KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internetkriminalität
Service de coordination de la lutte contre la criminalité sur Internet
Servizio di coordinazione per la lotta contro la criminalità su Internet
Cybercrime Coordination Unit Switzerland

Swiss Coordination Unit for Cybercrime Control CYCO

Annual Report 2011

Swiss Coordination Unit for Cybercrime Control (CYCO)
Nussbaumstrasse 29
3003 Bern

www.kobik.ch
www.cybercrime.ch

Published: 4 April 2012

Contents

1. A brief overview

- In 2011, CYCO received a total of 5,330 reports via the online complaints form. This represents a decline of nearly 14 percent over 2010.

- Once again, most of the incoming reports concerned the category *illegal pornography* (especially child pornography).

- By monitoring P2P networks CYCO succeeded in identifying 214 people who were exchanging child pornography. Anyone who views child pornography encourages the production of new material and therefore indirectly participates in child abuse.

- There was a further increase in the number of reports from the category *economic crime*.

- CYCO made considerable progress with the National Data and Hash Value Collection project. It successfully trained the cantonal police corps and received the first pictures for its database.

- Since May 2011, CYCO has been on the National Strategy for Cybercrime Defence project team and will also represent the interests of cantonal and federal law enforcement agencies on implementation of the strategy.

- CYCO has considerably strengthened international co-operation on fighting cybercrime with INTERPOL and Europol.

2. Reporting volume

In 2011, CYCO received a total of 5,330 online reports concerning suspicious web content. This represents a decrease of nearly 14 percent over the previous reporting period (2010: 6,181 reports). With the exception of the record year of 2007, the average reporting volume from online reporting has remained between 6,000 to 7,500 reports. Although the downward trend in the number of incoming reports does not allow us to draw any conclusions on the true development of cybercrime or volume of illegal subject matter on the Internet, it does say something about the willingness of the public to report cybercrime and society's perception thereof. There may be several reasons for the decline in the number of online reports. One reason could be that certain types of Internet crime are now so common that they tend to be trivialised by the public, and victims therefore refrain from reporting the incident to CYCO. Although there were fewer reports compared to previous years, the content of the reports was of a better quality. The most likely reason for fewer reports is the absence of major incidents attracting wide public attention.

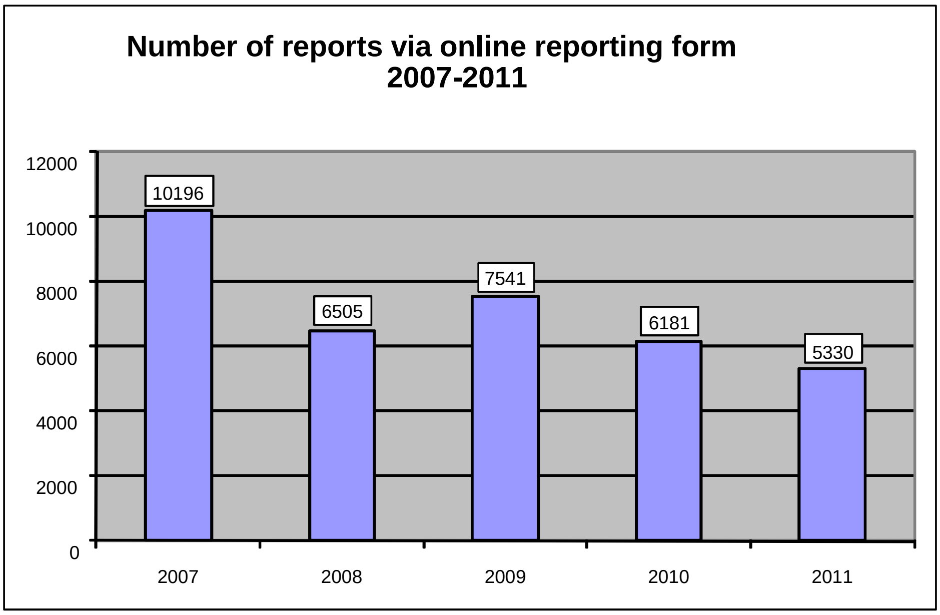

Diagram 1: Reporting volume 2007-2011 via www.kobik.ch

The number of incoming reports per month was steady (see diagram 2). Fluctuations can often be attributed to specific incidents of limited duration. This supports the theory that the decline in overall reporting volume is primarily due to the absence of major incidents.

