Rapport d'activité 2003

Service de coordination de la lutte contre la criminalité sur Internet

SCOCI

Résumé

Un an après son entrée en fonction, le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) est à même de présenter un bilan positif de son action:

- **Le Service de coordination a entamé ses activités dans les délais prévus. Tous les postes sont pourvus. Les processus de travail au niveau interne fonctionnent bien et une assistance technique efficace est fournie par le matériel et le logiciel informatiques (hardware et software). Toutefois, des mesures de rationalisation devront être apportées dans les secteurs d'activités qui se recoupent au sein de fedpol.**

- **Désormais reconnu au niveau national comme la cellule de contact en matière de cybercriminalité, le Service de coordination devra continuer à mettre tout particulièrement l'accent sur l'information du public.**

- **La majorité des communications se rapportent à des faits n'ayant aucun lien avec la Suisse. Le SCOCI décharge ainsi les cantons de laborieuses opérations de tri.**

- **Les moyens actuellement disponibles permettent de traiter avec une grande efficacité les communications de soupçons reçues, relativement nombreuses en comparaison internationale (500 à 600 par mois).**

- **Le « patrouillage » actif sur Internet entraîne de nombreuses investigations supplémentaires (environ les trois-quarts des communications de soupçons proviennent du monitoring). Malgré des moyens modestes, les taux de découverte sont nettement plus élevés qu'en Allemagne par exemple.**

- **Plus de 100 communications ont été transmises par le SCOCI aux cantons qui ont presque tous poursuivi le traitement des dossiers.**

- **L'analyse des directives émanant des autorités de poursuite pénale montre que les autorités cantonales de poursuite pénale ont pu résoudre la plupart des cas avec leur propre personnel et disposaient à cet égard des connaissances nécessaires.**

- **Un renfort modéré de personnel dans le domaine du monitoring (p. ex. par le biais d'une collaboration avec le canton de Zurich) serait souhaitable et permettrait d'accroître encore le taux de découverte des infractions.**

1. Introduction

Conformément au règlement interne approuvé par le comité directeur, un rapport d'activité doit être établi chaque année sur l'année civile précédente.

Ce premier rapport d'activité retrace brièvement l'historique du SCOCI, présente le comité directeur ainsi que la mise sur pied de l'équipe SCOCI. Il comprend par ailleurs des données statistiques, accompagnées de commentaires, sur les communications et le monitoring. Le rapport présente aussi deux études de cas choisis pour leur représentativité et, pour terminer, fait état des perspectives pour l'année à venir.

2. Brève rétrospective et historique

En juin 2000, la Conférence des commandants des polices cantonales de Suisse (CCPCS) a constitué un groupe de travail intercantonal[1] (BEMIK) chargé de procéder à un examen approfondi des qualifications et des conditions cadres d'une cellule nationale de monitoring et de formuler des propositions concrètes. Face aux besoins urgents en matière de coordination policière, le GT BEMIK a proposé une série de mesures concrètes et recommandé à l'unanimité la mise sur pied d'un service national de coordination en matière de cybercriminalité.

S'appuyant sur les recommandations du GT BEMIK, le Département fédéral de justice et police (DFJP) et la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) ont décidé de lutter conjointement contre la criminalité sur Internet. Le mandat, l'organisation et le financement d'un service national de coordination ont été définis dans le cadre d'un arrangement administratif.

Le comité et le plénum de la CCDJP se sont prononcés à l'unanimité pour la mise en oeuvre de l'arrangement administratif. Par lettre du 4 février 2002, le président de la CCDJP a invité les cantons à inscrire les montants nécessaires à leur budget 2003. Tous les cantons, à l'exception du canton de Zurich, ont par la suite confirmé leur participation au projet.

Pour sa part, le 20 février 2002, le Conseil fédéral a réaffirmé son intention de mettre sur pied avec les cantons, à compter du 1er janvier 2003, un centre national de coordination afin de lutter plus efficacement contre la cybercriminalité (SCOCI). La création de trois nouveaux postes au sein de l'Office fédéral de la police a été approuvée à cet effet.

Fin novembre, fedpol a remis une estimation détaillée des coûts au secrétariat de la CCDJP. Les cantons, pour leur part, ont reçu de celui-ci un calcul des coûts distinct.

3. Le SCOCI débute le 1er janvier 2003

Le 1er janvier 2003, donc dans les délais prévus, le SCOCI a entamé ses activités par la publication sur Internet d'un formulaire d'annonce en quatre langues.

Outre-ce formulaire, le site <http://www.cybercrime.admin.ch/> fournit des informations de base sur le SCOCI et sur la cybercriminalité en général. La présence sur la Toile permet surtout de réagir rapidement à des besoins spécifiques d'information du public, comme des informations générales et les règles de comportement concernant le multipostage abusif (le *spamming*[2]), les restrictions d'accès en fonction de l'âge[3] et les programmes *dialer*[4]. Au cours de l'année, ces priorités ont été modifiées en fonction de l'analyse des communications reçues.

4. Comité directeur

La conduite stratégique du service de coordination est assurée par un comité directeur paritaire composé de trois membres, le représentant de la Commission COSE de la CCDJP, Andreas Keller, le représentant de la CAPS, Jean Treccani et le représentant de la direction de fedpol, Urs von Däniken.

Le comité directeur du SCOCI s'est réuni pour la première fois le 4 mai 2003 dans les locaux de fedpol, à la Bolligenstrasse, à Berne. Cette rencontre fut l'occasion de concrétiser le mandat fondamental figurant dans l'arrangement administratif, de présenter l'équipe du SCOCI, d'adopter le règlement interne ainsi que de fixer les priorités thématiques pour l'année en cours.

Le comité directeur a décidé que le SCOCI accorderait la priorité tout spécialement à la lutte contre la pornographie enfantine et en général aux représentations de la violence.

Le directeur de fedpol a remis la conduite opérationnelle du service de coordination à Philipp Kronig. Le responsable opérationnel du SCOCI est chargé de mettre en œuvre les priorités et les stratégies établies par le comité directeur, de garantir la coordination au sein de l'équipe du SCOCI, d'assurer la transmission d'informations au comité directeur et aux cantons, de représenter le service de coordination vis-à-vis de l'extérieur ainsi que de rédiger un rapport d'activité annuel à l'intention du comité directeur.

Le comité directeur a souhaité en outre que l'esprit d'équipe soit encouragé parmi les nouveaux collaborateurs du SCOCI. Dans cette optique, des rencontres régulières ont été organisées; elles se sont avérées fructueuses. Par ailleurs, étant donné l'éloignement géographique des collaborateurs et les différentes modalités organisationnelles des équipes, ces rencontres sont absolument indispensables à une harmonisation de leurs activités.

