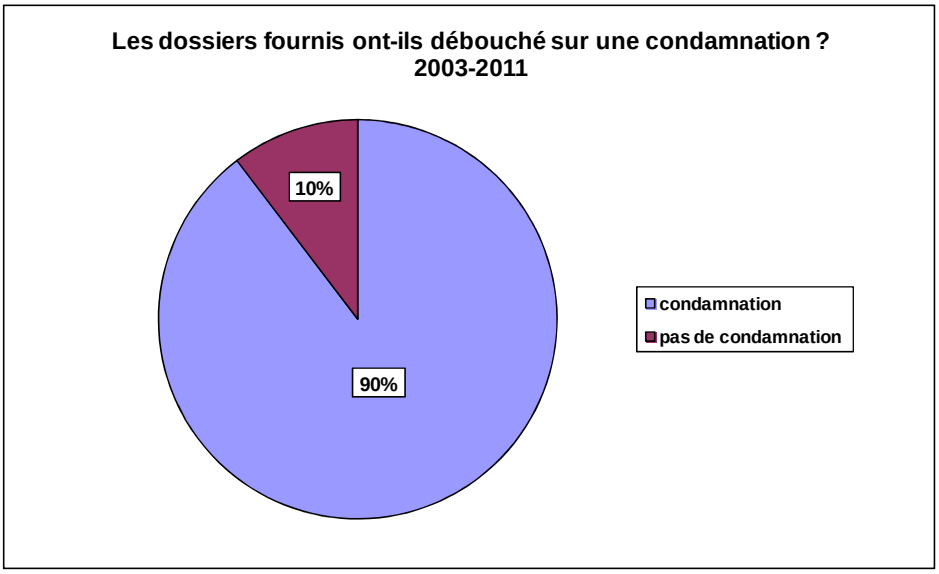
Graphique 13 : type de matériel saisi, en pourcentage (N=251 Feedback)

En ce qui concerne la forme du matériel illégal saisi, il s'agit de films dans 80% des cas et d'images dans 63%. Le total excède 100%, puisque bien souvent, 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 images.

7.2 Feedback des autorités judiciaires

Les feedback reçus des autorités judiciaires des cantons, que ce soit sous la forme de questionnaires ou copies du jugement, nous informent que dans 90% des cas, une condamnation a été prononcée a l'issue de la procédure.



Graphique 14 : condamnations prononcées, en pourcentage (N=589 feedback)

Les condamnations les plus fréquentes concernent logiquement l'article 197 CP (pornographie), et principalement ses chiffres 3 et 3bis [6]. Il s'agit donc de possession de pornographie dure. Les condamnations pour infraction à l'art. 187 ch. 1 CP, donc pour des actes d'ordre sexuels sur des enfants commis sur des sites de dialogue en direct, sont en revanche plus rares.

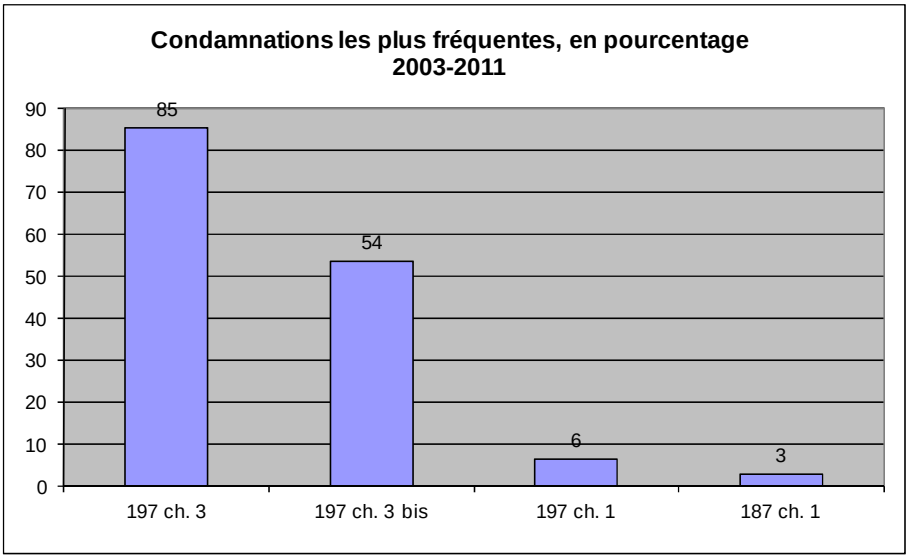
6

Ch. 3. Celui qui aura fabriqué, importé, pris en dépôt, mis en circulation, promu, exposé, offert, montré, rendu accessibles ou mis à la disposition des objets ou représentations visés au ch. 1, ayant comme contenu

des actes d'ordre sexuel avec des enfants, des animaux, des excréments humains ou comprenant des actes de violence, sera puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire. Les objets seront confisqués.

