



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 national de coordination de la lutte contre la criminalité sur Internet SCOCI**

## **Rapport annuel 2010**

---

## **Table des matières**

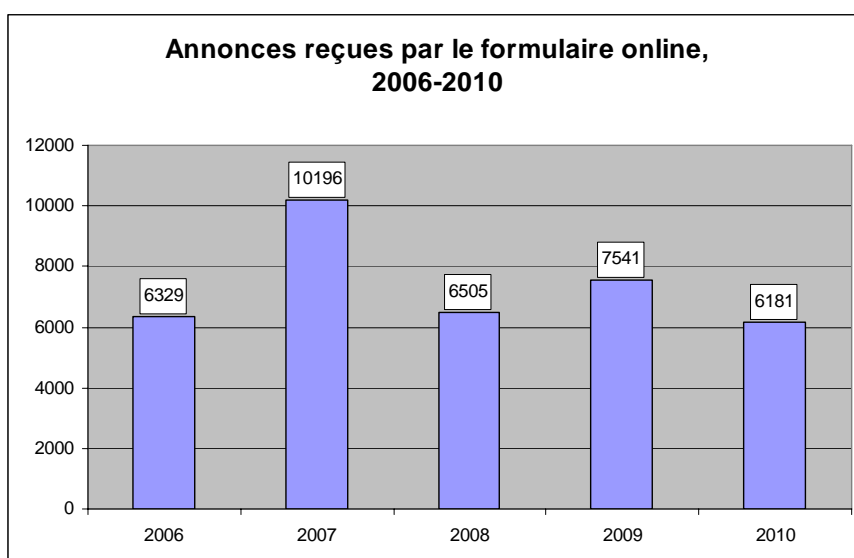
<b>1. L'ESSENTIEL EN BREF</b> .....	<b>3</b>
<b>2. NOMBRE DE COMMUNICATIONS REÇUES</b> .....	<b>4</b>
<b>3. TYPES D'INFRACTIONS ENREGISTRÉES</b> .....	<b>5</b>
<b>4. RECHERCHE ACTIVE (MONITORING)</b> .....	<b>9</b>
<b>5. QUELQUES CAS INTÉRESSANTS</b> .....	<b>10</b>
<b>6. DOSSIERS TRANSMIS AUX AUTORITÉS</b> .....	<b>11</b>
<b>7. FEEDBACK DES CANTONS</b> .....	<b>13</b>
<b>8. GROUPES DE TRAVAIL</b> .....	<b>14</b>
<b>9. PROJETS</b> .....	<b>15</b>
9.1. COLLABORATION AVEC LES FOURNISSEURS D'ACCÈS INTERNET POUR FILTRER LES SITES DE PORNOGRAPHIE ENFANTINE.....	15
9.2 INVESTIGATION SECRÈTE.....	15
<b>10. INTERVENTIONS PARLEMENTAIRES AU NIVEAU FEDERAL</b> .....	<b>16</b>
<b>11. MÉDIAS, ENSEIGNEMENT ET CONFÉRENCES</b> .....	<b>18</b>
11.1 PRÉSENCE MÉDIATIQUE.....	18
11.2 ENSEIGNEMENT ET CONFÉRENCES.....	18
<b>12. PARTENARIATS ET CONTACTS</b> .....	<b>19</b>
12.1 COLLABORATION AVEC D'AUTRES SERVICES DE LA CONFÉDÉRATION.....	19
12.2 SÉANCES DE TRAVAIL ET ÉCHANGE D'EXPÉRIENCES AVEC LES CANTONS.....	19
12.3 VISITES EXTÉRIEURES.....	19
12.4 COLLABORATION INTERNATIONALE OPÉRATIONNELLE.....	19
<b>13. GLOSSAIRE</b> .....	<b>21</b>
<b>14. TENDANCES 2010</b> .....	<b>22</b>

## 1. L'essentiel en bref

- Malgré une baisse du nombre total d'annonces, le SCOCI enregistre, pour la deuxième année consécutive, une forte hausse des annonces de sites contenant du matériel pornographique illégal. Il s'agit principalement de sites contenant du matériel pédopornographique. Les plateformes à disposition des pédophiles sont nombreuses et en constante évolution.
- Les annonces pour escroquerie sont également en hausse, ce qui démontre que les utilisateurs suisses sont toujours fortement visés par de nombreux types d'arnaques. De nouveaux modus operandi sont fréquemment répertoriés, mais certains types d'arnaques connus continuent de faire des victimes.
- Le SCOCI a poursuivi l'intensification de son travail de recherche active de contenus illicites. Le nombre de dossiers de suspicion transmis aux autorités cantonales est en hausse.
- Les feedback reçus par les cantons témoignent à nouveau de la fiabilité des dossiers transmis aux cantons. En effet, la grande majorité d'entre eux sont à l'origine d'une perquisition ayant permis de saisir du matériel illégal.
- La question de l'investigation secrète a été au centre des préoccupations du SCOCI au cours de l'année. Depuis le 1<sup>er</sup> janvier 2011, la plupart des polices cantonales n'ont plus le droit de mener d'enquêtes sous couverture contre les pédocriminels sur Internet de manière préventive et sans soupçon d'infraction. Cela résulte de l'entrée en vigueur du nouveau code de procédure pénale suisse au 1<sup>er</sup> janvier 2011 et du fait que la majorité des règlements de polices cantonaux ne prévoient pas ce genre d'intervention policière. Divers travaux parlementaires ont été menés dans le but de remédier à cette lacune. Le DFJP et la Conférence des directrices et directeurs des départements cantonaux de justice et police ont proposé une solution qui permet au SCOCI de continuer à mener cette activité d'investigation secrète. Grâce à un accord avec le canton de Schwyz, le SCOCI est dorénavant autorisé à investiguer de manière préventive et de surveiller les sites de dialogue en direct de son propre chef ou sur demande d'un canton.

