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

Swiss Coordination Unit for Cybercrime Control CYCO

Annual Report 2010

Contents

1. A brief overview

- Despite a decrease in the overall number of incoming reports in 2010, there was once again a marked increase in the number of reports from the category *hardcore pornography*, especially relating to websites containing child pornography. Paedophiles continue to have a vast number of ever evolving communication platforms at their disposal.

- The renewed increase in reports relating to fraud illustrates that Internet users in Switzerland remain popular victims of Internet fraud. Although new modi operandi appear at regular intervals, tried and trusted ploys still lure victims.

- CYCO has stepped up its monitoring, which is illustrated by the increase in the number of incident files forwarded to the cantons.

- Analysis of the responses from cantonal police forces and judicial authorities showed that the incident files forwarded by CYCO to the cantons had been well investigated. Most of the incident files led to house searches, during which police officers were able to secure incriminating evidence.

- Undercover investigations was a topic that kept CYCO preoccupied throughout 2010. Since 1 January 2011, most cantonal police forces have no longer been allowed to conduct preventive undercover investigations against paedophiles on the internet without having prior cause for suspicion. This loophole in cantonal legislation arose following the enactment of the new Criminal Procedure Code and triggered a series of parliamentary procedural requests. The Federal Department of Justice and Police (FDJP) and the Conference of Cantonal Justice and Police Directors have, however, found a solution that allows CYCO to continue its monitoring activities. Thanks to an agreement with the canton of Schwyz, CYCO can continue its own preventive undercover investigations and those it conducts on behalf of the cantons, and continue monitoring chat rooms.

2. Reporting volume

CYCO received a total of 6,181 online reports in 2010 concerning suspicious web content. This represents a decrease of 18 percent over the previous reporting period (2009: 7,541 reports). It is too earlier to say whether this decrease represents a general downward trend in reporting practices or is merely a result of normal periodic fluctuation, as CYCO has observed on several occasions since its establishment. With the exception of the record year of 2007, the annual average reporting volume via CYCO's online reporting form remains static at between 6,000 and 7,500 reports.

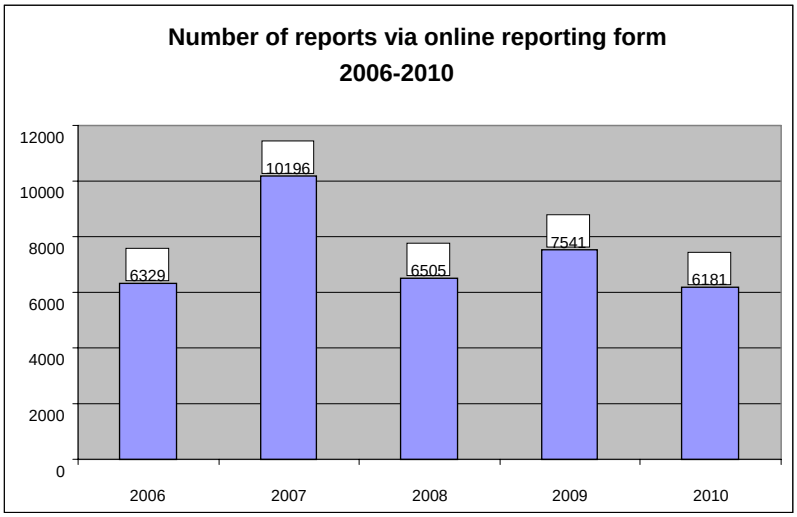

Diagram 1 : Reporting volume via www.kobik.ch 2006-2010

Closer analysis of the incoming reports in 2010 shows noticeable differences between the months when reports were submitted (see diagram 2). However, the differences can often be attributed to specific incidents of limited duration.

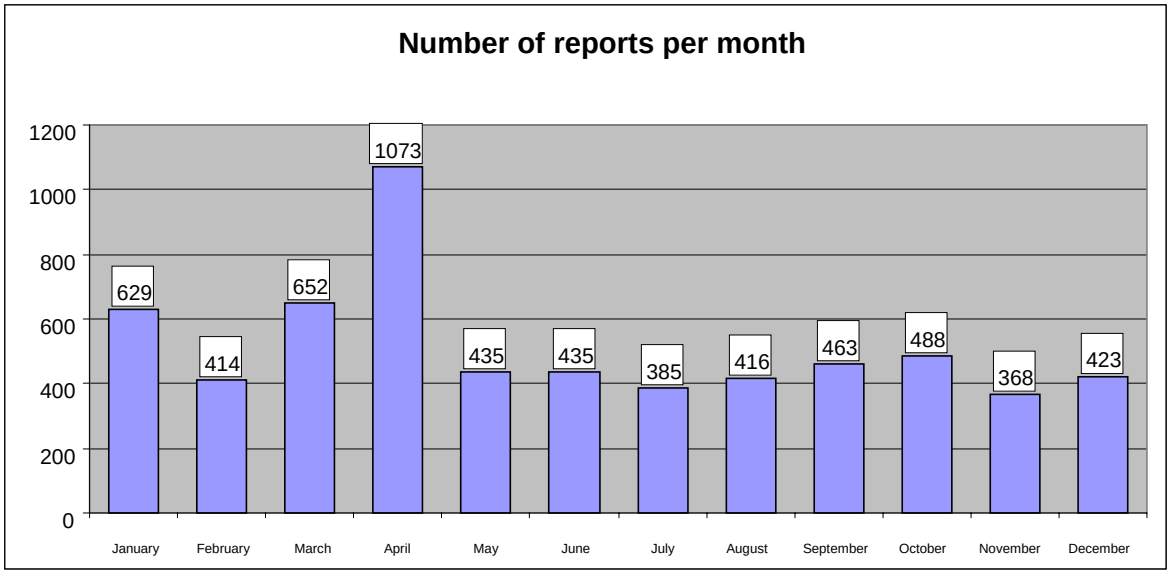

Diagram 2 : Reporting volume via www.kobik.ch according to month (total = 6181 reports)

