KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

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

Rapport annuel 2007

TABLES DES MATIERES

1. L'essentiel en bref

- La cinquième année de service du SCOCI a été marquée par une nette augmentation des communications émanant de la population. Le SCOCI a accompli en 2007 un énorme travail de tri portant sur plus de 10 000 communications reçues et a affirmé son rôle d'interlocuteur national en matière de criminalité sur Internet. En 2007, il a transmis 734 cas, y compris ceux issus de ses propres recherches, aux autorités de poursuite pénale suisses et étrangères.

- Cette nette augmentation du nombre de communications est due à une forte hausse des cas relevant de la criminalité économique. Depuis mai 2007, la Suisse, tout comme d'autres pays européens précédemment, a été à plusieurs reprises la cible d'actes de cybercriminalité d'envergure internationale. Les instituts financiers ont été submergés de spams qui ont permis l'installation de maliciels sur de nombreux ordinateurs suisses.

- Les communications de la population étaient avant tout liées à la pornographie dure (19,91 %). Comme en 2006, les communications ont souvent été transmises suite à la réception de spams. Un grand nombre de communications n'ont pas pu être vérifiées car les sites incriminés n'étaient plus disponibles au moment de l'analyse automatique, ce qui indique que les milieux criminels se montrent toujours plus dynamiques.

- Les dossiers élaborés par le SCOCI ont permis, cette année également, d'obtenir des taux de réussite élevés. Ils semblent constituer une base fiable pour ouvrir une procédure pénale contre des suspects et saisir du matériel illégal lors de perquisitions, permettant ainsi en règle générale la condamnation des suspects.

- Les feedback des autorités de poursuite pénale indiquent toutefois que les auteurs tentent de plus en plus souvent de cacher du matériel illégal sur des ordinateurs ou de le supprimer. Dans presque 10 % des cas, ils ont utilisé des logiciels de cryptage ou des programmes permettant un effacement irréversible des données.

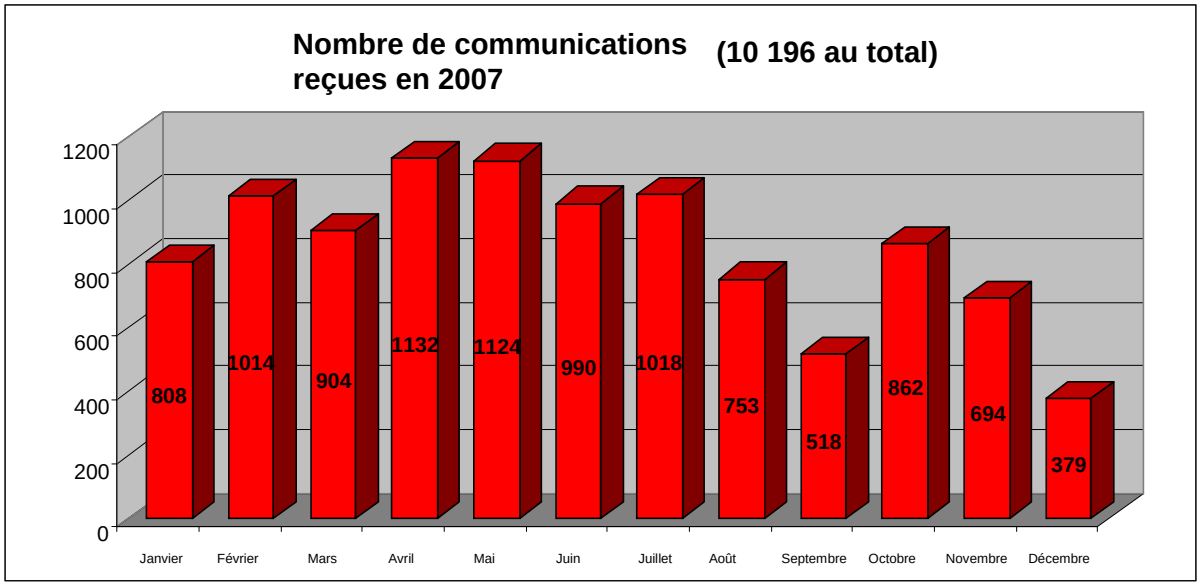
- Dans plus d'une centaine de cas, le SCOCI a directement signalé aux fournisseurs les sites illégaux, qui ont été retirés de la Toile grâce aux communications du SCOCI.

- La direction du SCOCI tire un bilan positif de ces cinq dernières années et est convaincu qu'en tant que centre de compétence national le SCOCI possède les instruments nécessaires pour faire face aux défis du futur.