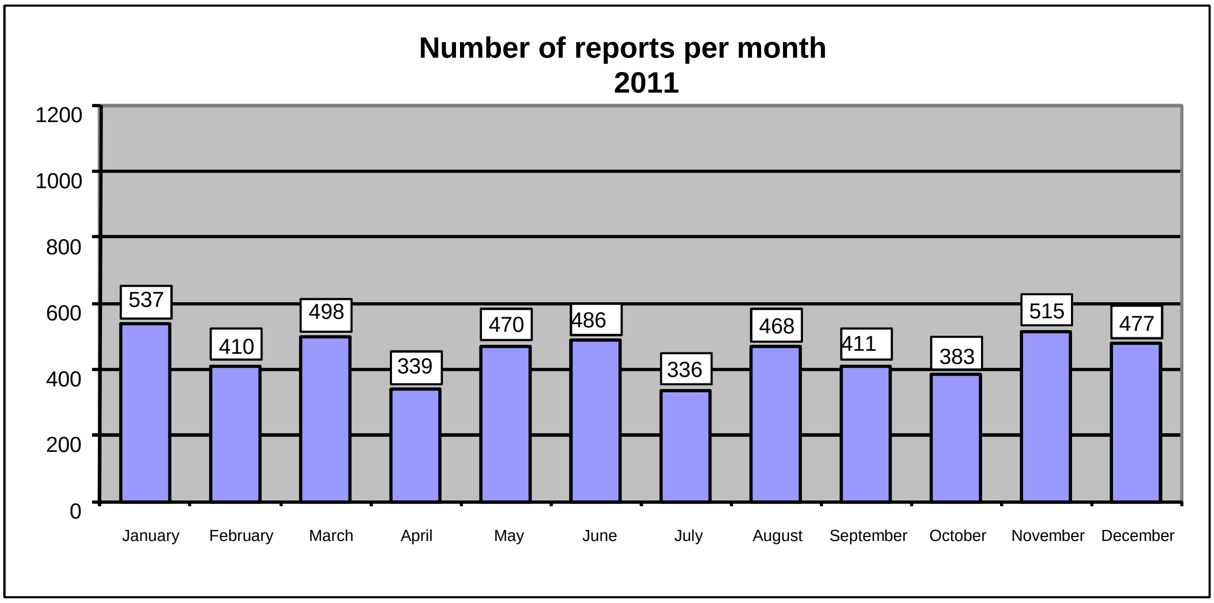

Diagram 2: Reporting volume via www.kobik.ch according to month (total = 5,330 reports)

3. Subject matter of reports

There was a significant decrease in the number of reports concerning *hardcore pornography* (see diagram 3). This category comprises criminal acts subsumed under Article 197 paragraph 3 of the Swiss Criminal Code (SCC). Ninety percent of the reports in this category in 2011 concerned child pornography. The fall in the number of reports in this category directly correlates to the general decline in overall reporting volume. However, it would be wrong to conclude that it is due to a general decrease in the volume of such subject matter on the Internet, a fact that is confirmed through CYCO's day-to-day work and through exchanging information with our national and international partners. The decline in the number of reports is primarily due to the fact that such subject matter is increasingly less visible on the Internet to the general public: paedophile criminals are purposely retreating to closed or difficult-to-access platforms (forums, groups, social networks), which allow them to exchange child pornographic material more discretely and anonymously. Despite the decline in the reporting volume of *hardcore pornography* (especially child pornography), it remains the category yielding the highest number of reports.

Following the decline in the number of reports concerning *general pornography* in 2010, there was a slight increase again in 2011. In contrast, the number of reports concerning *spam* fell for the fourth consecutive year. The number of reports submitted to CYCO does not necessarily reflect the true development of cybercrime, however: although studies on the development of spam indicated a slight decrease in the volume of spam worldwide in 2011[1], none of the studies established a decrease over several years. It is possible that the general public is becoming indifferent to spam and therefore reports fewer incidents to CYCO. Also, spam filters have become more effective, identifying and blocking undesired e-mails early so that the user is less aware of them.

In the category *economic crime*[2] there was a noticeable rise of 53 percent in the number of reports concerning *fraud,* confirming the trend of the previous years. People who purchase goods over online exchange platforms or through classified advertisements (e.g. for cars, apartments, electrical household appliances) are especially vulnerable to mainly foreign fraudsters. On the same websites sellers are cheated out of their money by fraudsters issuing bogus confirmations of payment or by writing bogus checks for more money than the cost of the item and then asking the seller to wire the excess money back to them. Advance fee scams, promising large winnings against payment of a small fee, remain rife. Besides the advance fee, fraudsters are becoming more and more interested in their victim's personal data and identity documents (passports or identity cards). Anyone who discloses personal information must nowadays expect their identity to be misused for fraudulent purposes.