5. Application CLEMONA[5]

Relativement peu doté en personnel, le service de coordination doit être soutenu dans l'accomplissement de ses tâches par une infrastructure technologique efficace. Là aussi, le SCOCI a emprunté la voie de l'innovation par rapport aux services similaires étrangers.

L'application CLEMONA a été mise au point dans le cadre d'un projet informatique urgent, pour les besoins spécifiques du SCOCI. Cette application permet un premier traitement automatisé des communications entrantes éclaircissements, saisie des données, regroupement des communications en double et la gestion des opérations y compris le contrôle des activités. La réception des communications est automatisée et le système permet en outre la gestion des documents et une transmission directe des données aux autorités compétentes.

CLEMONA décharge donc le service de coordination d'une multitude de tâches de routine, notamment le domaine du monitoring qui peut ainsi concentrer la quasi totalité de ses capacités à la recherche de contenus illégaux sur Internet sans être retardé par des recherches préliminaires fastidieuses et répétitives sur les communications entrantes.

6. Personnel / Organisation

Suivant l'étude préliminaire de fedpol, quelque neuf postes avaient été estimés nécessaires à la mise sur pied et à l'exploitation du nouveau service de coordination. L'impasse financière provoquée par le désistement du canton de Zurich a eu pour conséquence une réduction des postes à huit.

6.1 Recrutement

L'équipe SCOCI est composée entre autres de techniciens réseau, de spécialistes en matière de protocoles Internet et de sécurité des informations, ainsi que de juristes, de policiers et d'analystes criminels. Ces collaborateurs viennent de Suisse romande (NE, FR), de Suisse alémanique (BE, ZH, SG) et du Tessin. Grâce à la diversité de leurs profils respectifs, les collaborateurs sélectionnés ont permis de couvrir tous les critères recherchés. Aucun départ n'a été enregistré jusqu'ici.

6.2 Formation des collaborateurs

Dans le domaine du *monitoring*, l'accent a été tout particulièrement mis sur la formation technique des collaborateurs pour leur permettre de suivre l'évolution rapide de la technologie Internet. Il s'est essentiellement de cours sur l'administration, sur la configuration et l'installation de systèmes Linux[6] et de serveurs web, ainsi que sur les langages de programmation et de script.

En matière de *clearing*, la priorité a été accordée aux questions actuelles relatives au commerce électronique et au droit lié à l'Internet. Les collaborateurs ont également eu l'occasion de visiter des postes de police, élargissant ainsi leurs connaissances

pratiques et d'approfondir leurs connaissances de l'Internet (structure des réseaux, etc.) grâce aux cours d'informatique.

Enfin, étant donné la diversité des tâches dans ce domaine, la formation en matière d'*analyse* a couvert une palette très diversifiée d'activités et de thèmes, comme les conférences sur le droit et l'Internet ou encore les symposiums consacrés à la criminalité sur Internet et à la guerre de l'information[7].

6.3 Organisation

L'intégration des trois domaines principaux du SCOCI au sein de l'Office fédéral de la police a permis d'éviter la création de postes supplémentaires pour les tâches de conduite et de support. En outre, les nombreuses synergies ainsi créées ont pu être exploitées, notamment dans les domaines de l'analyse et du monitoring.

L'attribution – décidée par le comité directeur – de la conduite de SCOCI à un responsable s'est avérée très positive. Cette uniformisation de la conduite opérationnelle devra être renforcée l'an prochain.

Par ailleurs, la collaboration avec la Police judiciaire fédérale (coordination et enquêtes dans le domaine de la technologie de l'information - enquêtes TI) devra encore être renforcée.

7. Interventions publiques, présentations du SCOCI, présence médiatique du SCOCI (y compris le bilan semestriel)

7.1 Présence médiatique

En qualité de service national de coordination et de réception des annonces, le SCOCI se doit d'être très présent dans les médias.

Les débuts du SCOCI ont rencontré un large écho auprès des médias, tout particulièrement des médias électroniques et de la presse spécialisée dans les techniques de l'information. Divers articles de fond et interviews ont ensuite permis d'en donner une image plus complète et lui ont assuré ainsi une présence médiatique régulière. Au terme de ses six premiers mois d'activité, un communiqué de presse a permis de faire état de ses acquis.

7.2 Interventions publiques, Présentation du SCOCI

Des contacts ont tout d'abord été noués avec les fournisseurs de services Internet ainsi qu'avec des entreprises TI (SIMSA[8], SWINOG[9], Internet Society, Luzerner Tagung für Informationssicherung, AVANTEC[10], OSS[11] et Internet Security Services), auprès desquels le SCOCI s'est présenté. Une collaboration exempte de préjugés, surtout avec les professionnels de la branche TI, est en effet indispensable à la bonne marche des activités du SCOCI.

D'autres présentations ont permis d'informer les autorités de poursuite pénale au titre de futurs "clients" du SCOCI (par ex. Société suisse de droit pénal, Conférence des commandants des polices cantonales et municipales de Suisse, Conférences des

enquêteurs spécialisés en technologie de l'information, cours pour cyberflics, diplôme postgrade sur la cybercriminalité, Conférence des juges suisses, cours postgrade en criminalité économique). En outre, diverses autorités cantonales de poursuite pénale ont été informées sur le SCOCI dans leurs propres locaux.

Au niveau politique, une présentation a été effectuée en décembre à l'intention des parlementaires et une autre à l'intention des collaborateurs du Secrétariat général du DFJP.

7.3 Collaboration avec les OGN

Le SCOCI a conseillé diverses organisations non gouvernementales (ONG) dans l'organisation de leurs campagnes de prévention et participé à des conférences et panels d'experts. Le service de coordination est également représenté au sein du groupe de travail interdisciplinaire « Organisations non gouvernementales – Autorités de poursuite pénale ». Bien qu'il n'ait pas organisé ses propres campagnes, le SCOCI contribue à la prévention en veillant à la mise à jour permanente des informations qu'il fournit sur son site Internet.

8. Collaboration avec les cantons

Un bilan très positif peut être tiré de la collaboration avec les représentants des autorités cantonales de police. Les enquêteurs des corps de police des cantons d'AG, BE, ZH, VD, SO, TI, SG et GR ont répondu à l'invitation qui leur avait été faite et ont rendu visite « en personne » au SCOCI à Berne. Outre de fructueux échanges d'informations, cette rencontre leur ont permis de nouer de bons contacts personnels. Pour sa part, l'équipe de clearing du SCOCI s'est rendue dans les locaux de la police municipale zurichoise.