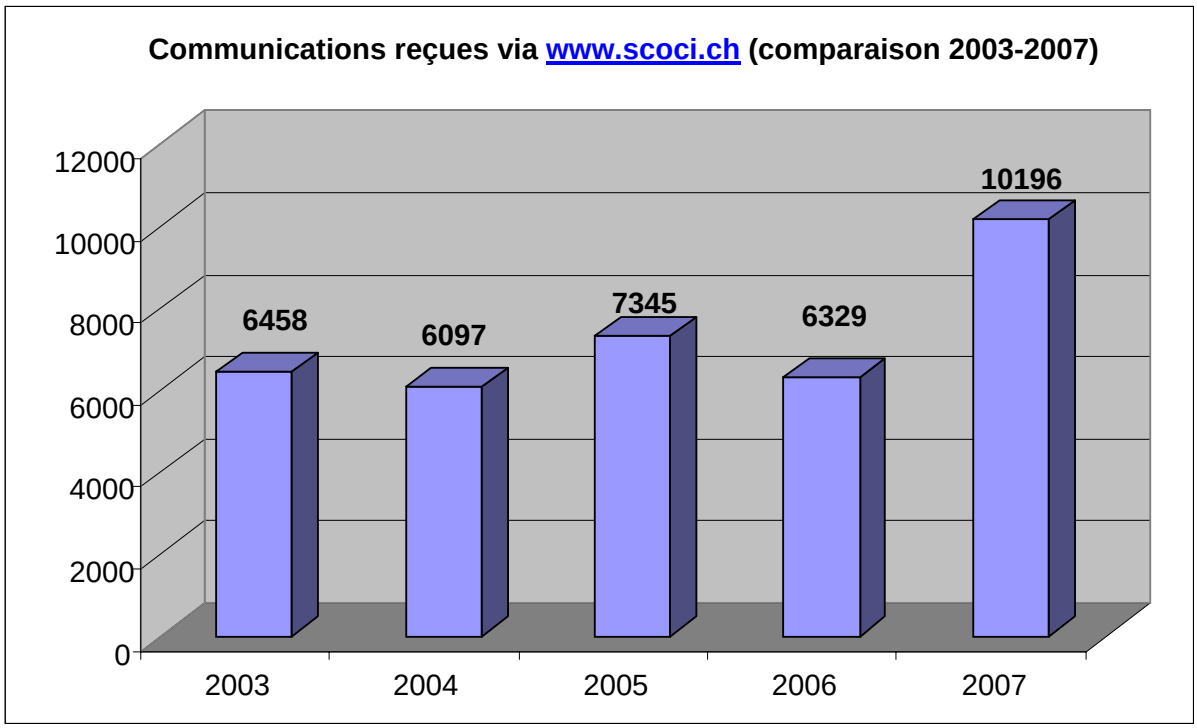
2. Nombre de communications reçues

En 2007, le SCOCI a reçu environ 10 100 communications de soupçons. L'augmentation du nombre d'infractions dans le domaine de la criminalité économique a entraîné une hausse de plus de 3000 communications par rapport à l'année précédente. Il s'agit en général d'attaques de spams avec des chevaux de Troie contre des banques suisses, que les victimes ont immédiatement signalées au SCOCI.

Graphique 1 Communications reçues via www.scoci.ch



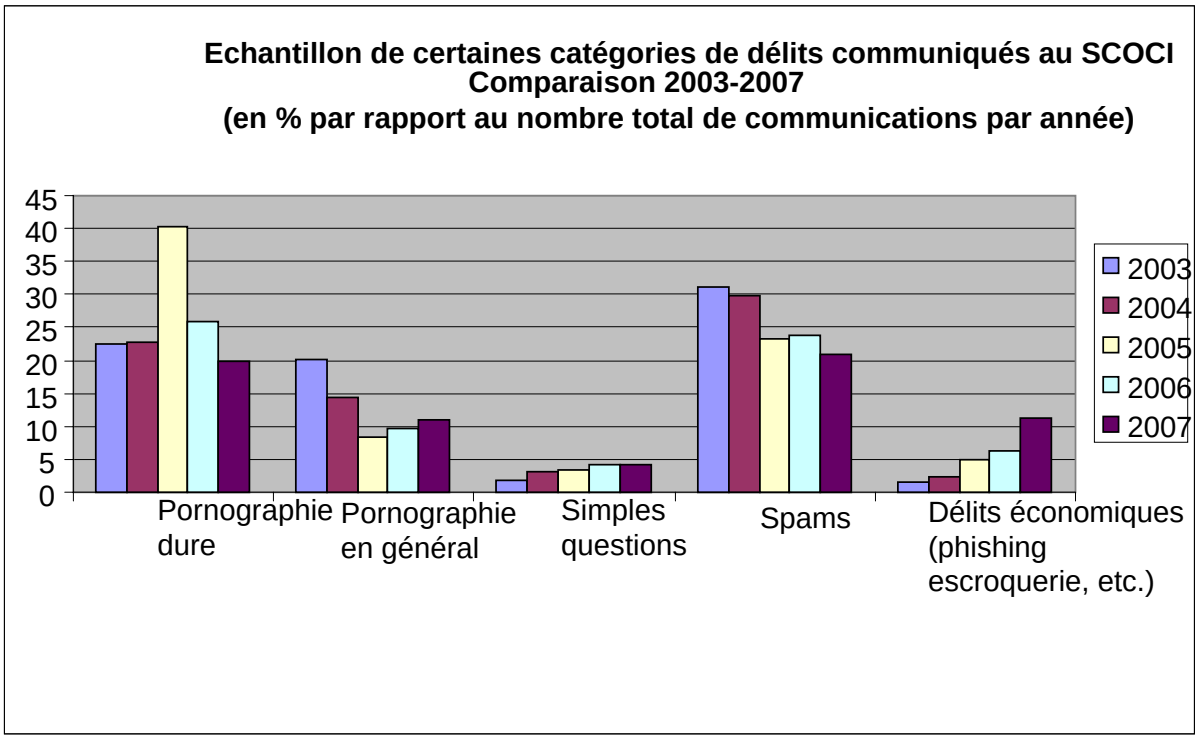
Graphique 2 Communications reçues via www.scoci.ch (comparaison sur cinq ans)