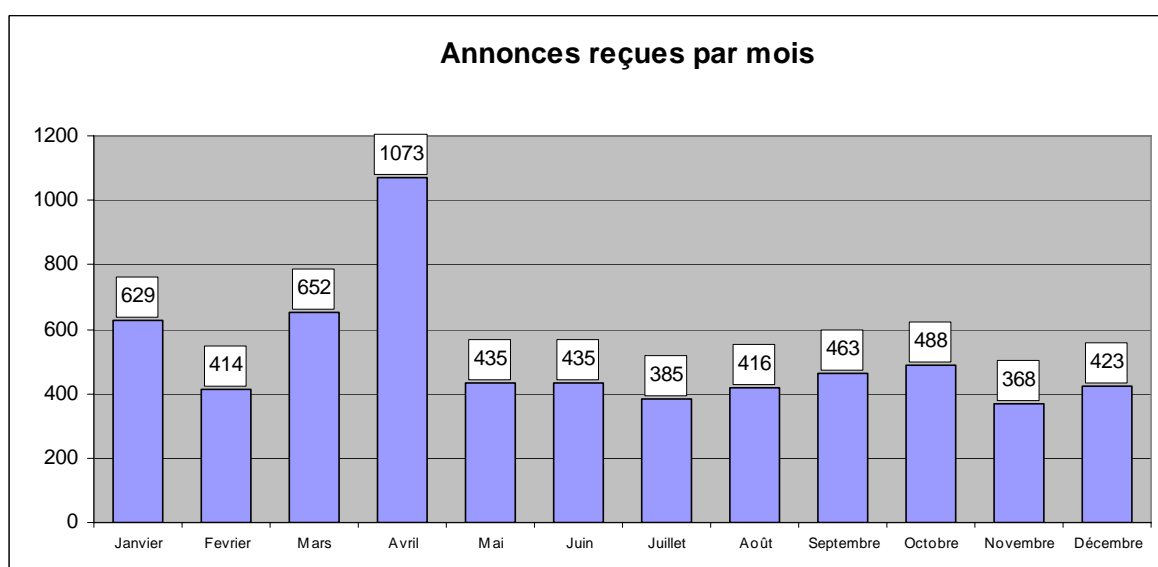
## 2. Nombre de communications reçues

En 2010, le SCOCI a enregistré 6181 annonces via son formulaire online. Il s'agit d'un recul par rapport aux années précédentes. Il conviendra de vérifier dans les années prochaines si nous sommes en présence d'une tendance ou d'une simple variation comme s'en sont produites de nombreuses depuis la création du SCOCI. Néanmoins, si l'on excepte 2007, on note que la moyenne annuelle du nombre d'annonces est relativement stable, se situant entre 6000 et 7500.



Graphique 1: Annonces reçues via [www.scoci.ch](http://www.scoci.ch) (comparaison sur 5 ans)

La comparaison par mois permet de constater de grandes disparités (cf. graphique 2). Il semble néanmoins difficile d'en tirer de quelconques conclusions, puisque ce sont parfois des événements bien particuliers qui permettent d'expliquer ces variations.



Graphique 2: Annonces reçues via [www.scoci.ch](http://www.scoci.ch), par mois (au total: 6181 annonces)

### 3. Types d'infractions enregistrées

Le premier résultat significatif est la forte augmentation des annonces de sites proposant de la pornographie dure. La catégorie "pornographie dure" regroupe les différents types de pornographie illégale (pédopornographie, pornographie avec des excréments, de la violence et des animaux), mais il s'agit dans la très grande majorité des cas de pornographie enfantine (96 % du total de la catégorie). La tendance à la hausse observée l'année dernière se confirme et se renforce nettement, aussi bien en termes de nombres absolus qu'en pourcentage du total des annonces (graphiques 3 et 4). Cette catégorie est d'ailleurs celle qui a fait l'objet du plus grand nombre d'annonces en 2010, devançant ainsi les annonces pour spam, qui sont en baisse par rapport à l'année précédente. Un phénomène marquant est notamment l'importance accrue des sites web communautaires ("communities"), qui sont désormais un des vecteurs privilégiés de transmission du matériel pédopornographique.

Parallèlement, on constate une baisse significative des annonces pour des sites proposant de la pornographie dite légale. En particulier, les annonces pour des sites gratuits proposant des films pornographiques en streaming sont en forte baisse, ce qui peut être interprété comme le signe d'une banalisation ou une plus grande tolérance face à ce type d'offres chez les utilisateurs.

La tendance à la hausse des annonces dans le domaine des escroqueries se poursuit. Les annonces dans cette catégorie ont connu des hausses régulières depuis 2006, ce qui démontre encore une fois qu'il s'agit là d'une préoccupation majeure chez les utilisateurs suisses. Ce type de délit est en perpétuelle évolution et nous notons que de nouveaux modus operandi apparaissent chaque année. Les sites de petites annonces sont toujours fortement utilisés par les escrocs. Le marché des voitures d'occasion est particulièrement visé, avec des arnaques à la vente ou à l'achat, faisant notamment intervenir des fausses entreprises de transport, complices de l'escroquerie. Bien entendu, d'autres types de marchandises peuvent également être visées par ce type de fraude. A côté de cela, les arnaques à l'abonnement, dans lesquelles l'utilisateur pensant profiter d'un service gratuit contracte en fait un abonnement onéreux, sont toujours en vigueur. Il en va de même des différentes variations sur le thème de l'"advance-fee fraud"<sup>1</sup>.

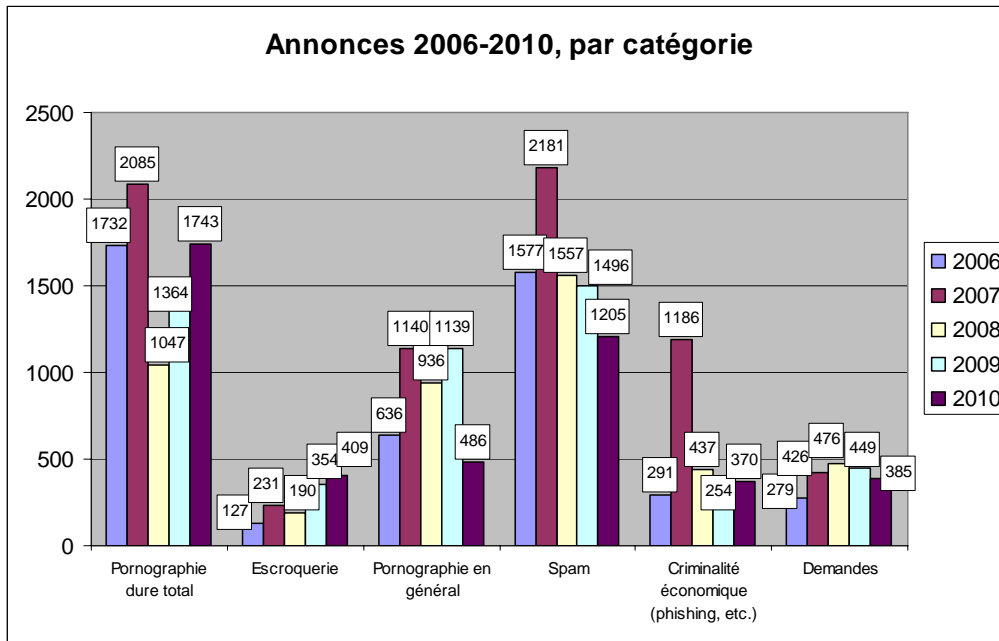
Les annonces enregistrées dans la catégorie "criminalité économique" connaissent également une hausse par rapport à l'année dernière. En particulier, de nombreuses vagues de phishing<sup>2</sup> ont été observées au cours de l'année. Les services de paiement sur Internet ont notamment été visés, mais également les services de messagerie. Dans ce dernier exemple, on a également observé de nombreux cas où après s'être introduit sur le compte de sa victime, l'escroc cherche à extorquer de l'argent aux contacts figurant sur le compte.