Ch. 3bis. Celui qui aura acquis, obtenu par voie électronique ou d'une autre manière ou possédé des objets ou des représentations visés au ch. 1 qui ont comme contenu des actes d'ordre sexuel avec des enfants ou des animaux ou comprenant des actes de violence, sera puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire.

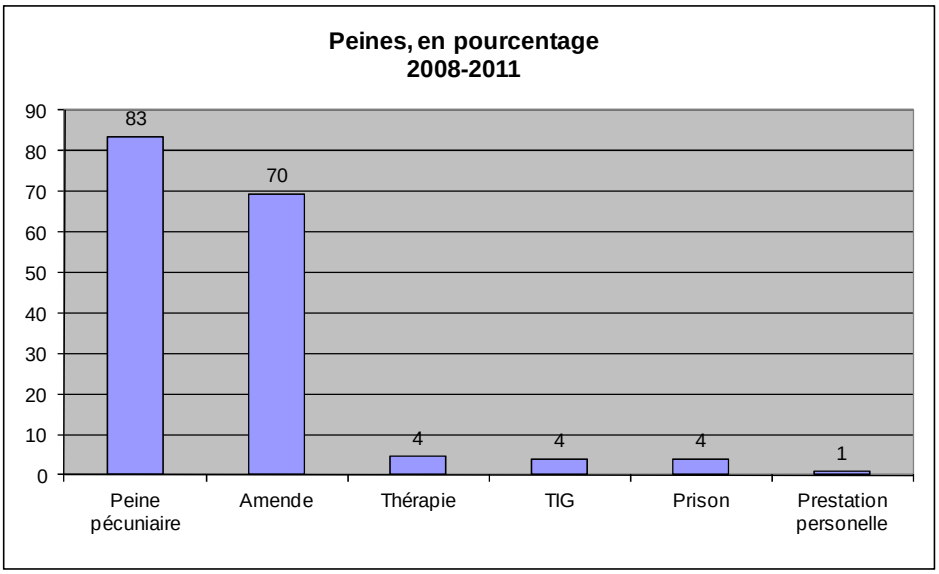
Les objets seront confisqués.



Graphique 15 : condamnations prononcées (N=532 condamnations)

La peine la plus fréquemment prononcée dans les cas de possession de pornographie illégale consiste en des jours-amende, auxquels s'additionne souvent une amende. Dans 91% des cas, la peine pécuniaire est assortie d'un sursis. Les sanctions alternatives comme le travail d'intérêt général (TIG) et les mesures thérapeutiques sont plus rares mais tout de même appliquées. Enfin, les peines les plus sévères, comme la peine privative de liberté (prison) mais également les peines pécuniaires fermes sont principalement réservées aux cas impliquant des récidivistes.

En ce qui concerne le montant des amendes, la quasi-totalité se situe entre 500 et 3000 CHF, et la plus haute s'élève à 6000 CHF. Précisons tout de même qu'à ces amendes s'ajoutent parfois des frais de procédure qui peuvent être élevés. Quant aux peines pécuniaires, le nombre de jours-amende se situe majoritairement entre 20 et 200 jours, pour des montants allant dans la plupart des cas de 20 CHF. à 200 CHF.



Graphique 16 : peines prononcées par les tribunaux (N=242 Feedback)

8. Groupes de travail

8.1 Nationaux

Au cours de l'année dernière, le SCOCI a été engagé dans différents groupes de travail nationaux, en particulier dans le domaine de la prévention des phénomènes criminels.

En collaboration avec le commissariat *pédocriminalité*-pornographie, le SCOCI a continué à s'engager cette année dans le groupe de travail « Kindsmissbrauch » (abus sur les enfants). En plus des représentants de fedpol, cette entité regroupe des représentants d'organisations non-gouvernementales, de cantons, ainsi que de la prévention suisse de la criminalité.