3. Subject matter of reports

There was a significant increase in the number of reports concerning websites containing illegal pornography. The category *hardcore pornography* consolidates criminal acts subsumed under Article 197 paragraph 3 of the Swiss Criminal Code (SCC) and includes child pornography and pornography depicting excrement, animals or violence, whereby 96 percent of these reports concerned child pornography. Thus, the increasing trend in hardcore pornography observed in 2009 continued in 2010 and was evident both in absolute terms as well as in comparison to other categories (see diagrams 3 and 4). The increase in the number of reports concerning child pornography is partly linked to the increasing number of Web 2.0 applications such as so-called communities, which are being used more and more for the fast and anonymous exchange of child pornography. For the first time in 2010, the category *hardcore pornography* (1,743 reports) exceeded the category *Spam* (see diagram 3).

There was a significant fall in the number of reports concerning *legal pornograph*y, particularly in the number of reports concerning websites that provide pornography by means of streaming technology. The decrease may be attributed, amongst other things, to Internet users becoming inured or increasingly tolerant of such offers.

The number of reports concerning *fraud* increased once again in 2010. Indeed, this category has witnessed a continual increase since 2006, a factor which illustrates its significance for Internet users in Switzerland. Fraud is a category of crime that is in constant transition and continues to gain in importance due to ever emerging new methods of deception. Classified advertisements and auction sites, in particular, are being used more and more to commit fraudulent acts: one method readily employed by fraudsters is the trade in used cars, whereby unsuspecting buyers are deceived by means of bogus transport companies and local accomplices. Besides these forms of deception, online fraud also includes other products. Moreover, well-known scams such as so-called online subscription traps, in which users are deceived by what they believe to be a free offer into signing up for a costly subscription, or advance fee fraud[1] and its numerous variations, remain current and efficient forms of deception.

Compared with 2009, there was an increase in the number of reports in 2010 relating to the category *economic crime*, possibly resulting from various waves of phishing attacks[2] directed at banking and money transfer service providers. What was especially noticeable was the way in which fraudsters in the initial phase of the deception gained unlawful access to e-mail accounts. In the second phase, the fraudsters sent written pleas for financial help, claiming a case of personal emergency.

The number of queries from the public about Internet crime has remained high but static in the last few years. This indicates that CYCO is, indeed, being perceived on a national level as the competence centre for Internet crime.

[1] This method of deception involves the victim being persuaded by means of false promises (such as a lottery win) to pay an advanced fee to the fraudster. The victim pays the advanced fee and then waits in vain for the return service or reward.

[2] Methods by which fraudsters attempt to attain the data of Internet users (password, user name, etc.) via forged website addresses.

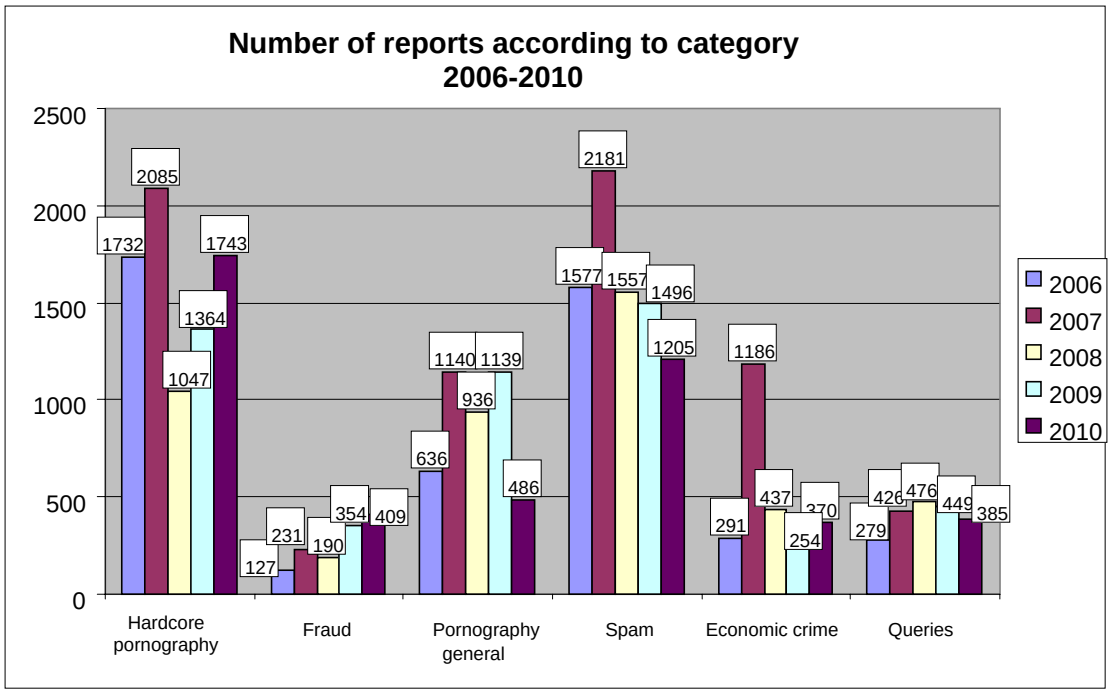

Diagram 3 : Absolute comparison of incoming reports according to category 2006-2010