Enfin, le niveau de demandes adressées au SCOCI par des citoyens peut être considéré comme relativement stable (en pourcentage du total) au cours des dernières années, ce qui témoigne de l'importance de ce service fourni au public.

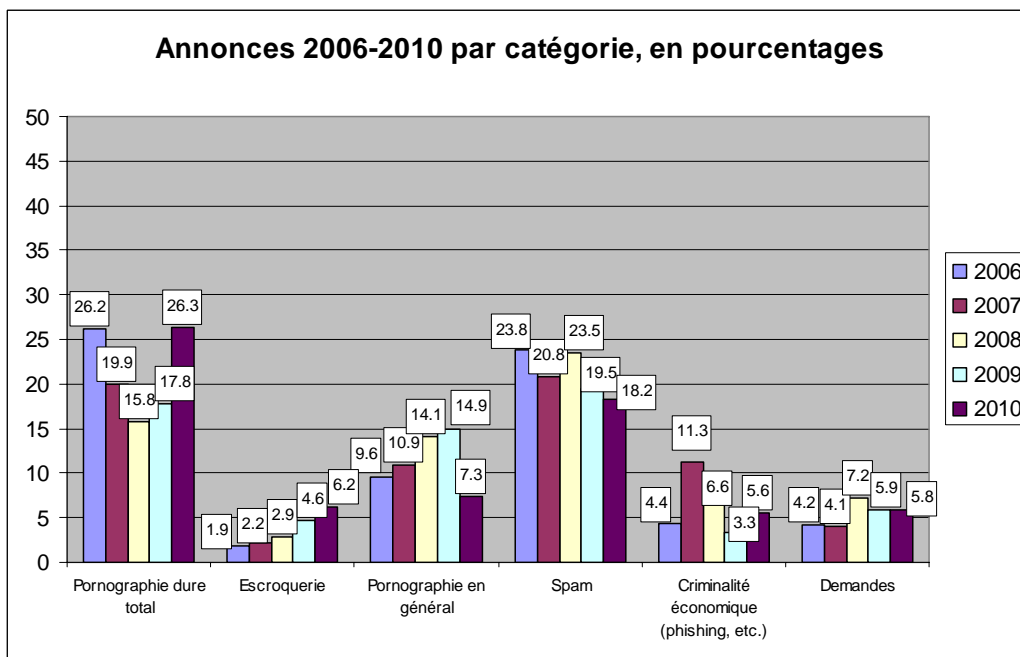
---

<sup>1</sup> Arnaque consistant à solliciter des paiements préalablement au versement d'un prétendu gros gain (par exemple de loterie).

<sup>2</sup> 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.