3. Types d'infractions enregistrées

Les tendances constatées au cours des dernières années se sont confirmées en 2007. Le graphique 3 montre que la catégorie des délits économiques est en constante augmentation depuis cinq ans. Les communications les plus fréquentes dans ce domaine concernent le phishing, la fraude à la commission et les offres gratuites frauduleuses. Ce phénomène s'explique notamment par le fait que l'appât du gain a conduit bon nombre de personnes à ne plus programmer des maliciels uniquement par "amusement", mais également pour gagner de l'argent. En outre, on constate que les instruments utilisés et les logiciels sont toujours plus professionnels, ce qui signifie que la technique – et par conséquent les résultats – ont été affinés et améliorés et qu'ils ne nécessitent plus la participation active de l'utilisateur. Toutefois, les cas requérant encore la participation active de l'utilisateur s'accompagnent d'une professionnalisation toujours plus grande, notamment dans les intentions visant à tromper.

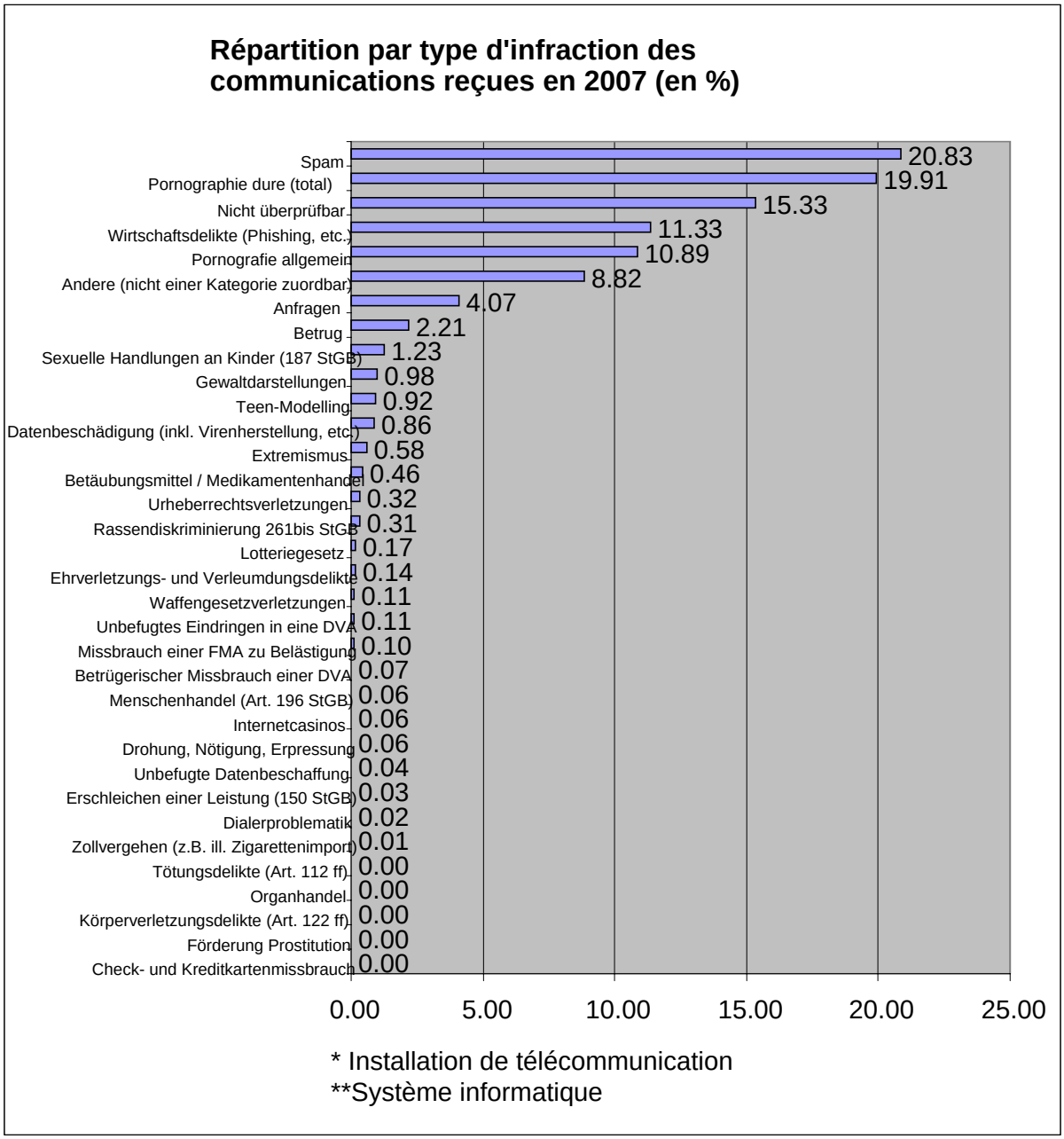
Graphique 3 Comparaison de certaines catégories sur cinq ans



C'est dans le domaine de la pornographie dure, et notamment de la pornographie enfantine, que le nombre de communications est le plus élevé. La catégorie "Non vérifiables" est également importante. En effet, certaines communications ne peuvent pas être vérifiées car les adresses URL transmises ne sont plus actives au moment de l'analyse automatique. Cela est en particulier dû au fait qu'un grand nombre de sites présentant un contenu illégal (notamment de la pornographie enfantine) sont hébergés auprès de fournisseurs d'accès gratuits. Lorsque l'adresse URL est identifiée par les autorités, l'administrateur la supprime immédiatement. L'auteur a toutefois déjà diffusé des copies de la page incriminée sur l'ensemble de la Toile, qui sont ensuite activées les unes après les autres. Cette constatation indique entre autres

que la méthode dite du "serveur à l'épreuve des balles" (bulletproof hosting)[1] n'est pas encore trop employée pour diffuser des contenus de pornographie enfantine.