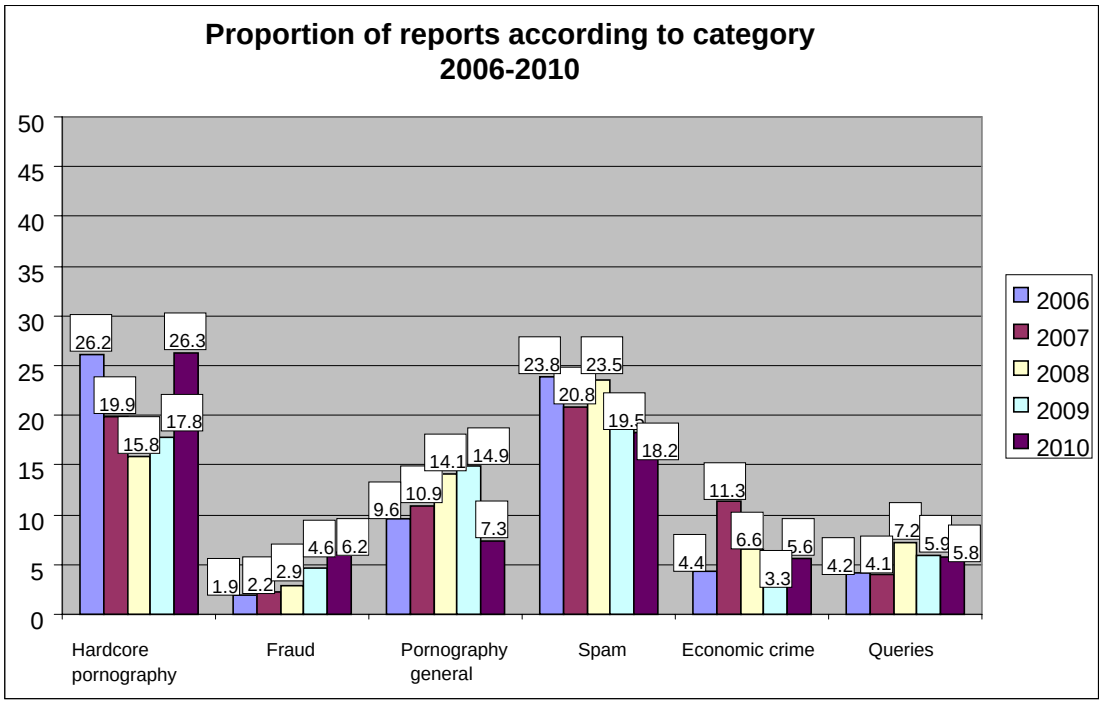

Diagram 4 : Relative comparison of incoming reports according to category 2006-2010

Diagram 4 provides an overview of the six most important categories of Internet crime and their development over the past five years. Like every year, a significant number of reports in 2010 had, ultimately, to be categorized under *other* or *not verifiable* (see page 12). The category *not verifiable* comprises mainly websites that were no longer active at the time CYCO tried to process the report. The consistently high

number of reports from these two categories testify to the fast pace and variability of the Internet.

Although CYCO received comparatively few reports from the categories *defamation,* and *threat and coercion*, they include phenomena that greatly concern CYCO. One such phenomenon is cyber-bullying, which gained special political and media attention in 2010. CYCO processed a total of 25 cases in 2010 which could be ascribed to the definition of cyber-bullying[3]. At least four of these cases involved minors.