D'une manière générale, les cas de soupçons transmis par le SCOCI aux cantons ont rencontré un écho très positif, notamment parce qu'il s'agissait de cas actuels qui constituaient de « véritables » soupçons et dont le traitement pouvait être aisément poursuivi en raison de leur actualité.

Jusqu'ici, deux cas seulement n'ont pas été suivis de mesures d'enquêtes.

Indispensable au quotidien, le contact permanent et surtout personnel entre le SCOCI et les enquêteurs cantonaux spécialisés en technologie de l'information est un facteur de confiance. Relevons à ce propos que les prestations du SCOCI sont appréciées et reconnues.

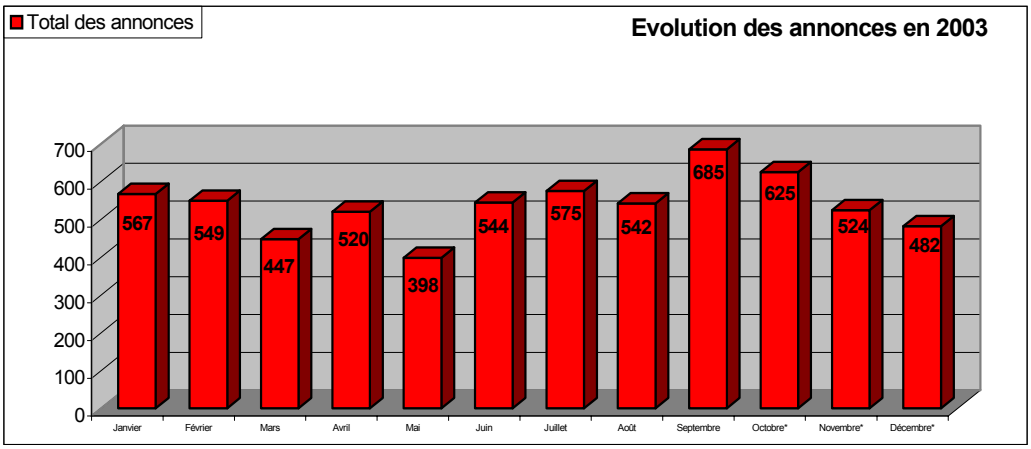
Enfin, l'échange actif d'informations a permis au SCOCI d'améliorer ses prestations et de les adapter aux nécessités cantonales.

9. Vue d'ensemble des données statistiques et bref commentaire

6457 communications ont été enregistrées au cours de cette première année. Présentant une fréquence étonnamment constante, elles ont pu être traitées sans retard.

9.1 Communications enregistrées

La présence médiatique active du SCOCI a manifestement influé sur le degré de notoriété du service, ainsi que sur le volume des communications dont le nombre a enregistré une hausse sensible en août, au terme de six mois d'activités.



9.2 Comparaison internationale

Il apparaît difficile de procéder à une comparaison des activités du SCOCI au niveau international. En effet, les chiffres concernant des services similaires ne sont que partiellement comparables. Néanmoins, une comparaison avec les services britanniques et allemands permet de situer approximativement le SCOCI.

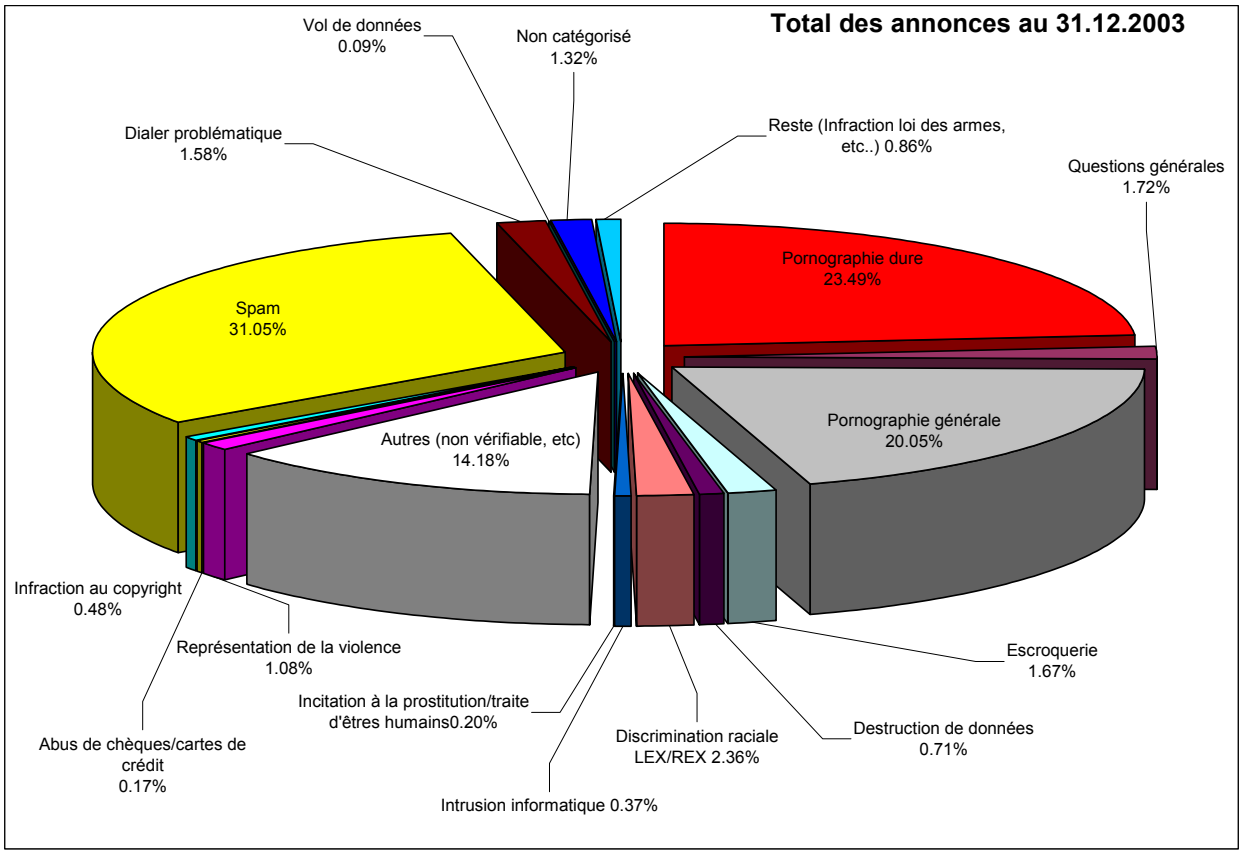
Volume des communications: en 2002, le portail commun du fournisseur de services Internet et des autorités de poursuite pénale britanniques ont enregistré 21 241 communications de soupçons. A titre comparatif, le SCOCI en a reçu à peine un tiers au cours de l'année 2003. Si l'on met en regard la « population Internet » suisse avec la population totale britannique, qui est 7 fois plus nombreuse, on constate avec étonnement que la propension à communiquer des cas de soupçons est deux fois plus élevée en Suisse.