Le SCOCI a par ailleurs poursuivi son engagement dans le cadre du programme national « Protection de la jeunesse face aux médias et compétences médiatiques ». Le SCOCI siège en effet aussi bien dans le groupe de travail chargé d'élaborer le programme d'action, que 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. Dans le cadre du programme, la première journée nationale des compétences médiatiques a été organisée le 27 octobre à Fribourg.

Depuis 2011, le SCOCI représente fedpol dans le cadre de la commission spéciale de la prévention suisse de la criminalité. Cette commission a pour fonction d'élaborer des projets et matériaux pour la prévention de la criminalité dans les cantons, et d'évaluer les activités accomplies.

Dans le cadre du concept « sécurité et confiance », coordonné par l'Office fédéral de la communication (OFCOM), le SCOCI a participé a un groupe de travail ayant pour but d'informer le public sur les moyens d'effectuer des achats sur Internet en toute sécurité.

Enfin, le SCOCI participe également aux groupes de travail « Investigation IT » et « surveillance des télécommunications », qui traitent notamment des évolutions techniques et visent à une efficacité accrue dans le domaine de la poursuite pénale.

8.2 Internationaux

Au cours de l'année, le SCOCI s'est engagé dans le cadre de l' « AWF Cyborg » d'Europol, qui concerne les cas de *cybercriminalité* ayant des implications supranationales, tels que les attaques de *phishing*, les Botnets ou encore le piratage de bases de données à grande échelle. Le service est également partie prenante au projet « CIRCAMP », qui vise à contrecarrer la distribution de pornographie enfantine illégale sur Internet, tout en s'attaquant aux réseaux qui l'organisent. Enfin, Le SCOCI a également été représenté dans le groupe de travail de la *European Financial Coalition* à Bruxelles, et participe au T-CY (Convention Committe on Cybercime), qui est

l’organe de consultation des pays membres de la convention sur la *cybercriminalité*. 2011 marquait les 10 ans de la convention et, pour la Suisse, annonçait également son entrée en vigueur au premier janvier 2012.

9. Projets

9.1. Collaboration avec les fournisseurs d'accès Internet pour filtrer les sites de pornographie enfantine

Depuis 2007, le SCOCI collabore avec les principaux fournisseurs d'accès Internet suisses, dans le but d'interdire l'accès à du contenu pédopornographique aux utilisateurs suisses. Il s'agit principalement de sites hébergés à l'étranger, restant en ligne, bien qu'ayant déjà été annoncés aux autorités des pays concernés. Concrètement, une liste de domaines à bloquer est mise à disposition des fournisseurs d'accès pour que ces derniers redirigent les utilisateurs cherchant à y accéder vers une « stop-page ». Les fournisseurs se basent sur leurs conditions générales d'utilisation et leur politique d'entreprise pour prendre ce type de mesures.

Dans le cadre de ce projet, le SCOCI collabore avec Interpol, qui élabore une liste de domaines sur lesquels se trouvent des représentations d'abus d'ordre sexuel sur des enfants (« worst of list »). Différents pays participent à ce projet. La liste utilisée en Suisse se base ainsi sur cette « worst of list », à laquelle s'ajoute des domaines provenant d'une liste propre à la Suisse. L'année 2011 a vu une intensification de la collaboration avec Interpol. La « worst of list » est implémentée quotidiennement dans le système, et certains domaines dont le SCOCI a connaissance sont communiqués à Interpol pour être ajoutés à liste et ainsi être bloqués dans d'autres pays également.

9.2 Collection nationale de fichiers et de valeurs *hash* (CNFVH)

Le CNFVH vise à mettre sur pied une collection de valeurs *hash* de matériel illégal. Les données (images, vidéos, etc.), provenant notamment du matériel saisi lors des perquisitions, sont transmises par les polices cantonales au SCOCI. Le SCOCI génère pour chaque donnée une valeur *hash*[7] et l'enregistre dans la CNFVH. Cette liste sera mise à disposition des cantons à travers la *JANUS-Community*[8]. Par la suite, les cantons vont eux-mêmes produire la valeur *hash* des données nouvellement saisies, afin de pouvoir effectuer une comparaison avec la liste du SCOCI. Ce travail de comparaison des valeurs *hash* permet de vérifier de grandes quantités de données, sans devoir visualiser le contenu lui-même. Les doublons peuvent également être évités. Cette méthode permet d'épargner aux enquêteurs une partie du travail pénible de visualisation des images saisies.