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

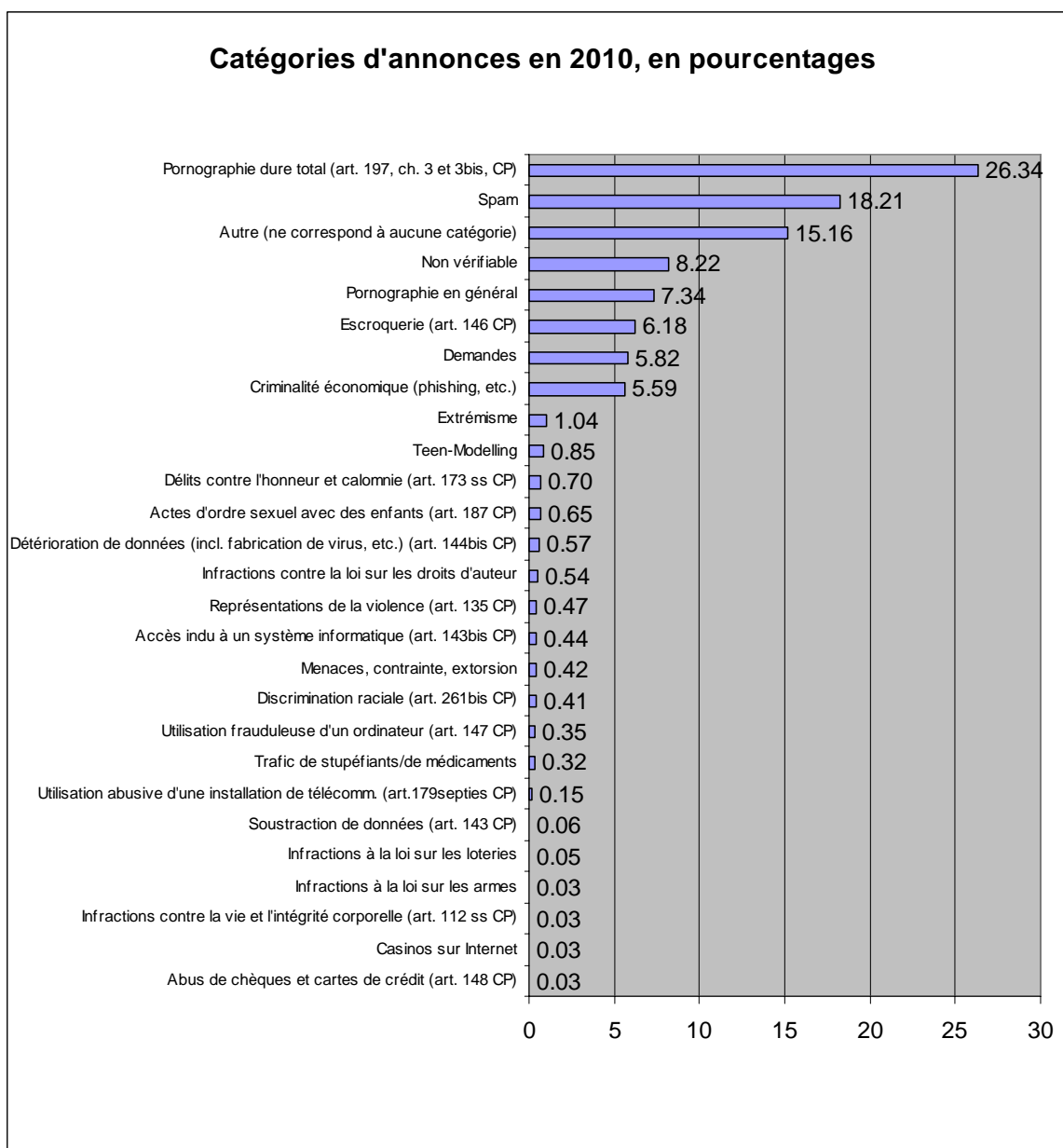


**Graphique 4: Evolution des catégories d'annonce principales (en pourcentages), sur 5 ans**

Le graphique 5 présente une vue d'ensemble des différentes catégories d'annonces faites au SCOCI. En particulier, et pour compléter ce qui précède, nous notons comme chaque année l'importance des catégories "autre" (n'entrant dans aucune des catégories prédéfinies cf. page 12) et "non vérifiable". Cette dernière catégorie, qui concerne principalement des URL n'étant plus actives, témoigne de la durée de vie souvent courte des sites nous étant annoncés.

Les cas issus des catégories "délits contre l'honneur et calomnie" et "menace, contraintes et extorsions", même s'ils sont relativement faibles en nombres absolus, sont néanmoins révélateurs de certains phénomènes assez préoccupants. Ce sont en effet dans ces catégories que l'on retrouve les cas de "cyberintimidation". Ce phénomène, qui fait l'objet d'une attention toute particulière, aussi bien au niveau

médiatique que politique, ne constitue pas une catégorie particulière. Il est néanmoins possible de retracer les cas rentrant dans sa définition<sup>3</sup>, qui s'élèvent à 25 (dont au minimum 4 concernant des mineurs) pour l'année 2010.



**Graphique 5: Annonces 2010, en pourcentages du total des annonces**

En dernier lieu, il convient d'ajouter à ces annonces parvenues par le formulaire celles qui nous sont transmises dans le cadre de notre collaboration avec Telefono Arcobaleno<sup>4</sup>. En 2010, Telefono Arcobaleno a annoncé au SCOCI 587 liens menant vers du matériel pédopornographique ou supposé comme tel. Dans la majeure partie

<sup>3</sup> 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 tchats, 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".

<sup>4</sup> Telefono Arcobaleno est une organisation italienne active dans le domaine de la protection de l'enfance.

des cas, il s'agit de liens vers du matériel hébergé sur des sites de "One Click-Hosting"<sup>5</sup>, basés en Suisse. Les liens annoncés, qui dirigent vers du contenu illégal, sont ensuite annoncés à cette société par le SCOCI en vue d'une suppression du contenu. Ce chiffre est en forte baisse par rapport à 2009, ce qui témoigne du fait que les sites concernés sont moins utilisés pour l'échange de contenus pédopornographiques, notamment en raison de la surveillance accrue dont ils font désormais l'objet.

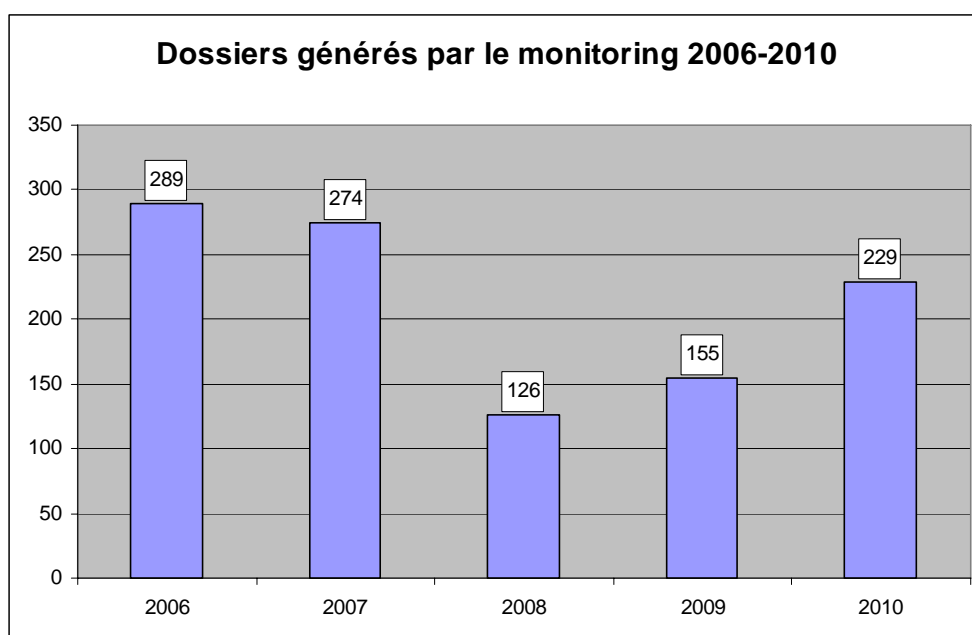
---

<sup>5</sup> 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.



## 4. Recherche active (monitoring)

En ce qui concerne les cas générés par la recherche active (monitoring) du SCOCI, l'année 2010 confirme l'accroissement de l'investissement effectué dans ce domaine. En effet, 229 dossiers ont été établis par le monitoring avant d'être transmis aux autorités cantonales de poursuite pénale, ce qui correspond à une hausse notable. Il s'agit toujours de cas de possession réitérée et de diffusion présumée de pornographie infantile. Ces dossiers sont issus du monitoring des réseaux peer-to-peer ciblant les utilisateurs échangeant de la pédopornographie.



Graphique 6: Dossiers créés à la suite de recherches actives du SCOCI<sup>6</sup>

---

<sup>6</sup> La date faisant foi est celle de la création du cas. La date de transmission du cas au canton peut parfois être repoussée à l'année suivante (pour les cas générés en fin d'année), et donc être comptabilisée différemment.