Graphique 4 Teneur des communications adressées au SCOCI par la population

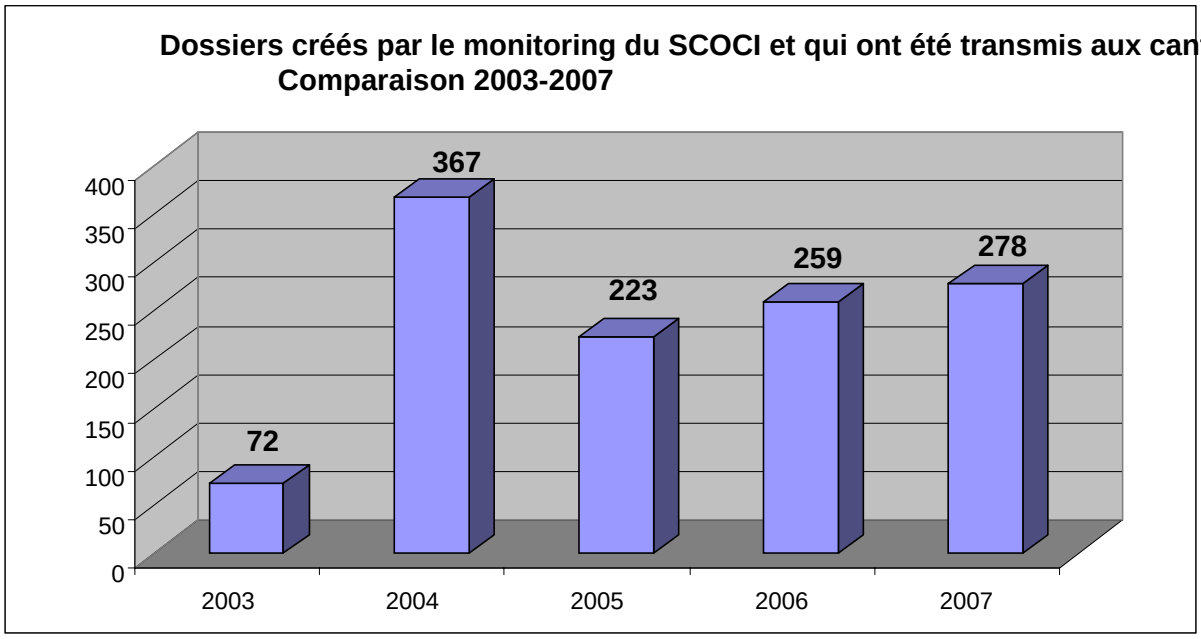


[1] La méthode "bulletproof" consiste à enregistrer et à rendre accessibles des contenus sur Internet de sorte à empêcher ou à compliquer le travail des autorités de poursuite pénale.

4. Recherche active (monitoring)

En plus des 88 dossiers créés dans le cadre du traitement des cas annoncés par le public, le SCOCI a pu identifier 278 cas de soupçons par ses propres recherches faites dans les réseaux P2P, les chats et les forums, avant de les transmettre aux autorités de poursuite pénale. Comme défini par le comité directeur dans son mandat, il s'agit toujours de cas de possession réitérée et de diffusion présumée de pornographie enfantine.