Monitoring: pour ce qui est des cas pénalement répréhensibles transmis aux cantons, il est possible de procéder à une comparaison horizontale avec le service allemand «Zentralstelle für anlassunabhängige Recherchen in Datennetzen (ZaRD)». Contrairement aux collaborateurs du SCOCI, les quelque 20 collaborateurs du monitoring du ZaRD ne se consacrent pas exclusivement aux cas ayant un lien avec leur pays, mais dénoncent aussi des cas touchant l'étranger. En 2002, le ZaRD a enregistré 790 cas punissables en droit pénal. 23 pour cent environ, soit quelque 180 cas, concernaient l'Allemagne. Ce pays possède une « population Internet » d'environ 37 millions de personnes, alors qu'en Suisse, elle est d'environ 3,6 millions,

soit dix fois plus petite. En prenant pour base cette population Internet, le SCOCI présente donc - avec quelque 70 affaires - un taux d'enquête cinq fois plus élevé que le ZaRD. Ce fait est d'autant plus remarquable qu'avec ses quatre collaborateurs affectés à la recherche « hors soupçons », le Service de coordination dispose de beaucoup moins de contrôleurs Internet que le ZaRD qui emploie dans ce domaine une vingtaine de personnes.

9.3 Que contiennent les communications ?

Un grand nombre de communications portent sur des contenus à caractère pornographique, sur des cas de multipostage d'e-mails (spam) et des tentatives d'escroquerie. Les communications ayant trait à des contenus racistes, à des délits contre l'honneur, à des violations du droit d'auteur et à des virus ont également été relativement fréquentes.



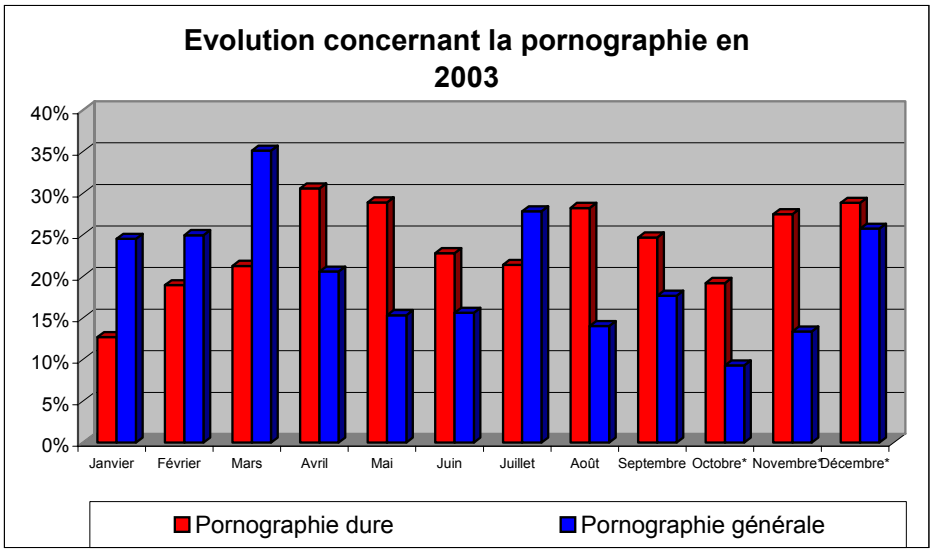
9.4 Correspondance avec les auteurs des communications

Le formulaire d'annonce a été souvent utilisé pour poser des questions concrètes au SCOCI. Il a été répondu personnellement à chaque question.

Lorsque la communication ne contenait pas de question particulière, l'expéditeur recevait un accusé de réception standard lui confirmant que son annonce était bien parvenue au Service de coordination et précisant son numéro d'ordre dans la gestion des documents.

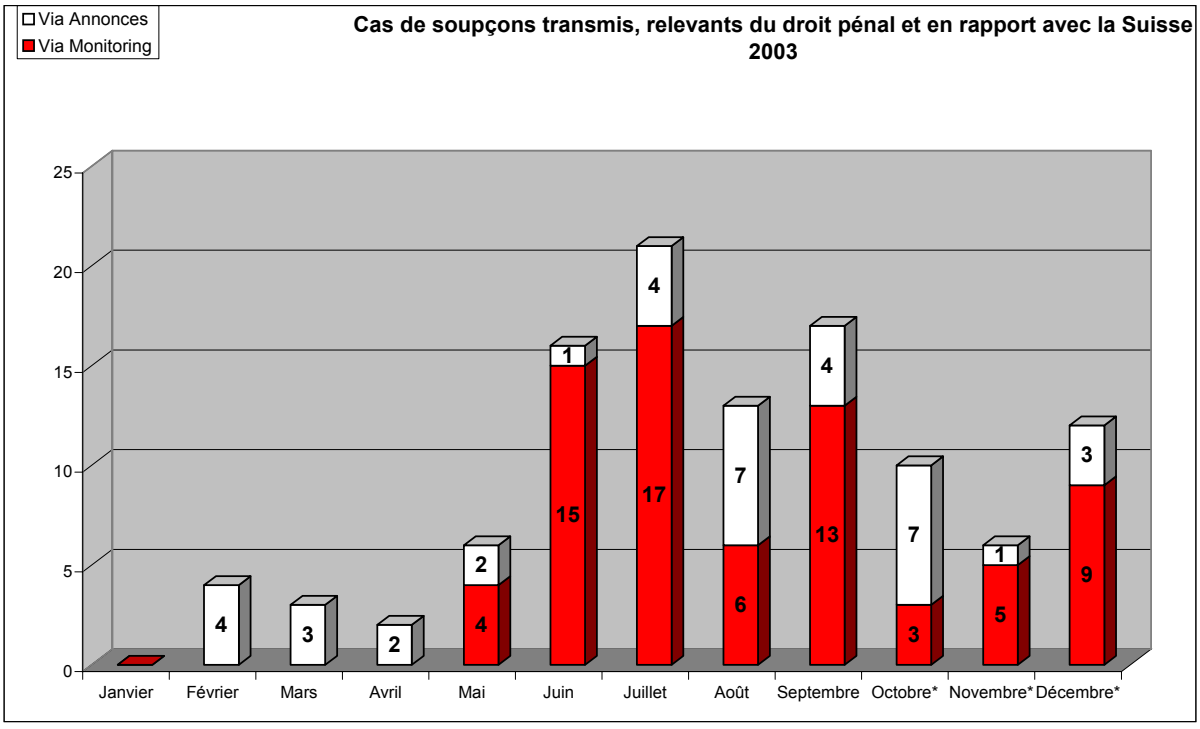
9.5 Déroulement des communications relatives à la pornographie en général ainsi qu'à la pornographie dure