## 5. Quelques cas intéressants

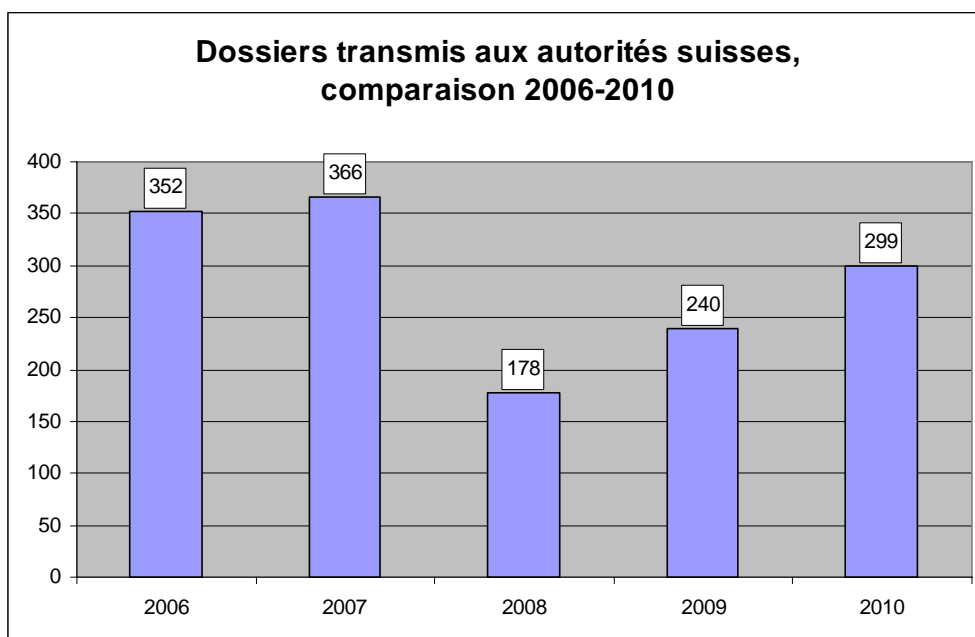
Dans le cadre de son activité de monitoring des réseaux peer-to-peer, le SCOCI a identifié un utilisateur échangeant du matériel pédopornographique. Comme il est d'usage dans ce type de cas, le dossier constitué a été transmis à la police du canton où se trouvait la connexion Internet de l'utilisateur en question. L'investigation menée par la suite par la police cantonale a permis de déterminer que cette connexion était utilisée par une personne résidant dans le canton la semaine, mais étant officiellement domiciliée dans un autre canton. Suite à cela, afin d'assurer la coordination entre les deux cantons concernés, le dossier a été transmis au Commissariat Pédophilie et pornographie de la Police judiciaire fédérale. Il a de plus été demandé au SCOCI de mener de nouvelles investigations, car l'auteur exerçait une fonction sensible, et la police cantonale souhaitait disposer de plus d'éléments avant de mener une perquisition. Des investigations secrètes ont alors été menées sur des réseaux sociaux, et les éléments ainsi réunis ont été transmis à la police cantonale. Suite à cela, une perquisition a permis de saisir des photos et vidéos à caractère pédopornographique, puis d'obtenir des aveux de la part de la personne.

Dans un autre cas intéressant, la perquisition menée par la police cantonale auprès d'un utilisateur échangeant de la pédopornographie sur les réseaux peer-to-peer a permis d'établir que l'utilisateur en question abusait sexuellement une victime mineure depuis une longue période. Des investigations plus poussées ont par ailleurs révélé que la victime mineure était livrée à son agresseur par sa mère toxicomane, contre rémunération.

Enfin, dans le cadre d'une enquête sous couverture, un Suisse de 42 ans a été identifié sur un site de dialogue en direct réservé aux jeunes, alors qu'il essayait d'entrer en contact avec un agent du SCOCI se faisant passer pour une jeune fille de 13 ans. L'âge de la prétendue jeune fille n'a pas empêché l'adulte en question de tenir des propos à connotation sexuelle, et de lui demander de manière répétée des photos. Le cas a été transmis à l'autorité cantonale de poursuite pénale compétente.

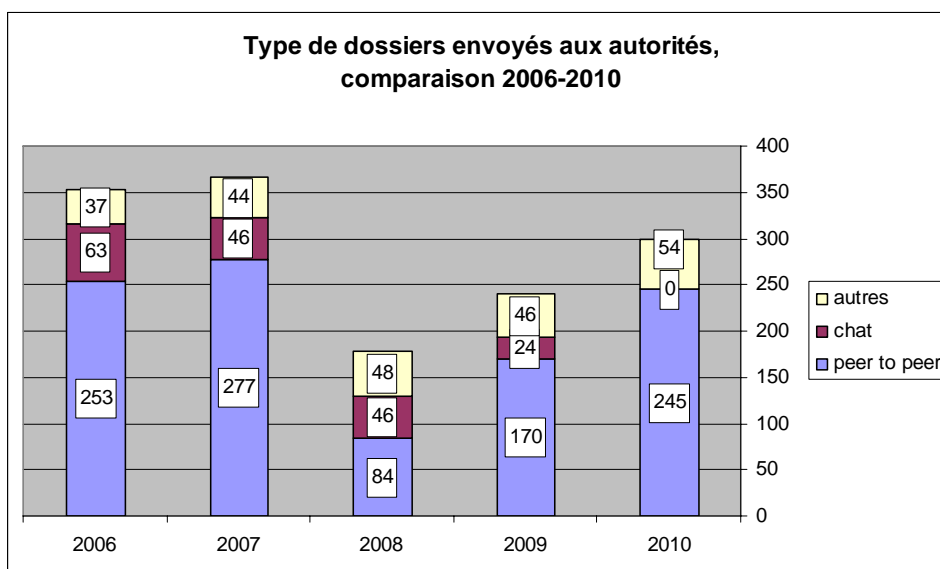
## 6. Dossiers transmis aux autorités

Pour la deuxième année consécutive, les dossiers de suspicion transmis aux autorités cantonales de poursuite pénale (299) sont en nette augmentation. Ce résultat est logique au vu de l'augmentation des cas générés par le monitoring évoquée plus haut.



Graphique 7: Dossiers transmis aux autorités, en nombres absolus

L'analyse du type de dossiers envoyés (cf. graphique 8) permet de confirmer que cette hausse est principalement le résultat de l'activité de monitoring des réseaux peer-to-peer. Durant l'année 2010, ce sont 245 dossiers de ce type qui ont été transmis aux autorités cantonales de poursuite pénale. 54 autres dossiers ont été transmis suite à des annonces du public.