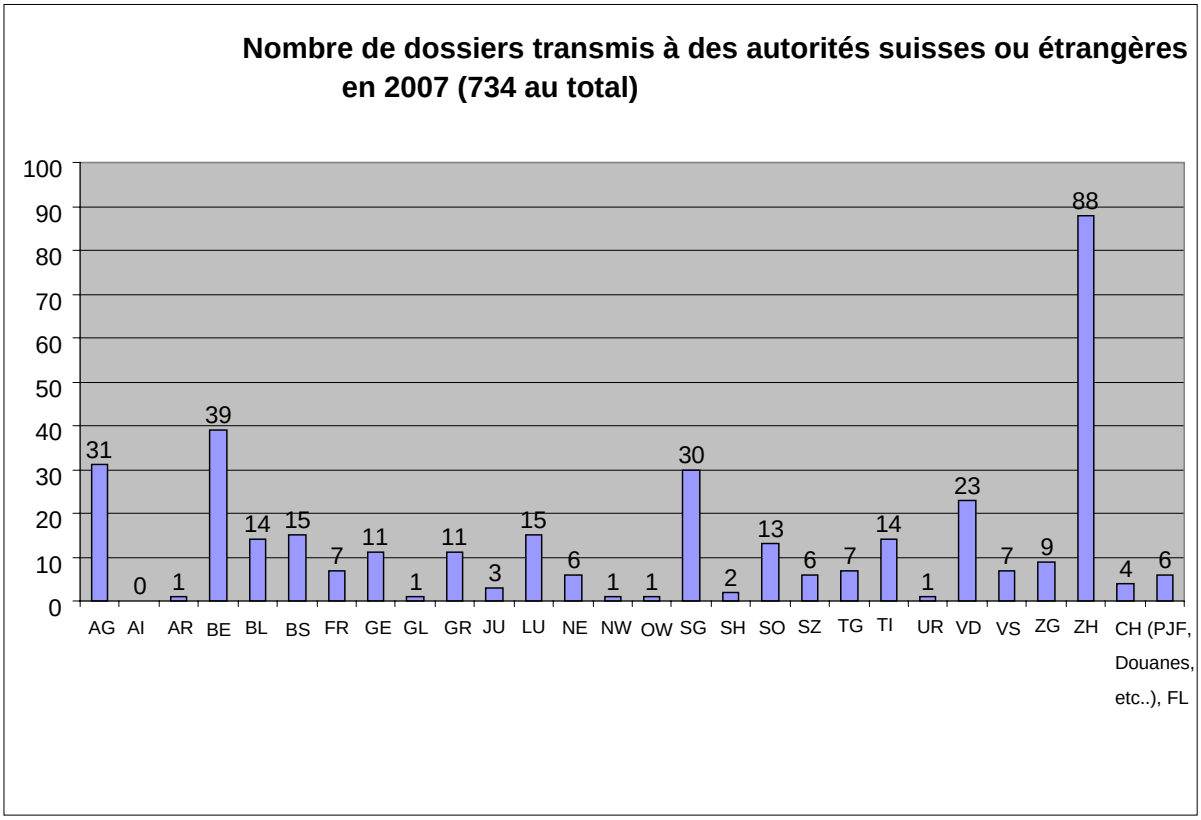
Graphique 5 Dossiers créés suite à des recherches actives



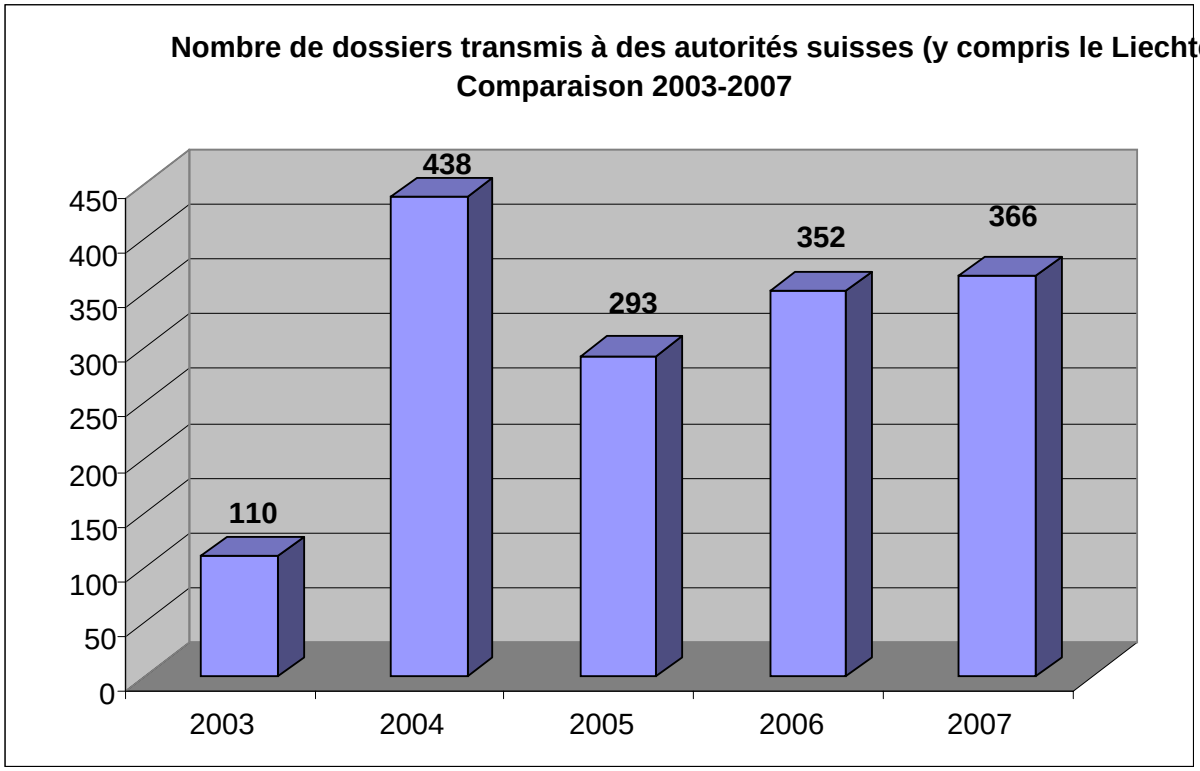
5. Destinataires des dossiers

A l'exception du canton d'Appenzell Rhodes-Intérieures, tous les cantons suisses ont reçu des dossiers de la part du SCOCI. De manière générale, la conclusion suivante peut être tirée: plus le nombre de personnes consultant Internet est élevé, plus il y a de dossiers.
Le SCOCI a transmis un total de 368 dossiers aux services de police étrangers (avant tout aux Etats-Unis et à la Russie) par l'intermédiaire d'Interpol.