L'année 2011 a vu des avancées majeures dans le cadre de ce projet. Le concept a été défini, en collaboration avec les cantons. Par la suite, l'infrastructure technique, de même que les procédures de travail ont été mises sur pied et sont désormais fonctionnelles. Le SCOCI a par ailleurs organisé une séance d'information et de formation à laquelle ont participé des représentants de tous les cantons. Enfin, les premiers lots d'images sont parvenus au SCOCI.

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

[8] Intranet permettant de mettre des informations à disposition des services de police à travers la Suisse.

Grâce à un programme de reconnaissance d'image, élaboré conjointement par le SCOCI et l'entreprise suisse ATG, le travail de catégorisation et de vérification des données devrait être nettement réduit. Après une phase de test, le programme pourra également être utilisé lors d'engagements opérationnels.

9.3 Stratégie nationale de défense contre les *cyberrisques* (anciennement appelée stratégie nationale de *cyberdéfense*)

En date du 10 décembre 2010, le Conseil fédéral a chargé le DDPS d'élaborer une stratégie nationale de *cyberdéfense* et a nommé le divisionnaire Kurt Nydegger comme chef de projet. L'objectif de la stratégie est la protection des infrastructures critiques contres les menaces cybernétiques. Elle doit fournir des indications précises en terme de mise en œuvre et sur les conséquences prévues au niveau des délais, frais, capacités, bases législatives et ressources. La stratégie définitive, avec différentes variantes quant à la mise en œuvre est attendue par le Conseil fédéral au premier trimestre 2012. Le SCOCI appartient depuis mai 2011 à l'équipe de projet et représentera les intérêts des autorités de poursuite cantonales et fédérales lors de la mise en œuvre de la stratégie.

10. Interventions parlementaires au niveau fédéral

10.1 Interventions parlementaires déposées en 2011

Protection de la jeunesse/pédophilie

Interpellation Pasquier : Protection des enfants contre l'exploitation et les abus sexuels
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20113141

Motion Savary : Pornographie sur Internet. Agir en amont
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20113314

Question Bruderer-Wyss : Répression des actes d'ordre sexuel avec des mineurs âgés de 16 à 18 ans
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20115351

Question Rickli : Registre national des pédophiles
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20115008

Motion Schmid-Federer : Eriger en infraction pénale la sollicitation d'enfants à des fins sexuelles
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20114002

Objet du CF : CP, CPM et DPMin. Imprescriptibilité des actes d'ordre sexuel ou pornographique commis sur des enfants
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20110039

Autres sujets

Interpellation Amherd : Renforcement de la surveillance sur Internet
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20113862

Postulat Eichenberger-Walther : Pour un réseau national de centres de compétences de police
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20113642

Question Leutenegger-Oberholzer : Utilisation de logiciels espions par la Confédération
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20115541

Question Reimann : Pratiques contestables de PayPal en Suisse
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20115438

Question Schmid-Federer : Campagnes de prévention annoncées l'an dernier par l'OFAS. Où en est-on?
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20115198

Postulat Amherd : Donnons un cadre juridique aux médias sociaux
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20113912

Postulat Schmid-Federer : Loi-cadre sur les TIC
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20113906

Pétition : Interdiction de jeux violents
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20112005

10.2 Evolutions législatives

La lutte contre la criminalité sur Internet présente également des enjeux forts en terme de jurisprudence et au niveau législatif. Les évolutions les plus marquantes dans ces domaines sont présentées ci-dessous.

Arrêt du tribunal fédéral 6B_744/2010

Le Tribunal fédéral a été confronté en 2011 à la question de la pénalisation des contenus *pédopornographiques* se trouvant dans le cache de l'ordinateur. Dans sa décision du 12 mai 2011, le Tribunal fédéral précise son interprétation : toutes les données électroniques et formes de sauvegardes tombent sous le coup de l'article 197, ch. 3bis du Code pénal. Les contenus des sites *web* visités sont en effet automatiquement enregistrés dans un fichier temporaire, ce qui permet un chargement plus rapide lors d'une nouvelle visite. A l'aide de programmes courants et gratuits (cache-viewer ou cache-reader) ces données sont par ailleurs accessibles, également sans être connecté à Internet. La possession illégale de pornographie dure au sens de l'article 197, ch.3bis du Code pénal suppose la possibilité et la volonté de posséder de tels contenus. Pour l'utilisateur peu aguerri, qui n'a pas conscience des sauvegardes effectuées dans le cache, on ne saurait parler de possession. En revanche, bien que les sauvegardes dans le cache s'effectuent automatiquement, on part du principe que les utilisateurs plus aguerris connaissent la possibilité de désactiver cette fonction, ou d'effacer ces fichiers temporaires.