Also, reports on other types of economic crime (especially phishing and money laundering) have increased considerably by 28 percent. People in Switzerland have been subject repeatedly to phishing attacks, whereby the fraudsters have mainly gone after access data to online banking accounts and auction platforms.

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

[2] Economic crime statistics are composed of fraud and economic crime (especially cases of Phishing and money laundering)

The continually high number of queries requesting information or help indicates that CYCO is, indeed, perceived by the population and internet service providers alike as a competence centre for cybercrime.

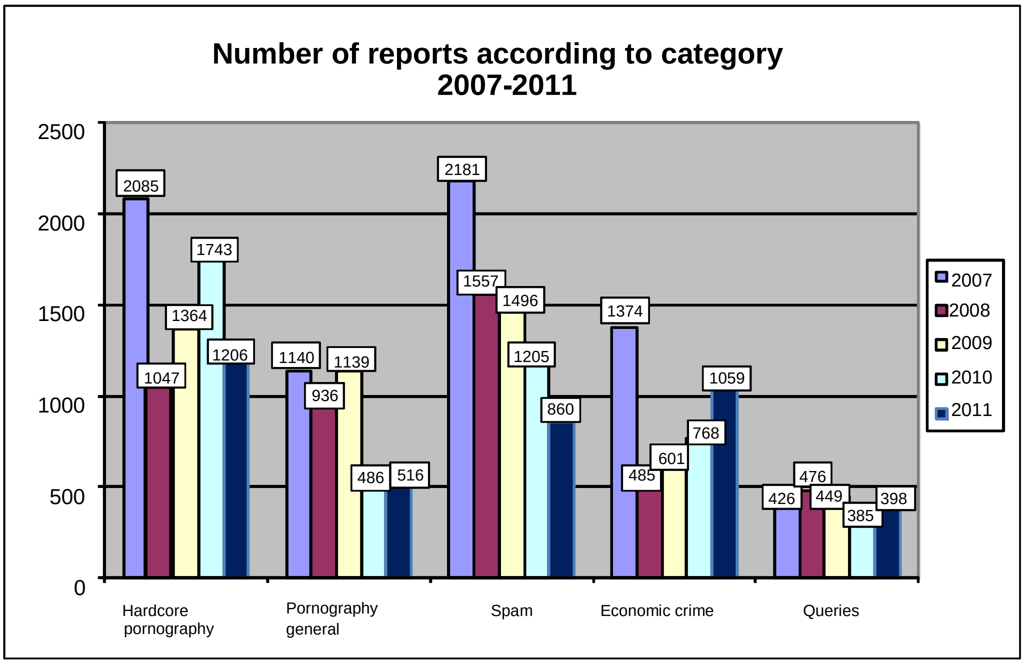

Diagram 3: Absolute comparison of incoming reports from top five categories 2007-2011