La qualité des communications a surpris par rapport au projet-pilote de la Confédération. Le formulaire d'annonce, par exemple, a rarement été utilisé pour se manifester contre la pornographie légale présente sur Internet. Même les annonces « canulars » ont constitué l'exception absolue. Le Service de coordination s'efforce de fournir sur son site les informations nécessaires afin de prévenir comme il convient l'auteur de la communication de la portée légale de certains contenus. Il faudra encore attendre pour savoir si ces aides et explications ont une influence directe sur le comportement en matière de communications. Une tendance semble néanmoins se dessiner dans le domaine de la pornographie surtout: avec le temps, les personnes transmettant des communications font de mieux en mieux la différence entre la pornographie légale et illégale.



9.6 Monitoring

Dès mai 2003, le SCOCI a aussi recherché activement les contenus suspects sur Internet. Le Service de coordination n'agissait alors pas en tant que police mondiale du réseau, mais entendait limiter sa surveillance à des faits liés à la Suisse, en



mettant l'accent sur la lutte contre la pornographie enfantine, conformément au mandat qui lui avait été imparti.

Du fait de l'évolution rapide des technologies, il a fallu adapter de manière suivie la recherche active sur Internet aux nouvelles possibilités d'échange des données. Ainsi, en août et septembre, certains réseaux peer-to-peer (P2P)[12] ont été la cible d'actions menées au niveau international dans la lutte contre les copies illégales, ce qui s'est traduit par une modification du comportement d'une partie des utilisateurs. Le monitoring a dû réaménager ses moyens en conséquence afin de pouvoir continuer à détecter des contenus illégaux présentant un lien avec la Suisse – avec pour conséquence des variations mensuelles importantes des cas suspects découverts par monitoring.

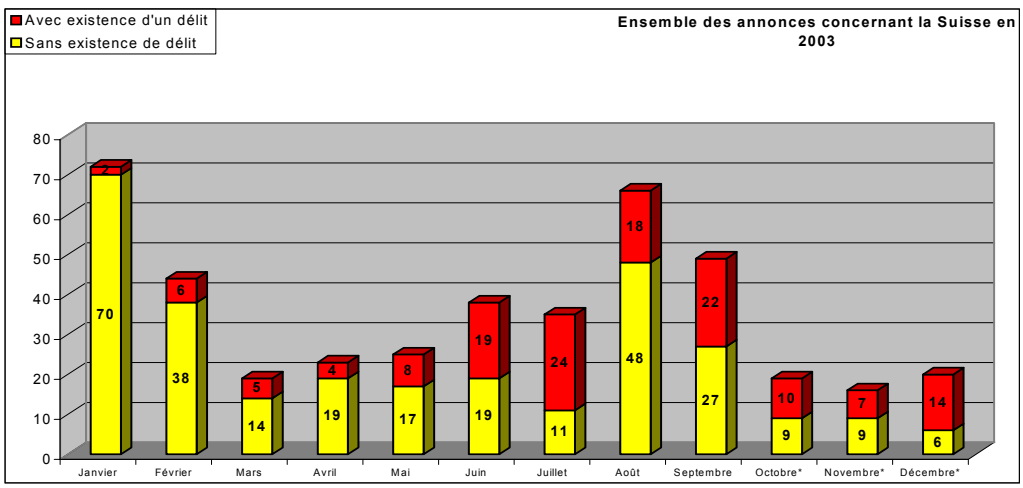
Parallèlement, les collaborateurs du monitoring du SCOCI ont développé les contacts avec les enquêteurs spécialisés dans les techniques de l'information en Suisse et à l'étranger afin d'intensifier les échanges.

À notre connaissance, les cantons ne pratiquent plus de monitoring actif depuis la mise en service du SCOCI.

9.7 Le lien des communications avec la Suisse

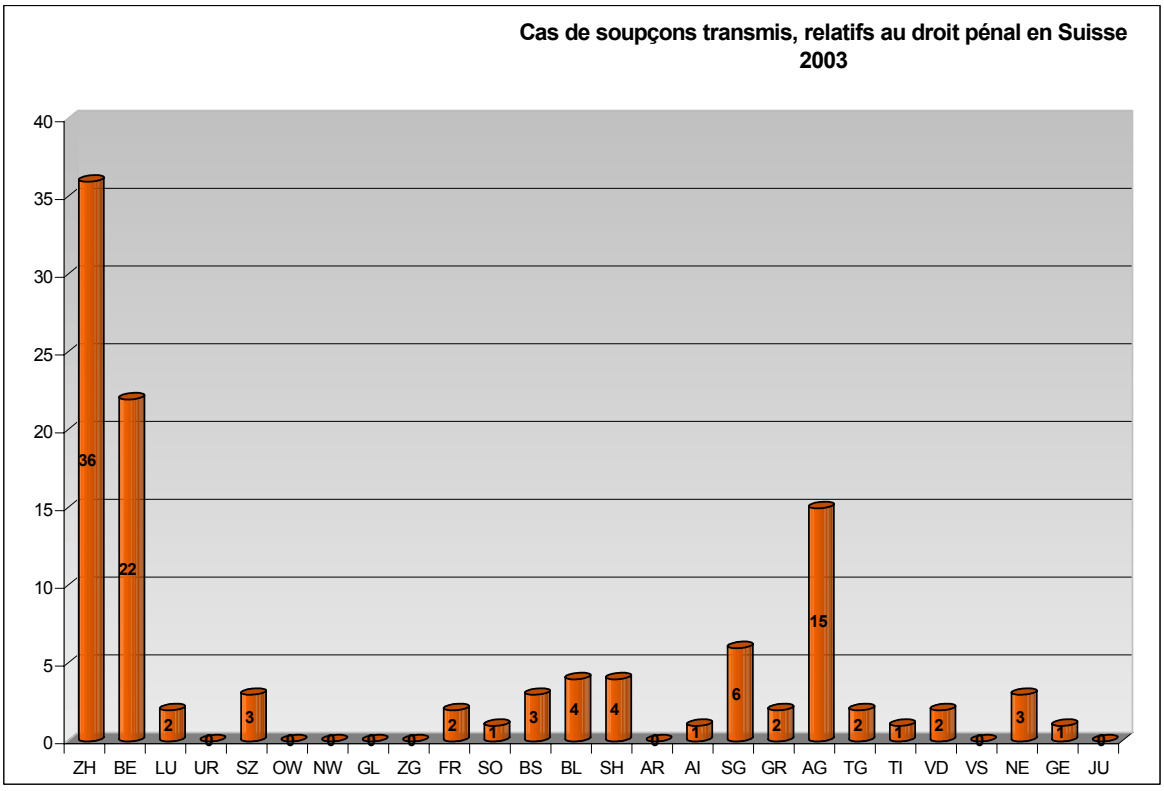
Conformément aux prévisions, la plupart des faits communiqués ne touchaient pas directement la Suisse. Ces communications ont donc été directement transmises aux autorités étrangères responsables sans autres investigations, à moins que les circonstances n'aient requis une conservation immédiate de la preuve. Les pays les plus concernés à ce propos ont été les Etats-Unis, suivis de la Russie et de l'Ukraine. Un cinquième des communications ayant un lien avec la Suisse étaient pertinentes en droit pénal. Ces dossiers, accompagnés des sauvegardes de données et d'un avis juridique, ont été transmis aux autorités cantonales compétentes de poursuite pénale.