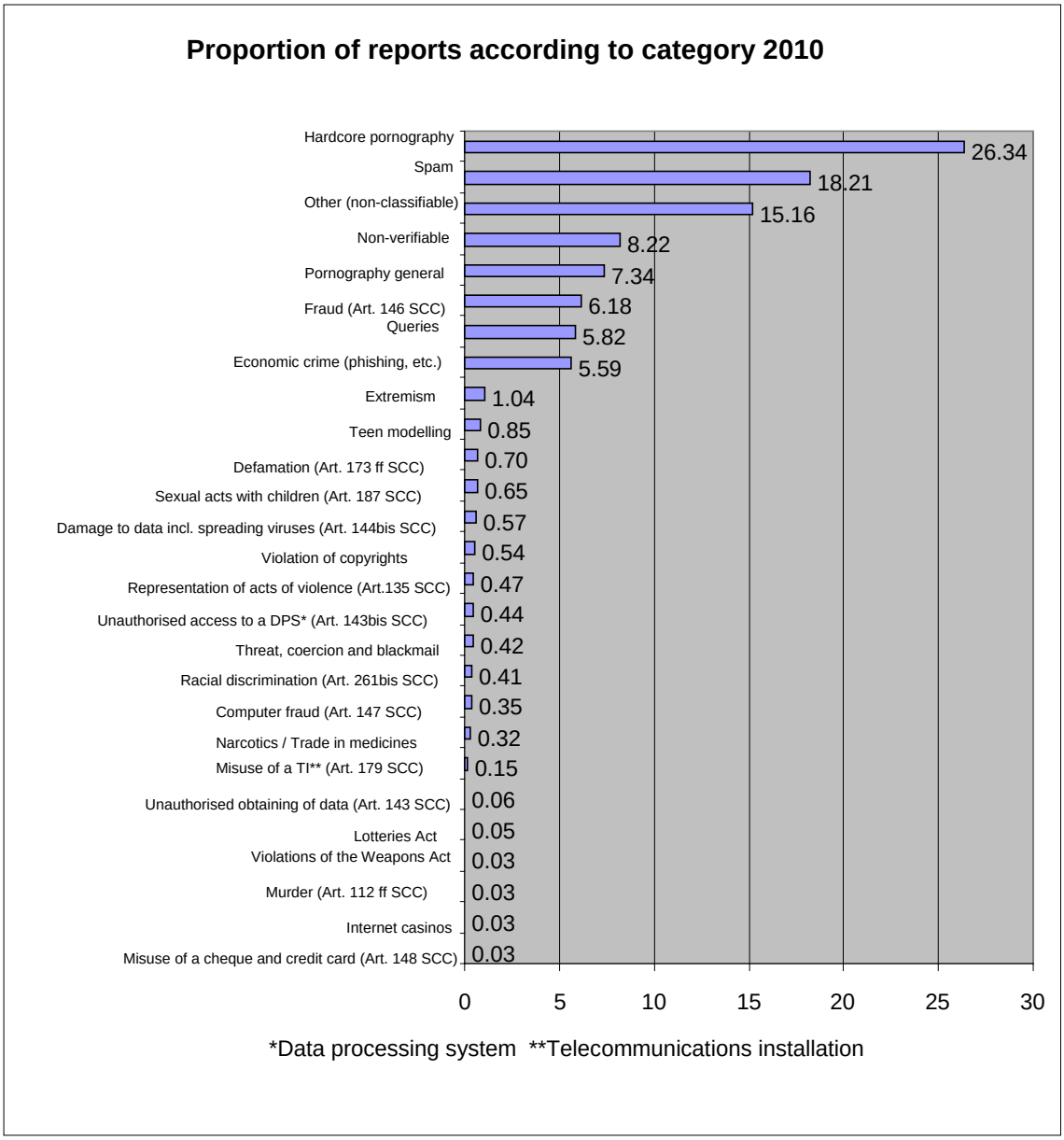

Diagram 5 : Proportion of incoming reports in 2010 according to category

[3] Definition of cyber-bullying according to the Federal Council's report of June 2010: "Cyber-bullying is when modern means of communication such as mobile phones, chat rooms, social networks like Netlog or Facebook, video portals or forums and blogs are used to publish defamatory texts, pictures or films intended to slander, embarrass or harass another person. The attacks usually take place repeatedly or over a long period of time, and victims have the distinction of being especially helpless."

Besides online reporting forms, CYCO also received reports through co-operation with *Telefono Arcobaleno*[4]. In 2010, the organisation reported 587 links leading to child pornography on the Web. Most cases involved content on so-called one-click hosting services[5] located in Switzerland. CYCO reported the illegal content to the service operators who arranged for its subsequent deletion. The number of reports has fallen significantly since 2009, which shows that these services are being used less frequently for exchanging child pornography thanks to these and other measures.

[4] Telefono Arcobaleno is an Italian child protection organisation.
[5] These sites offer free storage that can be used to upload data onto the Internet. The data can be made available to unlimited numbers of Internet users by means of a simple link.

4. Monitoring

CYCO was able to open a total of 229 incident files for the attention of cantonal law enforcement agencies in 2010. This represents an increase over 2009 and is due to CYCO optimising its monitoring activities. The increase also confirms the general trend of the previous two years.

The 229 incident files involved the systematic possession and distribution of child pornography. The cases arose from monitoring Swiss Internet users on P2P networks who were actively exchanging child pornographic material.

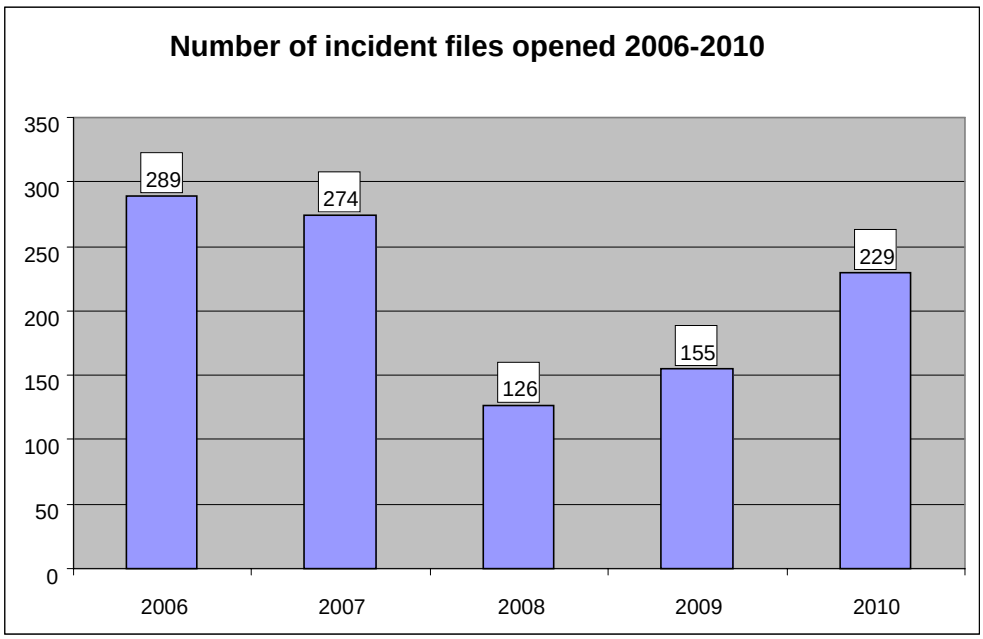

Diagram 6: Incident files resulting from active Internet monitoring [6]

[6] The year denoted in the diagram refers to the point in time when the incident file was opened by CYCO. For various reasons, files are sometimes not forwarded to the cantonal law enforcement agencies until the following year.

5. Selected case studies

In the course of its active monitoring of P2P networks, CYCO's attention was attracted by a Swiss national who was acquiring child pornographic material and distributing it to others. Further investigations revealed the location of the Internet connection and the file was subsequently forwarded to the cantonal law enforcement agencies. Inquiries by the cantonal police revealed that the suspect was a weekly resident in that canton but had his permanent domicile in another canton. The file was forwarded to the Federal Criminal Police's Paedophilia and Pornography Section, who assumed responsibility for co-ordinating with the authorities of the canton where the suspect had his permanent domicile. A short time later, CYCO was requested by the competent cantonal police force to conduct further investigations. The police justified its request by stating that the suspect was a professionally exposed person, and the current state of evidence was insufficient to warrant a house search. Undercover investigations allowed CYCO to monitor the suspect's activities in social networks, to gather further proof and provide the cantonal police with solid evidence to confirm their suspicion. During the subsequent house search the police seized child pornographic pictures and videos. In view of the volume of evidence, the suspect admitted his guilt.