Par ailleurs, celui qui visite des sites proposant des contenus pédopornographiques régulièrement et en ayant pleine conscience du contenu ne se limite pas à la simple contemplation. A travers l'accès répété aux contenus, il démontre sa volonté de posséder.

Ainsi, une acquisition au sens de l'article 197, ch. 3bis CP existe lorsqu'un internaute obtient à l'aide d'un mot de passe un accès illimité et de longue durée à un site proposant des contenus *pédopornographiques*. Il en va de même pour la possession. Sa définition est également remplie lorsque l'accès à des données *pédopornographiques* est possible en tout temps, par exemple à travers le cache. Ce n'est que de cette manière que la punissabilité absolue de l'accès à la pornographie dure telle que souhaitée par le législateur peut être atteinte.

Le Conseil fédéral confirme la loi sur le droit d'auteur

En novembre 2011, le Conseil fédéral a adopté un rapport concernant un postulat de la Conseillère aux Etats Géraldine Savary (PS/VD), daté de mars 2010. Le postulat chargeait le Conseil fédéral d'examiner s'il convenait de prendre des mesures contre les violations des droits d'auteur.

Le rapport brosse un tableau de la situation actuelle. Les enquêtes existantes permettent de conclure que jusqu'à un tiers des plus de 15 ans en Suisse téléchargent gratuitement de la musique, des films et des jeux. Internet a fondamentalement modifié la manière d'acquérir et de consommer ce type de production. Le Conseil fédéral juge cependant les craintes, de voir cette évolution avoir un impact négatif sur la

création culturelle suisse, infondées et arrive donc à la conclusion qu'il n'y a pas lieu de prendre des mesures législatives. Cela signifie pour les utilisateurs suisses, que le téléchargement de films ou de musique protégés par le droit d'auteur, pour une utilisation personnelle, reste non punissable.

Cybercrime convention

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 la 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'introduction illicite dans un système informatique protégé, mais aussi la pornographie enfantine et la violation des droits d'auteur sur Internet.

La 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 procédure. 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 de piratage informatique est déplacée en amont: 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 sur le trafic informatique, à l'autorité requérante avant la clôture de la procédure d'entraide. 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 que le point de contact 24/7 prévu par l'article 35 de la convention serait assuré par la centrale d'engagement de fedpol (SPOC, EZ fedpol). Le SCOCI soutient la centrale d'engagement dans le traitement des demandes selon la convention.

11. Médias, enseignement et conférences

11.1 Présence médiatique

Au cours de l'année, le SCOCI a eu l'occasion de s'exprimer et de présenter son activité dans différents médias, qu'il s'agisse de presse écrite, télévision ou radio. Certains reportages ont présenté le service d'une manière générale, alors que d'autres se sont focalisés sur des aspects ou des phénomènes particuliers. Les enquêtes sous couverture, mais également certaines attaques informatiques (notamment DDoS[9]) ayant eu lieu au cours de l'année sont des sujets ayant fait l'objet d'une attention médiatique soutenue.

11.2 Enseignement et conférences

Au cours de l'année 2011, les collaborateurs du SCOCI ont eu l'occasion de participer à différentes conférences et formations. Ces dernières constituent des occasions privilégiées de s'entretenir et nouer des contacts avec différents partenaires et experts.