Il convient de noter que la création du monitoring influe sur le rapport entre les communications ayant une importance pénale et celles qui ne le sont pas. La recherche active porte de manière ciblée sur les cas pertinents en droit pénal ayant un lien avec la Suisse, ce qui s'est traduit, au cours des derniers mois, par une nette augmentation des communications ayant une portée sur le plan pénal.



9.8 Répartition par canton des cas pertinents en droit pénal

Le clearing examine du point de vue juridique le contenu des cas communiqués et des cas issus de la recherche active sur Internet, qui sont ensuite transmis aux cantons compétents. En tout, plus de 100 communications de soupçons ont été transmises aux autorités cantonales de poursuite pénale. Aucune d'entre elles n'ont été jugées par les cantons comme étant incomplètes ou non pertinentes en droit pénal.



Ce sont les régions fortement urbanisées (Zurich, Berne, Argovie et St-Gall) qui ont reçu le plus grand nombre de communications de soupçons. Ce fait correspond également à la répartition des suspects établie par GENESIS[13] une année auparavant, opération au cours de laquelle les quatre cantons cités présentaient déjà le plus grand nombre de personnes suspectes. A ce propos, il convient de relever que dans les cantons de Zurich et d'Argovie surtout, le nombre de suspects par habitant était un peu plus élevé que la moyenne, cela dans les statistiques de GENESIS comme dans celles du SCOCI.

Enfin, bien que le canton de Zurich ne participe pas au Service de coordination, un tiers environ des communications ont été transmises à ses autorités de poursuite pénale. En effet, il est impossible d'exclure le canton de Zurich étant donné que la totalité de la population suisse peut transmettre ses communications anonymement et qu'en matière de monitoring, logiquement, le canton compétent ne mène son enquête sur les cas de soupçon qu'au cours d'une seconde phase.

10. Analyse de deux cas sélectionnés

L'analyse de tous les cas de soupçons enregistrés dépasserait largement le cadre du présent rapport d'activité et serait par ailleurs incomplète car la majorité des traitements sont encore en cours.

Il est néanmoins possible de tirer un certain nombre de conclusions:

- Il est apparu assez rapidement qu'un nombre considérable de communications de soupçons ont été transmises et notifiées aux autorités surtout grâce à l'anonymat offert par le formulaire d'annonce. Dans certains cas, les personnes transmettant les informations en question ont souligné expressément qu'elles désiraient demeurer dans cet anonymat et n'entendaient nullement contacter la police.
- La collaboration entre le service de coordination et les représentants des fournisseurs de services Internet (*Internet Service Provider, ISP*) s'est mise en place relativement vite et a abouti, dès les premiers mois, à des communications de soupçons exploitables, issues surtout de « sites de bavardage » (*chat lines*)[14] ; en l'occurrence, la collaboration avec les responsables du « *chat* » du fournisseur en question s'est révélée extrêmement utile.
- En matière de monitoring Internet, le contrôle du domaine du peer-to-peer est apparu plus facile et plus rationnel qu'on ne le pensait généralement. Néanmoins, à la fin de l'été, les utilisateurs des systèmes peer-to-peer ont apparemment appris à contourner le prétendu anonymat de certains programmes peer-to-peer. Peut-être cette circonspection croissante est-elle due aux actions très médiatisées de l'industrie musicale contre le piratage aux Etats-Unis? Il semble plus vraisemblable qu'un changement d'attitude général se dessine chez les utilisateurs de bourses d'échanges virtuelles vers plus de sécurité et d'anonymité.

Il convient fondamentalement de relever que toutes les communications de soupçon reçues par le SCOCI ont été traitées en l'espace de quelques jours seulement, ou de quelques semaines dans les affaires complexes. Cette durée de traitement est demeurée constante tout au long de l'année, bien qu'avec l'augmentation du nombre de cas et l'expérience, elle ait également diminué.

L'analyse des directives émanant des autorités de poursuite pénale montre que les autorités cantonales de poursuite pénale ont pu résoudre la plupart des cas avec leur propre personnel et qu'elles disposaient à cet égard des connaissances nécessaires.

Les deux cas présentés ci-dessous ont pour but d'illustrer les deux thèmes clés que sont les réseaux peer-to-peer et la pornographie enfantine.

10.1 Cas n° 1: pornographie enfantine

Le 22.5.2003, le SCOCI réceptionne la communication d'une femme qui avait reçu, peu de temps auparavant, un message électronique au contenu relevant de la pornographique enfantine. Ce message émanait d'une personne dont elle avait fait connaissance dans un *chat room*. La femme en question joignait également à sa communication un protocole du *chat* qui portait sur l'esclavage sexuel et, entre autres, sur les abus sexuels commis sur enfants.

Grâce à l'adresse IP[15] de l'interlocuteur du *chat*, le SCOCI a pu déterminer, auprès du fournisseur Internet compétent, le canton de domicile de l'homme et transmettre les moyens de preuve rassemblés aux autorités cantonales compétentes. Quelques semaines à peine après la réception de la communication, ces autorités ordonnèrent une perquisition au domicile du suspect chez qui elles découvrirent notamment quelque 70 000 photographies relevant de la pornographie dure.