In another case involving the active monitoring of P2P networks, CYCO identified a Swiss national who was acquiring and distributing child pornography. The subsequent house search by the cantonal police revealed that the suspect had been sexually abusing an underage girl over a period of time. Further inquiries into the case revealed that the mother of the child was a drug addict and had been prostituting her daughter.

In a further case which involved undercover operations, CYCO identified a 42 year-old Swiss national who, in a chat room reserved for children and young people, had targeted a girl claiming to be 13 years old. The age of the girl did not deter the man either from making sexually explicit comments or from repeatedly requesting photos and further contact. The case was forwarded to the competent cantonal law enforcement authorities.

6. Recipients of forwarded incident files

A total of 299 incident files were forwarded to cantonal law enforcement agencies in 2010. This represents a significant increase over the previous reporting period and is a direct result of CYCO's heightened monitoring activities.

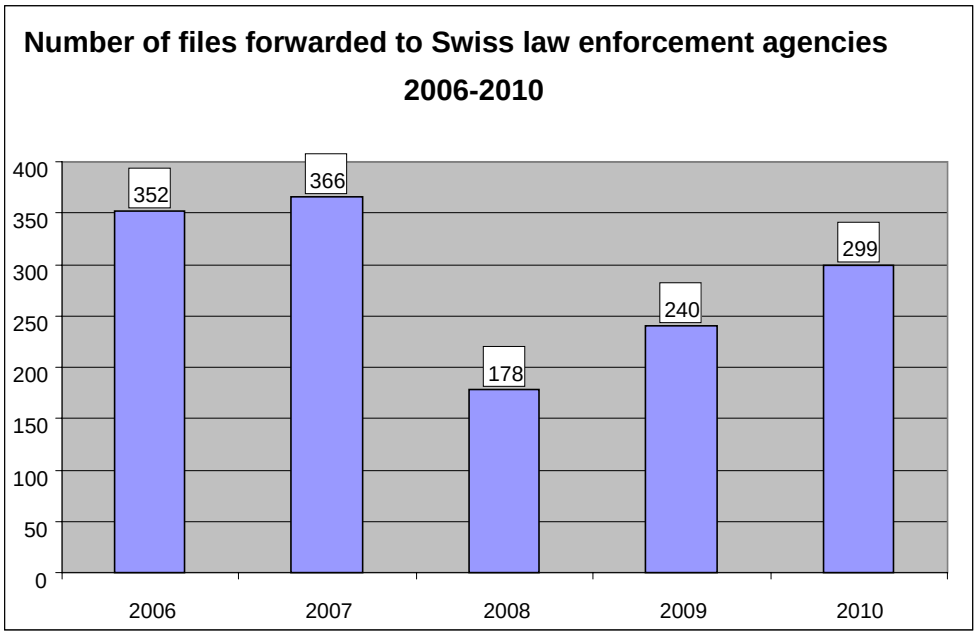

Diagram 7: Incident files forwarded by CYCO to cantonal law enforcement agencies

An in-depth analysis of the forwarded incident files (see diagram 8) shows that most cases forwarded to the cantonal law enforcement agencies in 2010 resulted from the active monitoring of *P2P networks* (245 cases). A further 54 forwarded incident files were a result of reports received by CYCO from members of the public.

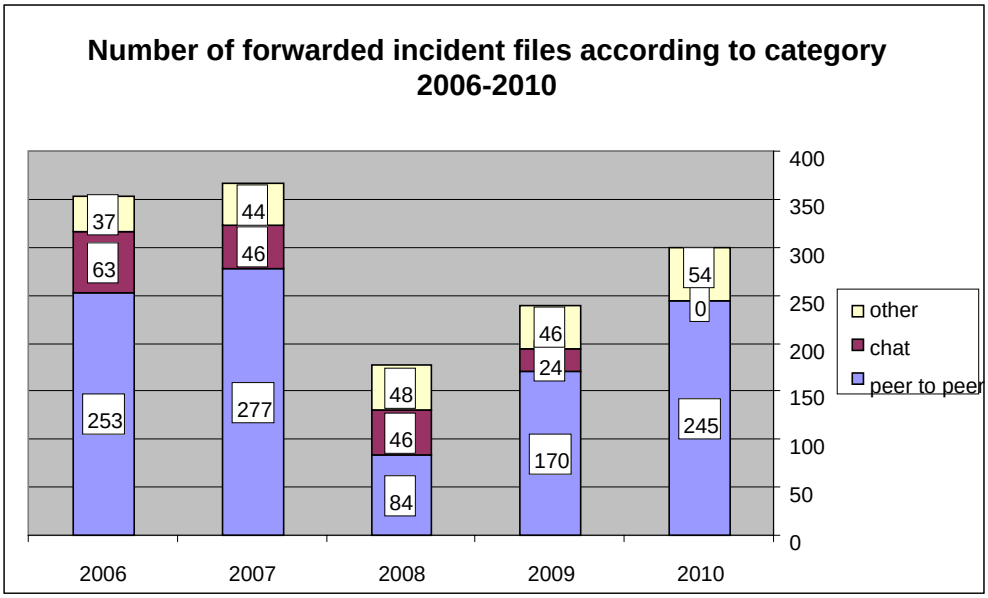

Diagram 8: Forwarded incident files according to category

None of the incident files forwarded to the cantonal law enforcement agencies in 2010 arose from the category *chat*. The main reason for this is that Swisscom withdrew in 2009 as provider from the two platforms "Teentalk" and "Kidstalk", and inci-

dent files arising from this category had until that time been based on a long-standing co-operation between Swisscom and CYCO. Developments in the field of undercover operations (see chapter 9.2) and a change in the provider of these chat rooms subsequently forced CYCO to reprioritise.