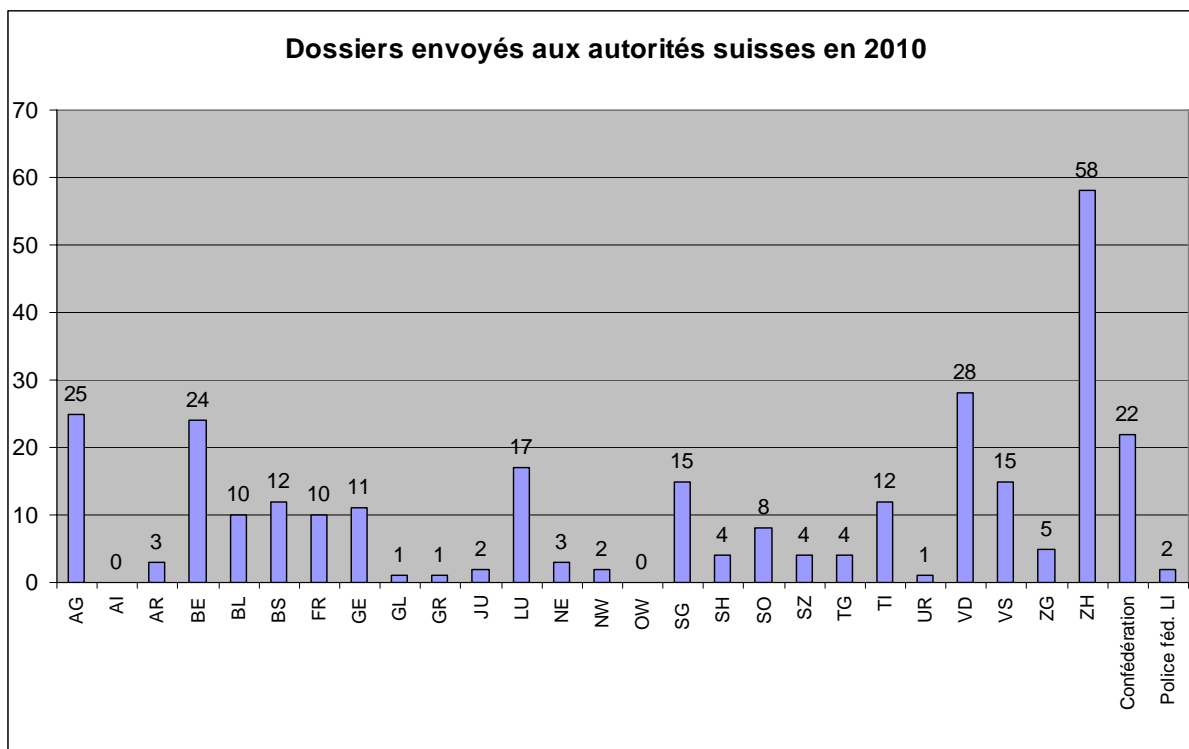


Graphique 8: Type de dossiers transmis, en nombres absolus

En revanche, aucun dossier de "chat", à savoir d'actes d'ordre sexuel avec des enfants constatés sur les sites de dialogue en direct, n'a été transmis aux cantons durant l'année 2010. Ce résultat est tout d'abord explicable par l'abandon par Swisscom de l'administration des sites "teentalk" et "kidstalk" dans le courant de l'année 2009, puisque c'est par ce biais que nous parvenions la quasi-totalité des cas de ce type annoncés aux cantons. Par ailleurs, les nouvelles prérogatives du SCOCCI en termes d'investigation secrète (voir chapitre 9.2) dans les "chat" ont nécessité une phase de transition.

Enfin, la catégorie "autre", qui comporte toutes les autres annonces faites au SCOCCI et transmises aux autorités, est d'une grande stabilité au fil des années (cf. graphique 8). Dans cette catégorie, on retrouve notamment les annonces pour des sites pornographiques ne disposant pas d'un contrôle d'âge efficace permettant de limiter l'accès aux seuls adultes, mais également d'autres sites hébergés en Suisse et dont le contenu peut être pénalement répréhensible. C'est dans cette dernière catégorie que l'on retrouve également des annonces faites à d'autres services de la Confédération, et pas uniquement aux cantons.

Les polices zurichoises (ville et canton) restent les destinataires les plus fréquents des dossiers de suspicion du SCOCCI (cf. graphique 9). On trouve ensuite les polices cantonales vaudoises, argoviennes puis bernoises. Par ailleurs, 22 dossiers ont été envoyés à d'autres services de la Confédération, notamment le Commissariat Pédophilie et pornographie de la Police judiciaire fédérale, Swissmedic, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani) ou la Commission des loteries et paris (Comlot).



Graphique 9: Nombre de dossiers transmis en Suisse et au Liechtenstein, par destinataire (au total: 299)

Outre ces cas transmis aux autorités suisses, 231 URL ont été annoncés à l'étranger. Il s'agit quasi exclusivement de sites proposant du contenu à caractère pédopornographique ayant été signalé par le biais du formulaire online du SCOCCI.

## 7. Feedback des cantons

Parallèlement à l'envoi de dossiers de suspicion d'infraction aux cantons (chapitre 5), 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. Sur l'ensemble des dossiers envoyés par le SCOCI, près de 90 % ont été à l'origine d'une perquisition de la police cantonale. Dans plus de 80 % des cas, ces dernières ont permis de saisir du matériel illégal. Enfin, les feedback reçus par les autorités judiciaires des cantons nous informent que dans près de 90 % des cas, une condamnation a été prononcée à l'issue de la procédure. Ces résultats sont révélateurs de la qualité élevée des dossiers de suspicion fournis par le SCOCI.

## 8. Groupes de travail

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 2010 encore, le SCOCI a continué à s'engager dans le groupe de travail "Kindsmisbrauch" (Abus sur les enfants), en collaboration avec le Commissariat Pédophilie et pornographie, et auquel participent des organisations non gouvernementales, des cantons et la Prévention suisse de la criminalité.

Le SCOCI est par ailleurs représenté dans le programme national "Protection de la jeunesse face aux médias et compétences médiatiques", 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. Sur le même type de problématiques, le SCOCI a participé à la rédaction du rapport du Conseil fédéral sur le cyberintimidation, faisant suite à un postulat déposé par la conseillère nationale Barbara Schmid-Federer. Le rapport a été publié le 2 juin 2010 et est disponible sur le site de fedpol.

Le SCOCI a également participé à l'élaboration du concept "Sécurité et confiance", coordonné par l'Office fédéral de la communication (OFCOM). Ce dernier présente différentes mesures visant à favoriser une utilisation des technologies de l'information et de la communication vigilante et conforme au droit.

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

## 9. Projets

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

Le blocage de sites connus de pornographie enfantine par le "child sexual abuse anti-distribution filter" est véritablement effectif depuis 2007. Les blocages sont dirigés contre les contenus pédopornographiques hébergés à l'étranger.