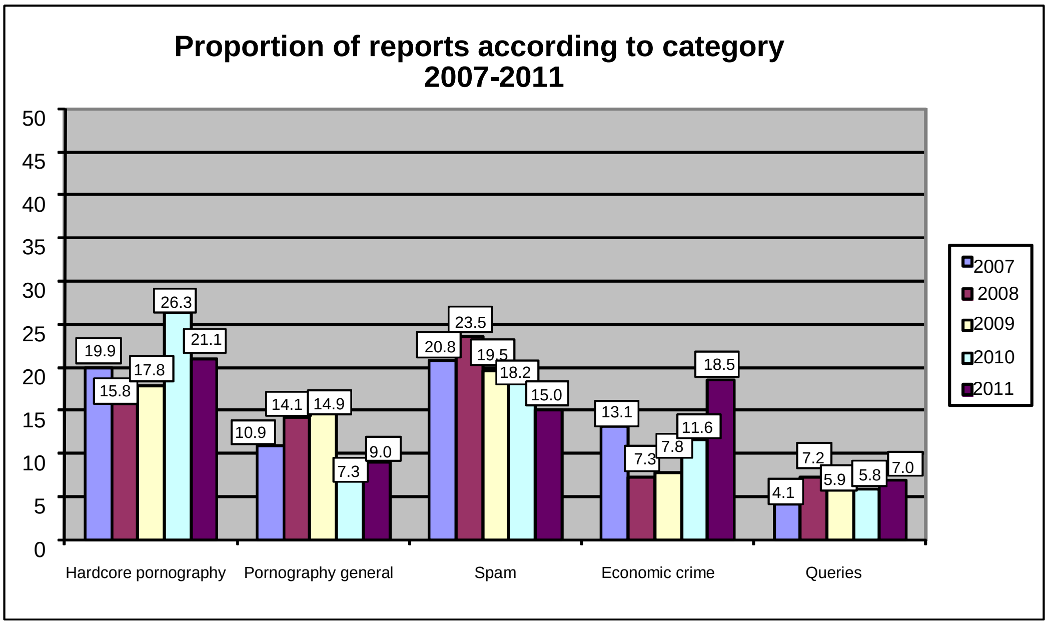

Diagram 4: Relative comparison of reports from top five categories 2007-2011

As every year, incoming online reports covered a wide variety of crimes. Diagram 5 provides an overview of the most important categories in the last five years. There was a noticeable increase in reports from the categories d*efamation* (from 0.70% to 1.97%) and *threat/coercion* (from 0.42% to 0.67%); in such cases criminals are increasingly using social networks to commit these offences. Both categories also include 30 cases of cyberbullying[3] (at least five of which involved minors).

There was also increased reporting volume from the category *unauthorised access to a data processing system* (from 0.44% to 0.84%) and *damage to data* (from 0.57% to 1.29%), CYCO received a number of reports from private individuals concerning attacks to IT systems . Special mention is made here of a malware attack that blocked the computers of numerous people and demanded a fee to unlock them (see case studies in chapter 5). CYCO is monitoring this development closely.