The category *others* has remained static for a number of years (see diagram 8). This category comprises, amongst other things, references to pornographic websites that do not duly verify the user's age, as well as to other kinds of websites located in Switzerland whose content may be illegal. Incident files forwarded to federal law enforcement agencies are also included in this category.

As in previous years, CYCO forwarded most incident files in 2010 to the municipal and cantonal police of Zurich (see diagram 9). In second, third and fourth place were the cantonal police of Vaud, Aargau and Bern, respectively. Twenty-two files were forwarded to federal law enforcement agencies such as the Federal Criminal Police's Paedophilia and Pornography Section, Swissmedic, the Reporting and Analysis Centre for Information Security (MELANI) or the Lotteries Commission (Comlot).

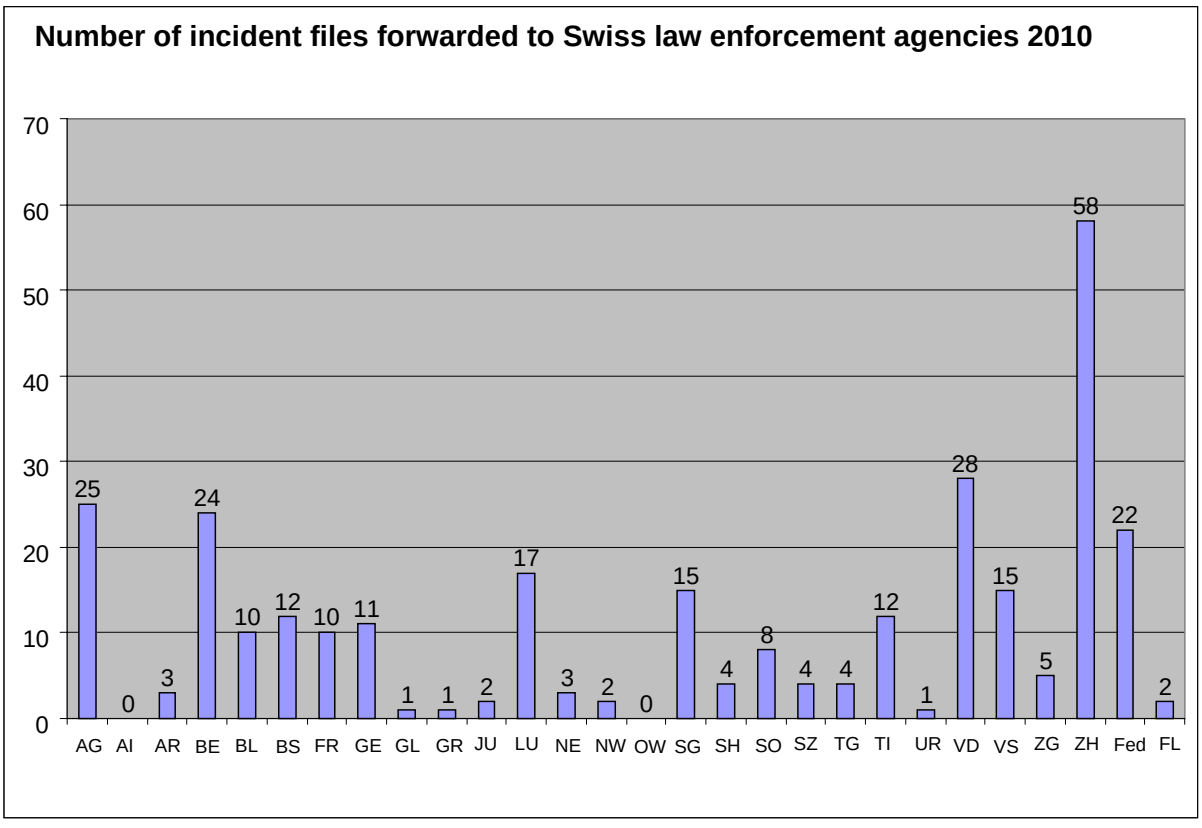

Diagram 9: Total number of incident files forwarded to Swiss law enforcement agencies (federal and cantonal) and the authorities of the Principality of Liechtenstein FL (total = 299 files)

In addition, CYCO reported a total of 231 websites to the competent agencies abroad. Nearly all the websites contained child pornographic material and had been brought to the attention of CYCO through the online reporting form.

7. Responses from the cantons

To obtain an overview of the steps taken by the cantons on receipt of an incident file, CYCO requested the cantons to provide further information on the progress of the cases, on the adopted measures and on the outcome of court proceedings. Approximately 90 percent of all incident files forwarded by CYCO to the cantons led to house searches by cantonal police forces. More than 80 percent of the house searches yielded relevant (illegal) material, which was subsequently seized. In approximately 90 percent of the cases, criminal proceedings resulted in a conviction.

8. Working groups

During the 2010 reporting period, CYCO participated in various national working groups on crime prevention.

CYCO remained active in 2010 in the national working group "Child Abuse" (German *Kindsmissbrauch*), together with fedpol's Paedophilia and Pornography Section, non-profit organisations, representatives from the cantons and from Swiss Crime Prevention.

Since 2010, CYCO has taken an active part in the national programme known as "Youth Media Protection and Media Literacy" (German *Jugendmedienschutz und Medienkompetenzen*). Within the programme, CYCO is involved not only in the steering group responsible for developing the programme, but also in the support group implementing it. The purpose of the programme is to help teach children and young people how to deal with modern media in a safe and responsible way and appropriate to their age. Similarly, CYCO assisted the Federal Department of Justice and Police in compiling its report on cyber-bullying, as demanded in a parliamentary procedural request by National Councillor Barbara Schmid-Federer. The report was published on 2 June 2010 and is available on fedpol's website.

Furthermore, CYCO was involved in developing the concept "Security and Confidence" (German *Sicherheit und Vertrauen*), which under the guidance of the Federal Office of Communications (BAKOM) highlights measures to promote the safety and confidence of the public in modern information and communication technologies.