En Suisse :

- Journée suisse des enquêteurs IT, Berne
- Journée des compétences médiatiques (dans le cadre du programme national « Jeunes et Médias »), Fribourg
- World Summit information society, Genève

A l'étranger :

- « RIPE NCC meeting », Londres
- Conférence « Octopus Interface », Strasbourg
- « E-crime Congress », Londres
- Réunion des experts en *cybercriminalité*, ONU, Vienne
- Symposium « Nouvelles technologies » BKA Wiesbaden
- « Fighting Cybercrime : cooperation between law enforcement agencies and the internet industry », Académie de droit européen, Trier
- « Child Sexual Exploitation Experts Conference » Europol, La Haye

[9] Distributed Denial of service

12. Partenariats et contacts du SCOCI

12.1 Collaboration avec d'autres services de la Confédération

Au cours de l'année, le SCOCI a poursuivi sa collaboration avec de nombreux autres services de la Confédération. Au sein de fedpol, le SCOCI entretient notamment des rapports fréquents avec les commissariats investigation secrète, protection de l'Etat, investigation IT, et avec la division principale coopération policière internationale. En raison de la proximité des thématiques traitées, et des 6 postes attribués en 2011 par le Conseil fédéral à la lutte contre la *pédocriminalité*, une relation particulièrement intensive existe par ailleurs entre le SCOCI et le commissariat *pédocriminalité*-pornographie.

D'autres partenaires fédéraux ont été consultés, ou ont eu recours à l'expertise ou au soutien du SCOCI. On pense notamment à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), l'entraide judiciaire internationale de l'Office fédéral de la justice (OFJ), l'Office fédéral de la communication (OFCOM), l'Office fédéral des assurances sociales (OFAS), le secrétariat d'Etat à l'économie (SECO), swissmedic ou la commission des loteries et paris (Comlot).

Enfin, il convient de souligner la collaboration étroite qui est entretenue avec la Prévention suisse de la criminalité (PSC). En particulier, le SCOCI représente depuis cette année fedpol dans le cadre de la commission spéciale de la PSC.

12.2 Séances de travail et échange d'expériences avec les cantons

La collaboration avec les différents représentants des autorités judiciaires et des polices cantonales a été particulièrement intense au cours de l'année. En plus des échanges habituels d'informations avec les cantons et le Liechstenstein, de nombreux contacts plus opérationnels ont eu lieu au cours de l'année, en particulier en lien avec le projet CNFVH et les enquêtes sous couverture.

Dans le cadre de la stratégie nationale de *cyberdéfense* et suite à différentes demandes politiques liées à la criminalité sur Internet, un bon contact privilégié a été établi avec le congrès informatique de la police suisse (SPIK).

12.3 Collaboration avec Action Innocence Genève (AIG)

Depuis de nombreuses années, le SCOCI collabore avec l'ONG Action Innocence dans le cadre de la lutte contre la pornographie enfantine. C'est en particulier grâce au soutien opérationnel et financier d'AIG que le projet de monitoring des réseaux *peer-to-peer* a pu être développé avec succès au cours des dernières années. L'outil permettant de monitorer ces réseaux a été directement développé et mis à disposition par AIG. La collaboration avec AIG est donc fondamentale pour le service, puisque c'est de son activité sur les réseaux *peer-to-peer* que découle la nette majorité des cas de recherche active effectués chaque année. En plus de cela, AIG soutient le SCOCI dans le cadre de différents autres projets liés à lutte contre la *pédocriminalité*.

12.4 Collaboration avec le secteur privé (Public-Private-Partnership, PPP)

La volonté du SCOCI d'intensifier sa collaboration avec les entreprises privées actives dans le domaine d'Internet ou des nouvelles technologies s'est, cette année, traduite par de nombreuses visites ou collaborations concrètes. Des contacts ont été instaurés avec plusieurs fournisseurs de services actifs sur Internet. Cette collaboration est en particulier nécessaire afin d'obtenir plus facilement des informations sur la connexion Internet des utilisateurs (notamment adresses IP) dans le cadre d'enquêtes ou d'enquêtes préliminaires.

12.5 Visites extérieures

Au cours de l'année, le SCOCI a eu l'occasion d'accueillir de nombreux visiteurs externes. Ces visites sont autant d'occasions pour le SCOCI de présenter son travail et de sensibiliser aux problématiques l'occupant au quotidien. En particulier, plusieurs médias sont venus visiter le service en cours d'année.

12.6 Contacts internationaux

En plus de la participation aux groupes de travail mentionnés au chapitre 8.2, le SCOCI a visité et accueilli plusieurs de ses homologues étrangers. Ces visites s'inscrivent dans une volonté d'instaurer des processus de collaboration d'une manière générale. A côté de la question de la lutte contre la *pédopornographie* sur Internet, la *cybercriminalité*, au sens strict du terme, et la criminalité économique sont des thèmes primordiaux lors de ces échanges. Ces derniers peuvent notamment aussi être liés à des opérations en cours ou à des activités telles que les enquêtes sous couverture.