### 9.2 Investigation secrète

La clarification de la situation juridique et des tâches du commissariat dans le cadre des investigations secrètes, rendue nécessaire par l'entrée en vigueur du nouveau code de procédure pénale au 1<sup>er</sup> janvier 2011, a nécessité un engagement tout particulier de la part du SCOCl au cours de l'année écoulée.

Depuis le 1<sup>er</sup> janvier 2011, la plupart des polices cantonales n'ont plus le droit de mener d'enquêtes sous couverture contre les pédocriminels sur Internet de manière préventive et sans soupçon d'infraction. Cela résulte de l'entrée en vigueur du nouveau code de procédure pénale suisse et du fait que la majorité des règlements de polices cantonaux ne prévoient pas ce genre d'intervention policière. Jusqu'ici, la base légale des enquêtes sous couverture à but préventif était contenue dans la loi fédérale sur l'investigation secrète (LFIS), qui a été abrogée avec l'entrée en vigueur du nouveau code de procédure pénale suisse.

Certains cantons, comme Schwyz, Uri et Obwald, ont pris conscience du besoin d'agir, et ont adapté leur loi sur la police cantonale au 1<sup>er</sup> janvier 2011. De son côté, le DFJP a, avec la Conférence des directrices et directeurs des départements cantonaux de justice et police, proposé une solution qui permet au SCOCl de continuer à mener cette activité d'investigation secrète. Grâce à un accord avec le canton de Schwyz, le SCOCl est dorénavant autorisé à investiguer de manière préventive et de surveiller les sites de dialogue en direct. Le travail du SCOCl dans ce domaine s'appuie sur la loi sur la police du canton de Schwyz, de même que sur un accord avec le tribunal des mesures de contrainte de ce même canton. Cette solution permet d'empêcher que les pédocriminels n'évoluent sans contrôle sur Internet.

# 10. Interventions parlementaires au niveau fédéral

Les interventions parlementaires suivantes ont été déposées en 2010:

## Protection de la jeunesse

- Initiative cantonale BE: Protection des enfants et des adolescents contre la violence dans les médias
- Initiative Schmid-Federer: Accroître l'efficacité de la protection de la jeunesse face aux médias et de la lutte contre la criminalité sur Internet
- Interpellation Amherd: Protection de la jeunesse et médias. Comment poursuivre au-delà des programmes de prévention
- Motion Bischofberger: Internet. Renforcer la protection des jeunes et la lutte contre la cybercriminalité
- Motion Schweiger: Apprendre aux jeunes à utiliser les nouveaux médias de façon responsable
- Question Graber: Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels
- Question Schmid-Federer: Surveillance des forums de discussion (chatrooms)
- Motion Amherd: Résolution de l'ONU pour lutter contre la pédopornographie sur l'internet
- Interpellation Markwalder: Accroître l'efficacité dans le domaine de la protection de la jeunesse face aux médias et des compétences médiatiques
- Motion Amherd: Protection des jeunes face aux médias. Création d'un centre de compétences national sur les médias électroniques
- Motion Amherd: Certification de sites web
- Postulat Amherd: Base constitutionnelle pour la création d'un organe suisse qui contrôlera la certification des sites web

## Investigation secrète

- Initiative Schluer: Recherches secrètes dans le but de prévenir les crimes
- Motion Fiala: Investigation secrète
- Question Baumann: Lutte contre les pédophiles sur Internet
- Question Rickli: Investigations secrètes contre les pédophiles
- Question Schmid-Federer: Investigation secrète sur Internet
- Question Schmid-Federer: Investigation secrète. Article 286a CPP

## Sphère privée

- Interpellation Hiltbold: Protection des personnes photographiées ou filmées et diffusion non consentie
- Postulat Graber: Atteintes à la sphère privée et menaces indirectes sur les libertés individuelles
- Postulat Hodgers: Adapter la loi sur la protection des données aux nouvelles technologies



## **Cyberguerre**

- Motion Büchler: Protection contre les cyberattaques
- Postulat Recordon: Evaluation de la menace de cyberguerre
- Postulat Büchler: Compléter le rapport sur la politique de sécurité en y ajoutant un chapitre sur la cyberguerre

## **Cyberintimidation**

- Postulat Schmid-Federer: Lutte contre le mobbing et la cyberintimidation. Instituer un préposé fédéral

## **Cybercriminalité en général**

- Question Büchler: Cybercriminalité
- Postulat commission des affaires juridiques CE : Identification des auteurs d'actes de cybercriminalité
- Motion Barthassat: Pour une plus grande maîtrise de la technologie en faveur de la sécurité
- Motion Barthassat: Relever la durée de conservation des journaux d'attribution d'adresses IP
- Postulat Darbellay: Elaboration d'une stratégie visant à protéger l'infrastructure numérique de la Suisse
- Postulat groupe libéral radical: Organe de direction et de coordination pour contrer les cybermenaces

## **Autres**

- Initiative cantonale ZG: Interdiction des jeux vidéo violents
- Interpellation Mörgeli: Charges financières élevées imposées par le DFJP aux fournisseurs d'accès à Internet privés
- Interpellation Parmelin: Danger de la contrefaçon et du trafic des médicaments
- Interpellation Rickli: Switch. Questions en suspens et baisse de prix pour les noms de domaines
- Interpellation Schmid-Federer: Scoci/Melani. Bilan de la réorganisation du SAP
- Postulat Savary: La Suisse a-t-elle besoin d'une loi contre le téléchargement illégal de musique?
- Question Graber: Affaire Wikileaks. Implications pour la Suisse et attitude du Conseil fédéral
- Question Rickli: Switch
- Motion Darbellay: SCOCI. Doublement de l'effectif et clarification du mandat et de la structure organisationnelle
- Initiative Schmid-Federer: Créer l'infraction pénale de la violation de domicile par des moyens informatiques

# 11. Médias, enseignement et conférences

## 11.1 Présence médiatique

Cette année encore, les représentants du SCOCI ont été régulièrement sollicités par différents médias afin de donner leur avis ou d'apporter leur expertise sur différentes problématiques en lien avec la criminalité sur Internet. En particulier, la question de la lutte contre la cyberintimidation, et celle de l'investigation secrète ont fait l'objet d'une couverture médiatique importante. Ces interventions ont également régulièrement donné l'occasion au SCOCI de se présenter et d'expliquer son action.