And last but not least, thanks to CYCO's participation in the working groups "IT Investigators" and "Monitoring Telecommunications" the Unit was also able in 2010 to stay abreast of technical developments and law enforcement.

9. Projects

9.1. Co-operation with Swiss Internet Access Providers[7] to filter websites containing child pornography

Since 2007, websites containing child pornography have been blocked in Switzerland with the aid of the software *Child Sexual Abuse Anti-Distribution Filter*. The filter is directed at foreign websites with child pornographic content.

9.2. Undercover investigations

Great effort was required to clarify the legal situation following the enactment of the revised federal Criminal Procedure Code (CrimPC), and by the Paedophilia and Pornography Section to reprioritise its tasks as a result of this new piece of legislation. Since 1 January 2011, most cantonal police officers are no longer permitted to conduct preventive undercover investigations against paedophiles on the Internet without prior suspicion, because cantonal police legislation does not provide sufficient legal bases in this regard. The loophole has arisen following the entry into force of the Criminal Procedure Code, which superseded the previous legal provisions on undercover investigations contained in the Covert Investigations Act but which were abolished with the entry into force of the Criminal Procedure Code.

Some cantons such as Schwyz, Uri and Obwalden recognised the need for action and adapted their (cantonal) police legislation with effect from 1 January 2011. The Federal Department of Justice and Police (FDJP) in collaboration with the Cantonal Conference of Justice and Police Directors (CCJPD) sought a solution to the problem to allow CYCO to continue its monitoring of paedophile crime on the Internet. Thanks to an agreement with the Security Department of Canton Schwyz, CYCO can continue its preventive undercover activities on behalf of the cantons and thus monitor chat rooms. CYCO's work is currently based on the Police Act of Canton Schwyz and on judicial authorisation from the Court for Coercive Measures of Canton Schwyz. This ensures that paedophile criminals on the Internet do not consider themselves beyond the grasp of law enforcement.

[7] Internet Access Provider facilitates an Internet user with Internet access.

10. Parliamentary procedural requests at federal level

Parliamentary procedural requests submitted in 2010:

Child and youth protection

- Cantonal Initiative Bern: Media violence – Effective protection for children and young people;
- Initiative Schmid-Federer: Effectiveness and efficiency in the fields of youth media protection and Internet crime;
- Interpellation Amherd: Youth media protection – further action after prevention programmes;
- Motion Bischofberger: Effectiveness and efficiency in the fields of youth media protection and Internet crime fighting;
- Motion Schweiger: Teaching youth the selective use of new media;
- Question Graber: Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse;
- Question Schmid-Federer: Monitoring chat rooms;
- Motion Amherd: UN Resolution on Combating Online Child Abuse;
- Interpellation Markwalder: Effiency in the fields of youth media protection and media literacy;
- Motion Amherd: Youth media protection – establishing a national competence centre for electronic media;
- Motion Amherd: Certification of websites;
- Postulate Amherd: Constitutional basis for establishing a national control board for the certification of websites;

Undercover investigations

- Initiative Schlüer: Undercover search for the purpose of crime prevention;
- Motion Fiala: Undercover investigation;
- Question Baumann: Preventing paedophile crime on the Internet;
- Question Rickli: Undercover investigations into paedophiles;
- Question Schmid-Federer: Undercover investigations on the Internet;
- Question Schmid-Federer: Undercover investigations, Article 286a SCC;

Protection of privacy

- Interpellation Hiltpold: Unauthorised circulation of photos or videos and the protection of the people concerned;
- Postulate Graber: Privacy under attack and the indirect threat to personal freedom;
- Postulate Hodgers: Adapting data protection legislation to the new technologies;

Cyberwar

- Motion Büchler: Protection against cyber attacks;
- Postulate Recordon: Cyberwar threat analysis;
- Postulate Büchler: Chapter on cyberwar in the Security Report;

Cyber-mobbing / Cyber-bullying

- Postulate Schmid-Federer: Appointing a federal mobbing and cyber-bullying officer;

General Internet crime

- Question Büchler: Internet crime;
- Postulate by the Commission for Legal Inquiries SR: Investigation of Internet criminals;
- Motion Barthassat: Greater safety thanks to better technology skills;
- Motion Barthassat: Extending the obligation to preserve records on the allocation of IP addresses;
- Postulate Darbellay: Concept on protecting Switzerland's digial infrastructure;
- Postulate FDP Liberal Fraction: Central and co-ordination office for cyber threats;

Others

- Cantonal initiative Zug: Banning violent games;
- Interpellation Mörgeli: Expensive restrictions by the FDJP to private Internet providers;
- Interpellation Parmelin: Dangers of counterfeit medicines and medicine smuggling;
- Interpellation Schmid-Federer: CYCO/Melani – Drawing a balance following the restructuring of SAP;
- Postulate Savary: Does Switzerland require legislation against the unlawful downloading of music?;
- Question Graber: Wikileaks Affair – consequences for Switzerland and the opinion of the Federal Council;
- Question Rickli: Switch
- Motion Darbellay: Increasing the number of staff in the CYCO office and clarifying its mandate and structure;
- Initiative Schmid-Federer: "Digital trespassing" as a statutory offence.

11. Media coverage, training and conferences

11.1 Media coverage

As in previous years, CYCO enjoyed generally very positive media coverage in 2010: numerous articles and reports appeared on CYCO's work both in the printed and electronic media, with special emphasis on cyber-mobbing and undercover investigations. CYCO, in its turn, had various opportunities for issuing statements on topics in its field of responsibility.