Graphiques 6 Nombre de dossiers transmis



Graphiques 7 Nombre de dossiers transmis



6. Travail de prévention

En 2007, le SCOCI s'est également engagé dans le domaine de la prévention. Il a continué à collaborer étroitement avec la Prévention suisse de la criminalité (PSC) dans le cadre de la campagne "Stop à la pornographie enfantine" menée à l'échelle nationale. Le SCOCI est par ailleurs l'un des partenaires de Microsoft Suisse dans le programme de prévention "La sécurité des jeunes en ligne" (Security for kids). Les collaborateurs du SCOCI ont en outre présenté l'année dernière divers exposés sur le thème de la prévention à l'occasion de conférences des maîtres, de rencontres d'associations de parents et d'organisations de protection de l'enfance.

7. Interventions parlementaires au niveau fédéral

Les interventions parlementaires suivantes ont été déposées en 2007:

07.3449 Motion Amherd

Rendre punissables les abus virtuels commis sur des enfants par le biais d'Internet: dans cette motion, il est demandé au Conseil fédéral de rendre punissables les abus virtuels commis sur des enfants, tout comme le fait de préparer la voie à une conversation à caractère incontestablement sexuel entre un enfant et une personne ayant manifestement atteint l'âge adulte. Dans des mondes virtuels comme "Second Life", il y a des joueurs qui commettent des abus sur des enfants virtuels et qui vont jusqu'à les violer. Il faut inscrire dans la législation qu'il s'agit là d'une offre relevant de la pornographie enfantine qui constitue un acte punissable.

Dans sa réponse du 28.09.2007 le Conseil fédéral indique que la motion porte sur deux objets qui doivent être traités séparément: a) les abus virtuels commis sur des enfants, b) l'établissement d'une conversation à caractère sexuel entre un adulte et un enfant.
a) Le Conseil fédéral soutient les visées de la motion, qui sont de lutter efficacement contre la pornographie enfantine. Toutefois, l'article 197 du code pénal s'applique non seulement aux représentations réelles mais aussi aux représentations virtuelles, si bien qu'il n'existe de prime abord aucune nécessité de légiférer sur les mondes virtuels.
Le Conseil fédéral est néanmoins prêt à étudier en détail les questions qui se posent et à proposer, si besoin est, une modification adéquate du code pénal.
b) Le deuxième point abordé par la motion ("préparer la voie à une conversation à caractère incontestablement sexuel" avec un enfant sur Internet) se réfère manifestement à ce que l'on appelle le "grooming". Le grooming - ou mise en confiance - consiste à mener avec un enfant un dialogue sur Internet au cours duquel une rencontre est proposée dans le but de commettre des actes sexuels punissables.
Plusieurs Etats ont modifié leur législation de sorte qu'il suffise, pour être passible d'une sanction, de proposer à un enfant, au cours d'une conversation à caractère sexuel sur Internet, une rencontre en vue de commettre des actes sexuels.
Il paraît judicieux d'examiner si la Suisse doit elle aussi adopter une réglementation légale sur le "grooming".
Le Conseil fédéral soutient la motion, mais il se réserve de soumettre la nécessité de légiférer à un examen minutieux et de proposer éventuellement aux Chambres fédérales de renoncer à compléter le code pénal.

07.3627 Motion Glanzmann-Hunkeler

Enregistrement obligatoire des cartes d'accès sans fil à prépaiement: dans cette motion, il est demandé au Conseil fédéral de proposer une loi prévoyant l'enregistrement obligatoire des cartes d'accès sans fil à prépaiement. La loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et les ordonnances pertinentes seront adaptées de manière à obliger l'usager à s'identifier, même sur les réseaux privés. On devra notamment pouvoir déterminer les ordinateurs connectés à ces réseaux.
Etat des délibérations: le Conseil fédéral propose d'accepter la motion; non encore traité au conseil.

07.3628 Motion Glanzmann-Hunkeler

Poursuites plus efficaces des cas de pédophilie sur Internet: dans cette motion, il est demandé au Conseil fédéral de veiller à ce que, dans les cas de pédophilie relevant de la coopération internationale, l'Office fédéral de la police communique directement les informations relatives aux suspects. Les cantons mobilisent suffisamment de ressources pour garantir le traitement des cas de pédophilie.
Etat des délibérations: non encore traité au conseil.

07.3629 Motion Glanzmann-Hunkeler

Convention sur la cybercriminalité: dans cette motion, il est demandé au Conseil fédéral d'entamer sans tarder la procédure de ratification de la Convention du Conseil de l'Europe sur la cybercriminalité, en souffrance depuis longtemps.
La motionnaire motive sa demande en indiquant qu'il est souvent très difficile d'identifier les auteurs d'actes délictueux commis par le biais d'Internet. On ne peut poursui-

vre efficacement et rapidement les auteurs de ces délits qu'en accélérant les procédures et en préservant à temps les indices, ce qu'interdit l'entraide judiciaire actuelle, trop lente et trop formaliste. Dans le contexte international, une ratification de la Convention sur la cybercriminalité garantirait un appui simple et rapide à la préservation des indices.
Etat des délibérations: non encore traité au conseil.