Dans ce cas précis, le SCOCI a assumé pour la première fois les fonctions d'autorité de coordination en raison d'une situation juridique relativement claire. La femme dont émanait la communication n'habitait pas dans le même canton que le suspect. Ainsi, les premières démarches effectuées par le SCOCI dans cette affaire avaient permis de déterminer le canton compétent et de le prévenir, sans qu'il ait fallu contacter inutilement les autorités d'autres cantons (p. ex. le canton de la femme l'origine de la communication).

Celle-ci refusait, pour des raisons personnelles compréhensibles, de renoncer à l'anonymat et de déposer plainte auprès de la police. Le formulaire d'annonce était la seule possibilité pour elle de transmettre ses soupçons aux autorités.

10.2 Cas n° 2: P2P (réseau peer-to-peer)

Début mai, le service de coordination a créé le monitoring Internet en mettant tout particulièrement l'accent sur les réseaux P2P. Dans un premier temps, la recherche porte sur les fichiers illégaux qui sont mis à disposition par des utilisateurs disposant d'un numéro IP suisse. Après avoir sauvegardé ces éléments de preuve, le SCOCI détermine le canton où se trouve l'utilisateur P2P à l'aide du fournisseur d'accès Internet compétent. Il en va de même dans le cas présenté ici: le clearing effectua une première appréciation pénale des fichiers sauvegardés et les transmit à l'autorité de poursuite pénale du canton compétent. Lors de l'audition, le suspect prétendit ignorer quelles données étaient téléchargées sur son ordinateur. Il ajouta qu'il n'avait recherché intentionnellement ni films ni photographies relevant de la pornographie dure. Toutefois, une perquisition à son domicile permit de mettre la main sur des films de pornographie enfantine et sur des représentations de la violence qui étaient enregistrées sur l'ordinateur du suspect.

Le peu de temps écoulé entre l'examen du matériel et la perquisition du 24.9.2003 a été déterminant pour permettre aux autorités compétentes de trouver des contenus illégaux sur l'ordinateur du suspect. Cette rapidité d'action est typique de l'action du SCOCI entre la découverte de contenus illégaux sur des systèmes P2P et l'intervention des autorités de police compétentes. C'est d'autant plus important que dans de nombreux cas, le suspect invoque pour sa défense tout ignorer des questions techniques ou juridiques. La découverte d'autres preuves en cas de perquisition domiciliaire est ici en mesure de clarifier la situation effective.

11. Problèmes et amorces de solutions

Très rapidement, il s'est confirmé que le lieu (n° postal) de l'utilisateur d'une adresse IP revêt une importance décisive dans la lutte contre la cybercriminalité. Pour le SCOCI, il est indispensable de pouvoir déterminer par le chemin le plus court et dans les plus brefs délais l'autorité locale compétente découlant de la détermination de la

compétence matérielle. Ce n'est qu'ainsi que les cas de soupçon peuvent être transmis sans détours ni démarches supplémentaires en vue de l'ouverture éventuelle d'une procédure pénale.

La majorité des fournisseurs suisses collaborent de leur plein gré avec le SCOCI. Le SCOCI communique aux fournisseurs l'adresse IP accompagnée de la date et de l'heure exactes de l'utilisation de l'Internet. Sur la base de ces renseignements, les fournisseurs déterminent le domicile ou le lieu de connexion du suspect, permettant ainsi d'établir le lien local nécessaire à l'ouverture d'une procédure pénale.

Dans l'optique de la sécurité du droit, cette possibilité de se renseigner devrait être ancrée dans la législation d'exécution de la LSCPT. Une proposition dans ce sens figure dans la procédure de consultation.

12. Contexte du SCOCI

Outre la mise en service du SCOCI, les instances les plus diverses de l'entourage du SCOCI se sont penchées sur les possibilités de lutte contre la cybercriminalité et les besoins en la matière.

12.1 Interventions parlementaires

Il convient de citer en particulier les interventions parlementaires ci-après, déposées ou traitées en 2003:

- **Postulat Meier-Schatz Lucrezia**. Lutte contre la pédophilie sur Internet

Madame Meier-Schatz demandait que le texte du site du SCOCI soit modifié. Les requêtes de l'auteur du postulat ont été acceptées dans le cadre de la réactualisation régulière du contenu du site.

- **Interpellation Studer Heiner.** Offres de services à caractère sexuel. Mieux protéger la jeunesse.

Dans sa réponse, le Conseil fédéral renvoyait entre autres aussi au SCOCI.

- **Motion Fehr Jacqueline**. Centre de compétences international pour la lutte contre la cybercriminalité.

Le Conseil fédéral établit dans sa réponse que la Suisse avait déjà fourni un travail considérable grâce au SCOCI.

- **Motion Aeppli Wartmann Regine**. Lutte contre les abus sexuels envers les enfants – Davantage de moyens.

Le Conseil fédéral a répondu qu'en ce qui concerne les autres moyens, la question des moyens supplémentaires devait être examinée dans le cadre de l'évaluation du SCOCI.

- **Motion Vermot-Mangold Ruth-Gaby**. Pornographie pédophile sur Internet et prostitution des enfants et interpellation Cornu Jean-Claude. Pédophilie via Internet. Affaire Landslide

Outre la mention de diverses autres mesures, le Conseil fédéral a souligné dans sa réponse que l'une des priorités du SCOCI était la lutte contre la criminalité sur Internet en général et contre la pornographie enfantine sur Internet en particulier.

12.2 Groupes de travail dans le cadre de l'opération GENESIS

Opération de grande envergure puisqu'elle portait sur 25 cantons, GENESIS a été l'occasion unique de révéler et de corriger les lacunes dans la coopération entre la Confédération et les cantons à partir de données empiriques.

Sur mandat de la conseillère fédérale Ruth Metzler-Arnold, deux groupes de travail ont été constitués. Ils ont pour mission de mettre en lumière les points où il y a nécessité d'agir pour améliorer la coopération entre la Confédération et les cantons. Le problème majeur réside manifestement en l'absence de compétences d'enquête au niveau fédéral dans la phase initiale de la procédure. Un rapport proposant des solutions de rechange est actuellement en consultation.

Le rapport final proposera aussi des mesures dans le domaine opérationnel à partir des expériences rassemblées par le SCOCI.

12.3 Commission d'experts Cybercriminalité

En novembre 2003, au cours d'un échange de vues, le Conseil fédéral a décidé de réglementer spécifiquement la responsabilité pénale de ceux qui propagent des contenus répréhensibles sur Internet et de doter les services fédéraux compétents de nouveaux pouvoirs d'investigation. En 2004, le DFJP mettra en consultation des propositions tendant à concrétiser ces deux décisions.