11.2 Training and conferences

CYCO staff participated in the following conferences, international conventions and training modules in 2010:

In Switzerland :

- IT Investigators Convention;
- Teaching assignment as part of the MAS Forensics at the Lucerne University for Applied Sciences and Arts;
- Teaching assignment as part of the main annual course at the Middle European Police Academy(MEPA);
- Participation in open forum, Tweakfest 2010;
- Participation in round table " Cybercrime & Cybersecurity " by the Democratic Control of Armed Forces (DCAF);

Abroad :

- RIPE NCC Meeting, London;
- Octopus Interface, Strasbourg;
- E-Crime Congress, London.

12. Partnerships and contacts

12.1 Co-operation with other federal agencies

The tremendous scope of topics and problems in the field of Internet crime requires close co-operation with other federal agencies. Within the Federal Criminal Police (FCP), CYCO collaborates closely with the Paedophilia and Pornography Section, Digital Crimes Investigations Section and Undercover Investigations Section. Depending on the nature of the crime, CYCO also co-operates with other FCP units.

Throughout 2010, CYCO strengthened its contacts and cross-departmental co-operation with various federal agencies such as the Reporting and Analysis Centre for Information Security (MELANI), the Division for International Mutual Assistance at the Federal Office of Justice (FOJ), the Federal Office of Communications (BAKOM), Swissmedic and the Lotteries Commission (Comlot).

12.2 Working meetings and exchanging experiences with the cantons

CYCO had contact with various cantonal police corps and examining magistrates in 2010. Moreover, there were working meetings with representatives from the cantons on specific topics, and the National Police of Liechtenstein paid CYCO a working visit as part of the annual exchange of experiences between the two agencies.

12.3 External visitors

CYCO received various external visitors in 2010. This gave the Unit the opportunity of presenting its work and drawing visitors' attention to the difficulties and correlations within the field of cybercrime. Some of the highlights of the year included visits from Federal Councillor Evelyne Widmer-Schlumpf, from various national councillors, from journalists and from the Director of Action Innocence (AIG) – a non-governmental organisation that CYCO has collaborated with for many years in the fight against child pornography.

12.4 International co-operation

In addition to the above-mentioned international conferences, CYCO collaborated closely on an operational level with international partners in the context of specific projects or working groups. As in 2009, CYCO was represented again in 2010 in the "Law Enforcement Cooperation Working Group" (LECWG) which is part of the European Financial Coalition (EFC) in Brussels.

13. Glossary

Adult check	Age verification system for youth protection. It limits access by minors to certain websites.
Chat	Electronic real-time communication, usually over the Internet.
Cloud Computing	Cloud Computing describes IT infrastructures (computer capacity, data storage capacity of computers and servers) that can be accessed from anywhere over a network such as the Internet. Instead of storing system applications and data on a few local computers, the computer load is distributed over as many computers as possible for an optimal use of resources and made available by numerous servers all over the world (so-called cloud cluster). One of the basic conditions for cloud computing is a high-performance band width.
Cyberbullying	Cyber-bullying is when modern means of communication such as mobile phones, chat rooms, social networks like Netlog or Facebook, video portals or forums and blogs are used to publish defamatory texts, pictures or films intended to slander, embarrass or harass another person. The attacks usually take place repeatedly or over a long period of time, and victims have the distinction of being especially helpless.
One-click hosting	One-click hosting describes web services that allow Internet users to store data (usually video and audio data) on the host's server without prior registration. The user is given a URL under which the data can be viewed and downloaded.
Peer-to-peer (P2P)	In a peer-to-peer network, members can access the same data and exchange data with third parties.
Phishing	Methods to acquire an Internet user's data (e.g. password, username, etc.) via fake websites.
Hardcore pornography	Sexual acts with children (paedo porn), animals or human excrement, or sexual acts depicting violence (Art. 197 para. 3 SCC).
Hash values	Clearly classifiable parameter of an image (digital fingerprint)
Proxy	Communications interface in an IT network between the client and a server by means of which a website can be accessed.
Redirect service	A redirect service changes long URLs into short ones that are easier to memorise. The browser is instructed to immediately activate the contents of the requested web page via a shortened URL.
Spam	Spam is the use of electronic messaging systems to send unsolicited bulk messages. Spam e-mails are usually sent for advertising purposes and to spread malware in a user system.
Streaming	The transmission of audio or video data. Data is not completely downloaded at once onto a system but made available via a computer network over time. Thus, a user does not need to download all the data, but can "listen in" on it.
URL	Uniform Resource Locator is an address (usually called an Internet address) consisting of a series of numbers specifying the address of a file.

14. Trends 2010

A significant feature of 2010 was the increase in the number of reports relating to child pornography on the Internet, thus confirming the developments of the last few years. Storage and distribution facilities for illegal web content are diverse and are undergoing perpetual development, and Internet criminals are very versatile with regard to their modi operandi. Moreover, the use of social networks for exchanging child pornographic material within closed user groups has increased enormously.

The increase in the number of reports from scam victims or victims of attempted online fraud kept CYCO extremely busy in 2010. New modi operandi have appeared, but victims are still lured using tried and trusted ploys, whereby cyber criminals deliberately use transnational mechanisms that make law enforcement difficult and complicated. This not only reinforces the need for closer international co-operation on cybercrime, but also underlines the fact that prevention and the awareness by Internet users of the dangers are often the most efficient means of fighting online fraud. By adhering to the simplest of precautions, most scams can be recognised in time. Most fraudsters use freely accessible data to target their victims.

In 2010, CYCO increased its investigations into P2P networks; this form of active monitoring remains one of CYCO's most important means of fighting online paedophile crime and ensures that paedophile criminals are made aware that they are not operating in a legal vacuum. To keep up with technical changes and with the versatility of the perpetrators, CYCO is continually developing its resources and methods.

The revision of the Federal Act on the Surveillance of Post and Telecommunications will accommodate the difficulties in identifying people that access the Internet with mobile telephones. Moreover, the revised legislation will be adapted to technical developments, thus explicitly including Internet as well as e-mail and Internet telephoning.