07.3509 Motion Büchler

Sécurité juridique pour les fournisseurs de prestations sur Internet: dans cette motion, il est demandé au Conseil fédéral d'orienter l'élaboration du projet consacré à la cybercriminalité de telle sorte que la sécurité juridique des fournisseurs de prestations sur Internet soit garantie en droit civil. Pour ce faire, il s'inspirera des législations édictées par l'Europe et par les Etats-Unis. Le projet doit créer une totale sécurité pour les investissements, tout en favorisant l'innovation. Le Conseil fédéral est chargé de présenter un projet en la matière au Parlement en 2008.
Etat des délibérations: non encore traité au conseil.

07.3510 Motion Büchler

Cybercriminalité. Combler les lacunes du droit pénal: dans cette motion, il est demandé au Conseil fédéral de présenter au Parlement, en 2008, un projet de loi sur la cybercriminalité qui comblera les lacunes que présente le droit pénal. Le motionnaire demande notamment une réponse concernant les résultats de la consultation et le message.
Etat des délibérations: non encore traité au conseil.

07.3689 Motion Büchler

Cybercriminalité: dans cette motion, il est demandé au Conseil fédéral de proposer une modification de la loi qui attribue globalement la compétence en matière de cybercriminalité aux autorités d'enquête fédérales lorsqu'Internet est essentiel à la commission du délit et que

- le délit a de fortes ramifications à l'étranger, ou que
- des victimes sont concernées dans plusieurs cantons.

Etat des délibérations: non encore traité au conseil.

07.3750 Motion Büchler

Cybercriminalité. Davantage de spécialistes auprès des autorités d'enquête de la Confédération: dans cette motion, il est demandé au Conseil fédéral de doter les autorités d'enquête fédérales d'une division qui, dans leur domaine de compétences, poursuivront avec efficacité et célérité les délits relevant de la cybercriminalité.
Etat des délibérations: non encore traité au conseil.

07.3751 Motion Büchler

Lutte contre le terrorisme: dans cette motion, il est demandé au Conseil fédéral de confier à l'Office fédéral de la police, qu'il dotera des moyens nécessaires, le mandat de rechercher sur Internet des informations sur le terrorisme, la traite d'êtres humains, la prolifération d'armes, la criminalité organisée et l'espionnage. Une attention particulière sera portée aux sites djihadistes dont les pages et celles des milieux extrémistes violents seront supprimées des serveurs suisses.

Etat des délibérations: non encore traité au conseil.

Les interventions parlementaires suivantes ont été traitées par le conseil ou les commissions juridiques pendant l'année sous revue:

06.3170 Motion Schweiger

Cybercriminalité. Protection des enfants: le Conseil fédéral est chargé de prendre les mesures qui s'imposent afin de lutter plus efficacement contre la cybercriminalité qui touche les enfants. Il devra notamment: 1) préparer une modification de l'art. 197, al. 3bis, CP, visant à rendre punissable la consommation intentionnelle de pornographie dure; 2) préparer une modification de l'art. 15, al. 3, LSCPT, visant à prolonger la conservation obligatoire des fichiers-journaux de six à douze mois et à punir de manière appropriée l'inobservation de cette disposition; 3) établir un catalogue d'infractions commun incluant le nouvel art. 197, al. 3bis, CP, applicable également aux art. 4 LFIS et 3 LSCPT; 4) élaborer un plan d'action visant à sécuriser les pages web auquel les fournisseurs et les hébergeurs participeront.
Dans sa déclaration du 24.05.2006, le Conseil fédéral propose d'accepter le point 1 de la motion, ainsi que d'accepter partiellement le point 2, pour ce qui est de l'élaboration d'une norme pénale réprimant spécifiquement l'inobservation de l'obligation de conserver les données accessoires. Il propose en outre de rejeter les points 3 et 4 de la motion, ainsi que de rejeter partiellement le point 2, pour ce qui est de la prolongation de la durée de conservation des données accessoires.
Depuis lors, la motion a été adoptée par le Conseil des Etats et la Commission des affaires juridiques du Conseil national a procédé à son examen préalable. La commission propose, à l'unanimité, d'adopter la motion en modifiant en simple mandat d'examen les mesures visées aux chiffres 3 et 4.

06.3554 Motion Hochreutener

Extension de la motion Schweiger à la représentation de la violence: il est demandé au Conseil fédéral d'étendre les mesures prises en vertu de la motion Schweiger 06.3170 (Cybercriminalité. Protection des enfants) concernant les infractions pénales prévues à l'article 197 CP aux infractions pénales au sens de l'article 135 CP (représentation de la violence).
La motion a été adoptée le 20 décembre 2006 par le Conseil national. Réunie le 5 novembre 2007, la Commission des affaires juridiques du Conseil des Etats a procédé à l'examen préalable de la motion et propose, sans opposition, de l'adopter.

8. Médias, enseignement et publications

8.1 Echo médiatique

Comme les années précédentes, le SCOCI a généralement rencontré un écho positif auprès des médias. De nombreux articles de presse et plusieurs articles publiés dans les médias électroniques ont également mis en lumière le travail du bureau de coordination.
Le SCOCI était représenté à égalité dans les médias de toutes les régions linguistiques, ce qui suggère qu'il est bien connu du public.