## 11.2 Enseignement et conférences

En 2010, des collaborateurs du SCOCI ont participé ou sont intervenus lors des conférences, réunions internationales et cours suivants:

### En Suisse:

- Journée Suisse des enquêteurs TI
- Intervention dans le cadre du MAS Forensics, haute école de Lucerne
- Intervention dans le cadre des cours de l'Ecole de police d'Europe centrale (EPEC)
- Tweakfest 2010
- Table ronde du Democratical Control of Armed Forces (DCAF) sur la cybercriminalité et la cybersécurité

### A l'étranger:

- RIPE NCC Meeting, Londres
- Octopus Interface, Strasbourg
- E-crime Congress, Londres

## **12. Partenariats et contacts**

### **12.1 Collaboration avec d'autres services de la Confédération**

Dans le cadre de ses activités, le SCOCI est amené à collaborer avec de nombreux autres services de Confédération. Cet aspect reflète la variété des problématiques traitées par le SCOCI. Au niveau de la Police judiciaire fédérale, le SCOCI collabore régulièrement avec le Commissariat Pédophilie et pornographie, pour tout ce qui est des affaires de pédopornographie, ainsi qu'avec le Commissariat Investigations secrètes, pour la problématique des enquêtes sous couverture sur Internet. Bien entendu, d'autres commissariats sont consultés selon les cas spécifiques traités par le SCOCI.

Des contacts et collaborations avec d'autres unités de la Confédération ont également eu lieu au cours de l'année écoulée. Citons notamment la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), le Domaine Entraide judiciaire internationale de l'Office fédéral de la justice, l'Office fédéral de la communication (OFCOM), le Secrétariat d'Etat à l'économie (SECO), Swissmedic ou la Commission des loteries et paris (Comlot).

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

Au cours de l'année 2010, les membres du SCOCI ont rencontré des représentants de divers corps de police cantonaux, ainsi que des juges d'instructions cantonaux. Il s'agissait notamment de visites ou alors de rencontres dans le cadre de projets bien spécifiques. Ils ont également rencontré la Landespolizei du Liechtenstein (LAPO) dans le cadre de leur échange annuel d'expériences.

### **12.3 Visites extérieures**

Le SCOCI a également reçu plusieurs visites extérieures durant l'année 2010. Ce type d'évènements souligne l'intérêt suscité par les activités du SCOCI et donne l'occasion à l'équipe de présenter son travail et de sensibiliser aux problématiques et enjeux qui y sont liées. Le SCOCI a notamment reçu les visites de plusieurs conseillers nationaux, de la cheffe du département (la conseillère fédérale Eveline Widmer-Schlumpf), mais également de nombreux journalistes. L'équipe a également reçu la visite de la directrice d'Action innocence (AIG), ONG avec laquelle le SCOCI collabore de longue date dans le cadre de la lutte contre la pédopornographie sur Internet.

### **12.4 Collaboration internationale opérationnelle**

En plus des conférences évoquées plus haut, les collaborateurs du SCOCI ont eu l'occasion de collaborer avec leurs homologues étrangers dans d'autres contextes plus opérationnels, notamment dans des projets concrets ou des groupes de travail.

Par ailleurs, le SCOCI était également représenté au groupe de travail de la "European Financial Coalition" à Bruxelles.

## 13. Glossaire

<b>Adult check</b>	Procédé permettant de limiter l'accès d'un site web à un public majeur uniquement.
<b>Chat</b>	Dialogue en direct.
<b>Cloud Computing</b>	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.
<b>Cyberintimidation</b>	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".
<b>One-click hosting</b>	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.
<b>Peer to peer</b>	Modèle de réseau informatique permettant l'échange de fichiers entre utilisateurs (les pairs).
<b>Phishing</b>	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.
<b>Pornographie dure</b>	Actes d'ordre sexuel avec des enfants (pédophilie, pédopornographie), avec des animaux, des excréments humains, ou comprenant des actes de violence.
<b>Proxy</b>	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).
<b>Redirect service</b>	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).
<b>Spam</b>	Communication électronique non sollicitée, principalement effectuée en masse et à des fins publicitaires, ou parfois dans le but d'installer un logiciel malveillant.
<b>Streaming</b>	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").
<b>URL</b>	Uniform Resource Locator, chaîne de caractère utilisée pour adresser les ressources du Web. Il s'agit de l'adresse Web.
<b>Valeur « hash »</b>	Valeur unique permettant d'identifier une donnée (notamment une image).

## 14. Tendances 2010

Un des enseignements de l'année écoulée pour le SCOCI est l'augmentation des annonces pour des cas de pédopornographie. Il s'agit là de la confirmation d'une tendance observée l'année dernière déjà. Les supports à disposition pour publier des contenus pédopornographiques sur Internet sont multiples, et leur utilisation évolue rapidement. Ainsi certains vecteurs peuvent-ils être abandonnés au profit d'autres, en particulier lorsque le monitoring de la police se focalise sur l'un d'entre eux. Les communautés d'utilisateurs, permettant de créer des groupes fermés, sont notamment un des nouveaux visages que prend l'échange de matériel pédopornographique sur Internet.

La multiplication des annonces d'utilisateurs victimes d'arnaques ou de tentatives d'arnaque est également particulièrement préoccupante. De nouveaux modus operandi apparaissent, mais des arnaques plus basiques et connues sont également toujours en cours. Les escrocs savent notamment jouer des frontières géographiques, qui rendent l'activité des autorités de poursuite complexe. Cet aspect souligne l'importance d'une meilleure coopération internationale dans ce domaine, mais nous rappelle également que face à des escrocs parfois insaisissables, la prévention reste un outil majeur. En observant des règles élémentaires de prudence, il est la plupart du temps possible d'éviter de se retrouver en position de victime. Notons enfin que les escrocs savent notamment utiliser les informations mises à disposition par l'utilisateur lui-même.

L'année 2010 a également vu l'activité de monitoring des réseaux peer-to-peer se renforcer. Cet outil reste primordial pour le SCOCI, aussi bien dans la volonté de réprimer les consommateurs de pédopornographie sur Internet, que par sa fonction préventive, qui vise à assurer une présence sur ce type de réseau et éviter qu'un sentiment d'impunité ne se propage parmi les criminels. En accord avec ce qui précède, et afin de s'adapter aux évolutions constatées dans les pratiques de ces derniers une extension de l'outil à d'autres réseaux est d'ailleurs en cours.

Les difficultés constatées pour identifier les personnes se connectant à Internet par le biais de téléphones mobiles sont actuellement discutées dans le cadre de la révision de loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT). Ainsi, la LSCPT va être adaptée en fonction des évolutions technologiques, pour désormais couvrir Internet dans son ensemble, donc également les communications par e-mail et la téléphonie par Internet.