S'inspirant de la directive de l'Union européenne (UE) sur le commerce électronique, la commission d'experts "cybercriminalité" propose de compléter le code pénal (CP) par des dispositions réglant spécifiquement la responsabilité pénale dans le domaine de l'Internet. Selon cette réglementation, l'auteur et le fournisseur de contenus seraient pleinement responsables pénalement des contenus punissables qu'ils diffusent sur la Toile. Quant aux fournisseurs d'hébergement - qui mettent à la disposition de leurs clients, les fournisseurs de contenus, un serveur destiné à accueillir leurs sites - ils ne devraient endosser qu'une responsabilité pénale limitée pour les contenus répréhensibles, par exemple lorsque, ayant été avisés par des tiers de l'existence de tels contenus, ils n'ont pas communiqué cette information aux autorités de poursuite pénale. En revanche, les fournisseurs d'accès ne devraient pas avoir à répondre pénalement des contenus répréhensibles diffusés sur le net.

Par ailleurs, la commission d'experts préconise de doter la Confédération de compétences supplémentaires afin d'accroître l'efficacité des poursuites pénales lors d'infractions commises dans plusieurs cantons et à l'échelon international. Il convient à cet égard de relever que le SCOCI ne serait pas touché par cet élargissement des compétences. Les cas traités par le SCOCI ont tous un lien avec la Suisse et concernent pour la plupart un seul canton. Seule l'enquête menée ultérieurement au niveau cantonal permet de donner éventuellement des indices présumant d'un état de fait supracantonal. Néanmoins, le Conseil fédéral n'entend pas instaurer une nouvelle compétence générale de la Confédération en matière de répression de la cybercriminalité, autrement dit de soumettre cette criminalité à la juridiction fédérale, sur le modèle du projet "efficacité".

13. Perspectives

- **En qualité d'entreprise de services, le SCOCI mettra l'accent sur les besoins des cantons, notamment quant à la transmission des cas de soupçons.**

- **La plupart des cas de soupçons du SCOCI concernant le canton de Zurich, la reprise des pourparlers avec les autorités politiques s'impose en vue de l'intégration de ce canton au sein du SCOCI.**

- **Il serait souhaitable d'élargir modérément l'équipe du monitoring. Cela permettrait d'accroître encore plus le taux de découverte d'actes punissables. Il convient néanmoins de relever qu'une augmentation du personnel dans l'un des trois domaines peut avoir pour conséquence un renforcement des besoins en personnel dans les deux autres (clearing, monitoring, analyse).**

- **Le débat sur un élargissement des compétences de la Confédération en matière de cybercriminalité se poursuivra. Les modèles présentés jusqu'ici n'ont toutefois aucune influence directe sur les travaux du SCOCI.**

- **La ratification de la Convention du Conseil de l'Europe sur la cybercriminalité devra aller de pair avec une définition plus précise des points de convergence avec le SCOCI.**

- **La mise en place d'une Centrale d'enregistrement et d'analyse (MELANI *Mel*de- und *An*alysestelle *I*nformationssicherung) auprès du SAP[16] et, de ce fait, la création de capacités supplémentaires en matière d'analyse laisse prévoir un très haut potentiel interne de synergie avec la section Analyse du SCOCI et contribuera à une amélioration des contacts avec le secteur privé.**

- **Enfin, une adaptation de l'OSCPT[17] donnera une base plus solide à l'obligation de renseigner, essentielle pour le SCOCI, dans le but d'établir la compétence des cantons en matière de poursuite pénale.**

Berne, le 9 janvier 2004

Le chef du SCOCI
Philipp Kronig

pour le Comité directeur du SCOCI
Urs von Daeniken

---

[1] BEMIK / Bekämpfung des Missbrauchs der Informations- und Kommunikationstechnologie (Lutte contre les abus relatifs aux techniques d'information et de communication).

[2] Courrier électronique publicitaire adressé de manière abusive.

[3] Contrôle de l'âge filtrant l'accès à des sites érotiques.

[4] Les programmes *dialer* ou *web-dialer* sont des programmes qui modifient les conditions d'accès à Internet. La connexion par le fournisseur d'accès Internet habituel est supprimée et remplacée par un service téléphonique payant 09xx - numéro à valeur ajoutée par lequel la liaison par exemple à des contenus érotiques est installée. Parfois, ces programmes sont camouflés et sont activés sans que l'on s'en rende compte par un clic de souris.

[5] **CL**earing, **MO**nitoring **AN**Alyse

[6] Système d'exploitation pour ordinateurs personnels.

[7] Techniques offensives apparues au début des années 90 au moyen des nouvelles technologies sur et par le biais de l'information: meilleure connaissance des capacités offensives adverses, amélioration des techniques de diffusion et de distribution de l'information, meilleure sensibilisation à la vulnérabilité des systèmes d'information afin de se protéger des attaques adverses et d'attaquer les systèmes de l'adversaire.

[8] Swiss Interactive Media and Software Association

[9] Swiss Network Operators Group

[10] Prestataire de solutions de sécurité

[11] Outsource Services AG

[12] Les réseaux P2P sont des réseaux décentralisés permettant de trouver et d'échanger toutes sortes de données. Dans la plupart des cas, l'utilisateur doit avoir un logiciel sur son propre ordinateur. Les données recherchées sont ensuite

directement transmises d'ordinateur à ordinateur. Les réseaux P2P les plus connus sont par exemple Kazaa, Gnutella und E-Donkey.

[13] Opération d'envergure nationale visant à réprimer la pornographie pédophile sur Internet et lancée dans le cadre de l'enquête sur le portail Landslide. Ce fournisseur d'accès américain permettait de télécharger contre paiement des images relevant de la pornographie enfantine. Parmi ses clients, plus de 1000 Suisses ont fait l'objet d'une plainte dans le cadre de l'opération GENESIS.

[14] Les sites de « bavardage » (*chat*) offrent à deux ou plusieurs personnes la possibilité de converser sur Internet en temps réel. La plupart de ces sites sont classés de manière thématique. Certains de ces sites sont ouverts à tous, d'autres sont réservés à certains interlocuteurs; ce sont les « salons de bavardage privés » (*Private Rooms/Channels/Chats*).

[15] Adresse Internet Protocol. Les ordinateurs doivent disposer d'une adresse Internet permettant de les identifier pour que les paquets de données puissent parvenir à leurs destinataires .

[16] Service d'analyse et de prévention.

[17] Ordonnance sur la surveillance de la correspondance par poste et télécommunication, RS 780.11