8.2 Enseignement

En 2007, des collaborateurs du SCOCI ont participé à titre d'intervenants aux colloques et aux cours suivants:

- enseignement dispensé dans le cadre du cours "Cybercops" de la Haute école de gestion de Lucerne
- enseignement dispensé dans le cadre des études postgrade en lutte contre la criminalité économique de la Haute école de gestion de Lucerne
- enseignement dispensé dans le cadre des études postgrade forensiques de la Haute école de gestion de Lucerne
- Journée nationale des Enquêteurs IT
- Journée du Parquet de Winterthur
- Dangers pour les enfants sur Internet, PDC Morat
- Pro Familia Suisse – familles et médias – chances et risques
- Autorité de tutelle de Bâle-Ville, réseau de protection de l'enfance, les jeunes en ligne – quand et comment les enfants et les jeunes sont-ils menacés?

8.3 Analyses juridiques

- Chat – Développement et état actuel de la jurisprudence (analyse et présentation des positions)

- Analyse détaillée de la plate-forme "Second Life" avant la prise de position sur la motion Amherd (07.3449)

9. Partenariats et contacts du SCOCI

9.1 Echange d'expériences et de connaissances avec l'Autriche

Deux enquêteurs du bureau de communication en matière de pornographie enfantine sur Internet de la Police judiciaire fédérale autrichienne sont venus à Berne au cours de l'été 2007 afin d'échanger des expériences et d'intensifier la coopération avec les collaborateurs du SCOCI. Dans le cadre des discussions, les méthodes d'enquête liées à la recherche de contenus relevant de la pornographie enfantine sur le réseau P2P leur ont été présentées. En août, le ministère autrichien de l'Intérieur a demandé par courrier le soutien du SCOCI pour l'installation, l'utilisation et la maintenance de ce logiciel modifié spécialement par le SCOCI. Deux collaborateurs du SCOCI se sont ainsi rendus à Vienne en novembre dernier, où ils ont accompli les tâches suivantes:

- installation du logiciel modifié par le SCOCI aux fins de recherches sur le réseau P2P;
- installation du filtre des adresses IP (grâce auquel les réponses ne portent que sur des fournisseurs d'accès autrichiens) élaboré par le SCOCI;
- formation pour l'utilisation et la maintenance du logiciel.

9.2. Collaboration avec des fournisseurs de services de télécommunication concernant le filtre mis en place pour lutter contre les abus commis envers les enfants

Le blocage de sites Internet connus de pornographie enfantine, appelé filtre contre les abus commis envers des enfants, est entré officiellement en fonction en 2007. Actuellement, dix fournisseurs suisses participent volontairement et bloquent l'accès aux sites Internet commerciaux de pornographie enfantine.
Les blocages sont dirigés contre les fournisseurs de contenus relevant de la pornographie enfantine à l'étranger. La liste des sites à supprimer est mise à jour au niveau international. Le SCOCI examine en plus chaque site mentionné du point de vue de la situation juridique particulière de la Suisse.

9.3 Séances de travail et échange d'expériences

Dans le courant de l'année 2007, les membres du SCOCI ont rencontré des représentants des corps de police cantonaux (visite de ou à la police cantonale VS, BS, BL, GE, et police municipale de ZH)

Une séance de travail sur le thème du "chat" a été organisée avec un fournisseur suisse. Par ailleurs des contacts directs ont pu être établis avec un registrar[2] sis en Suisse, ainsi qu'avec un grand fournisseur de places de mémoire externe (« online storage »).

10. Tendances

10.1 Criminalité économique

La criminalité économique est un domaine qui a connu, au cours des cinq dernières années, un développement constant et fait l'objet d'un nombre croissant de communications. En 2007, des attaques au moyen de maliciels (programme malveillant) ont été menées pour la première fois en Suisse contre des instituts financiers suisses, dans le but d'infecter les ordinateurs des clients des banques et d'effectuer des virements en leur nom. Au vu de l'efficacité de cette forme de criminalité, il est possible que les réseaux criminels améliorent ce mode opératoire au cours des prochaines années et qu'il devienne l'un de leurs moyens de prédilection.

10.2 Réseaux de zombies et serveurs corrompus

Par réseaux de zombies, on entend l'ensemble des ordinateurs infectés par un maliciel, qui sont reliés en réseau et utilisés à grande échelle pour mener des actes criminels. Les attaques dites DDoS (Distributed Denial of Service) sont notamment me-

[2] Un registrar est une société ou une association permettant le dépôt de noms de domaine Internet. Les registrars sont accrédités par l'autorité de régulation de l'Internet ICANN (Internet Corporation for Assigned Names and Numbers) ou par un registre d'un nom de domaine.

nées par le biais de réseaux de zombies. En Suisse, les premières attaques de ce type ont été constatées l'année dernière: qu'il s'agisse d'un petit site Internet ou d'un grand fournisseur, tous les services liés à Internet peuvent être la cible d'attaques DDoS.
Ces activités n'en sont qu'à leurs débuts et continueront à se développer. En raison de la vulnérabilité des 'infrastructures sensibles qui dépendent de réseaux informatiques, il est donc impératif de vérifier et d'améliorer en conséquence les processus liés à la sécurité des informations. Par l'entremise de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), la Suisse a déjà mis en place des mesures importantes dans ce domaine – comparativement à d'autres pays au niveau international.
Un autre type d'activité criminelle est également en pleine évolution, qui vise à compromettre des serveurs Internet dans le but d'infecter les ordinateurs des internautes sans qu'ils ne s'en doutent. Cette méthode, aussi connue sous le nom d'infection par "drive-by download", est actuellement très efficace et sans cesse améliorée.

Für den Leitungsausschuss KOBIK

Urs von Daeniken

Für KOBIK

Philipp Kronig