13. Glossaire

Adult check	Procédé permettant de limiter l'accès d'un site *web* à un public majeur uniquement.
Chat	Dialogue en direct.
Cloud Computing	L'informatique dans les nuages (en anglais, cloud computing) fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des 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 - métaphoriquement parlant - 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	Nous reprendrons ici la définition donnée par le Conseil Fédéral dans son rapport de juin 2010 : « On peut donc parler de cyberintimidation 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	De tels sites 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	Modèle de réseau informatique permettant l'échange de fichiers entre utilisateurs (les pairs).
Phishing	Par ces méthodes, les criminels tentent d'obtenir frauduleusement des données personnelles d'utilisateurs (mots de passe, nom d'utilisateur, etc.), principalement en imitant des sites Internet légitimes.
Pornographie dure	Actes d'ordre sexuel avec des enfants (pédophilie, *pédopornographie*), avec des animaux, des excréments humains, ou comprenant des actes de violence (art. 197, ch.3 CP).
Proxy	Un *proxy*, est un 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	Un *redirect service* permet de bénéficier d'un URL «simplifié» redirigeant l'utilisateur vers un contenu (notamment un URL plus simple à retenir ou plus court que celui vers lequel on est redirigé au final).
Spam	Communication électronique non sollicitée, principalement effectuée en masse et à des fins publicitaires, ou parfois dans le but d'installer un logiciel malveillant.
Streaming	Mode de transmission de données audio et vidéo. Ces dernières sont transmises en flux continu, plutôt qu'après téléchargement complet (permet la lecture de contenu « en direct »).
URL	*Uniform Ressource Locator*, chaîne de caractère utilisée pour adresser les ressources du *web*. Il s'agit de l'adresse *web*.
Valeur hash	Valeur unique permettant d'identifier une donnée, notamment une image (empreinte digitale).

14. Tendances 2011

La baisse globale des annonces, et en particulier de celles concernant des contenus *pédopornographiques* sont des signaux qu'il convient de chercher à comprendre. Tout d'abord, il serait faux de supputer une baisse des phénomènes criminels sur Internet, hypothèse ne correspondant pas à l'état de la connaissance actuelle, ni à ce qu'observe le SCOCI au quotidien. En revanche, la possibilité qu'un phénomène de banalisation envers certains de ces délits ne se développe dans la population mérite d'être prise en considération.

Ce phénomène de baisse des annonces souligne par ailleurs l'importance d'une communication visant à inciter les internautes à reporter les délits dont ils sont victimes ou les contenus suspects dont ils prennent connaissance. En effet, seules des autorités informées de l'ampleur du phénomène et de ses développements seront en mesure de prendre les mesures adéquates.

Cette tendance à la baisse doit également nous pousser à nous interroger sur le développement de réseaux de moins en moins visibles, en particulier dans le domaine de la *pédopornographie* en ligne. Des systèmes de communication fermés et anonymes (forums, groupes, réseaux sociaux) sont en effet de plus en plus utilisés pour échanger des contenus illégaux. En raison des évolutions technologiques continues et des nouvelles possibilités offertes, un renforcement de ces tendances est à envisager.

Face à ces phénomènes, les enquêtes sous couverture prennent tout leur sens. Dans un contexte de baisse des signalements du public, et de développement de réseaux difficiles à cerner et à pénétrer, la possibilité d'agir sous couverture pour déceler des infractions et protéger les victimes potentielles est d'autant plus nécessaire.

Dans ce contexte de baisse globale, la hausse constante des cas d'escroquerie est également un enseignement majeur. Les internautes suisses sont de plus en plus ciblés par des escrocs opérant pour la plupart depuis l'étranger. La prévention, en vue de former des internautes responsables sachant déceler les dangers d'Internet reste à ce titre une priorité.

Enfin, pour ce phénomène comme pour tous les autres types de délits commis 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 des différents pays impliqués, fournisseurs d'accès, hébergeurs et autres fournisseurs de services Internet, administrateurs des noms de domaines et des adresses IP. Différents groupes de travail auxquels participe le SCOCI, au niveau Suisse et international, visent à poursuivre ce but. Dans cette optique, la capacité à développer des solutions impliquant des organismes privés et publics (Public-Private-Partnership) dans la lutte contre la criminalité sur Internet jouera un rôle décisif à l'avenir.