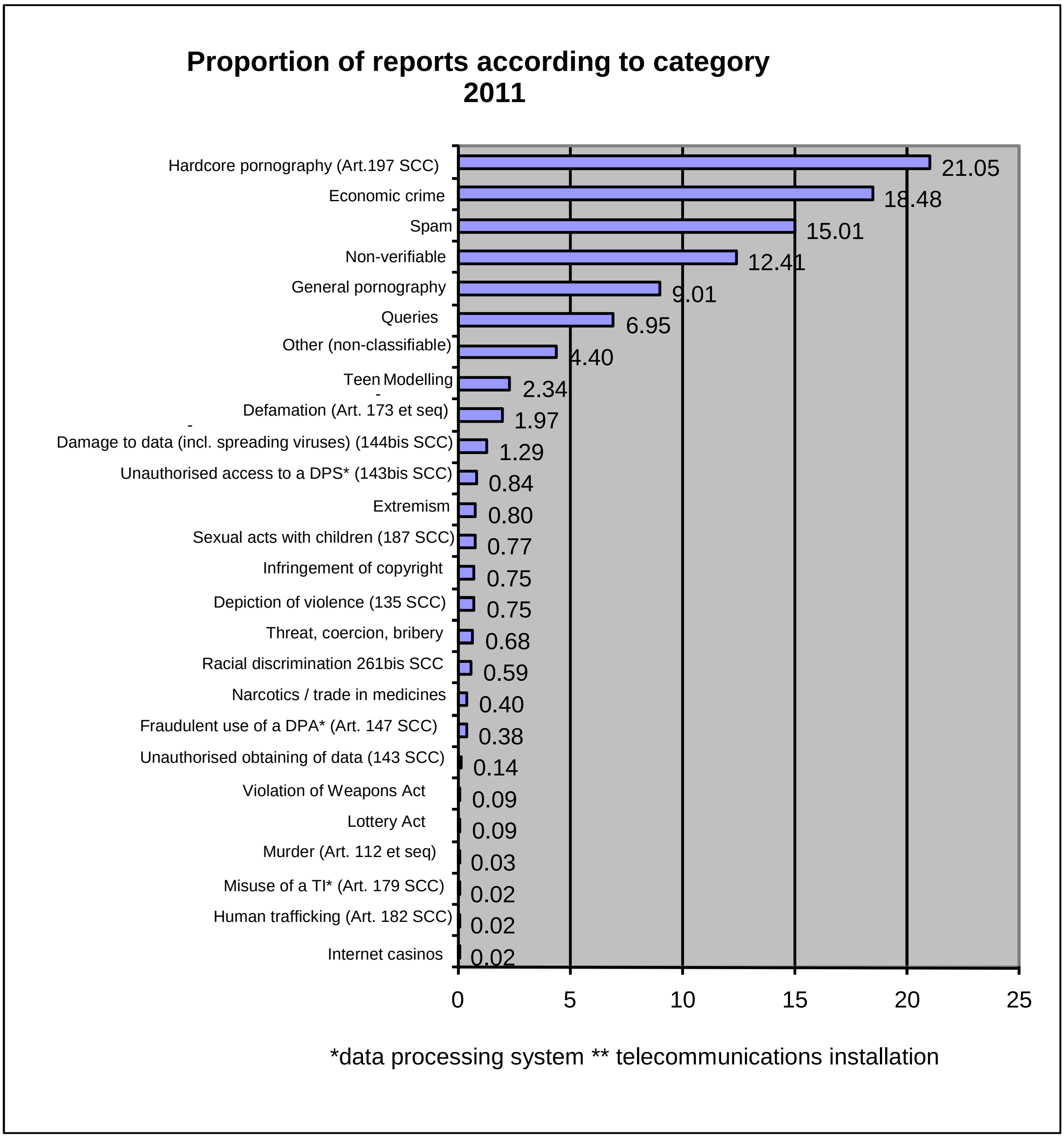

Diagram 5: Proportion of all incoming reports in 2011

[3] Cyberbullying is when modern means of communication are used to publish defamatory texts, pictures or films intended to slander, embarrass or harass another person.

4. Monitoring

Besides receiving and processing online reports from the public, CYCO also conducts its own search for suspect subject matter in areas of the Internet that are less accessible. Thus, CYCO's work is also of a preventive nature. Each year, CYCO's steering committee specifies the area of top priority. In 2011, as in previous years, this was placed on combating paedophile crime on the Internet. However, the steering committee also specified that CYCO should not forget economic crime and Internet crime.

Following active monitoring of the Internet, 225 incident files were forwarded to the cantonal law enforcement agencies in 2011. This figure confirms the high level of the previous year.

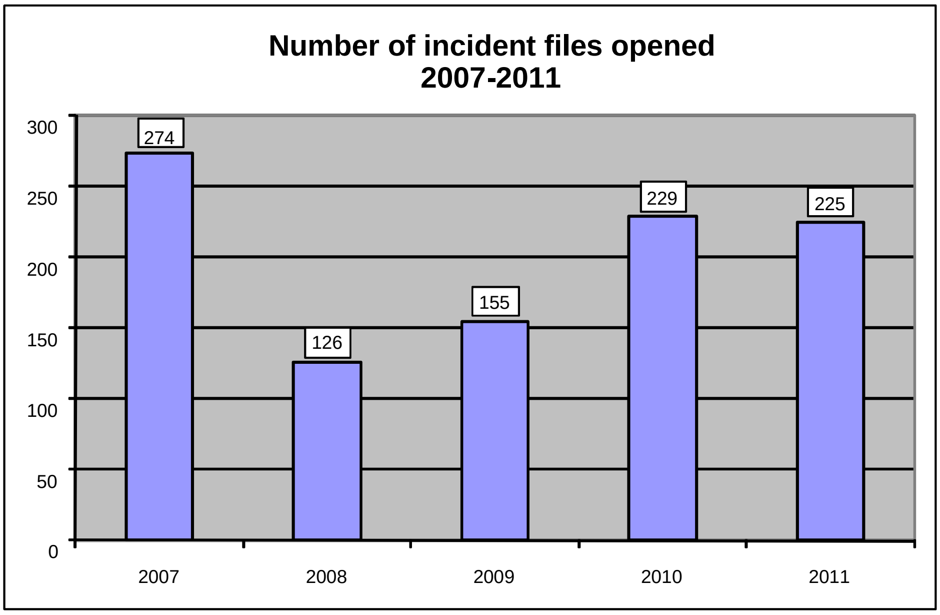

Diagram 6: Incident files resulting from active Internet monitoring

4.1 Active search of P2P networks

Most of the incident files (214 out of 225) were opened as a result of searching P2P networks for Internet users who were actively exchanging child pornography. P2P networks continue to be one of the most popular means of exchanging data relatively anonymously on the Internet.

Although CYCO specifically searches for users in Switzerland, it also identified crimes by two people outside of Switzerland. The findings were transmitted via INTERPOL to the competent authorities in the countries concerned.

4.2 Covert investigations without suspicion in chat rooms and social networks

On 1 January 2011, the new Swiss Code of Criminal Procedure (CrimPC) came into force, withdrawing authority from the federal authorities to conduct covert investigations independent of the presence of suspicion. Jurisdiction now lies with the cantons and must be regulated in each canton's police law. Because only few cantons had the appropriate legal provisions as of 1 January 2011, there was fear that this would create a legal vacuum. To avoid such a situation, the Federal Office of Police (fedpol) and the canton of Schwyz sought a solution to the problem, concluding an agreement of unlimited duration on 23 December 2010. The *Agreement on Co-operation in Police Investigations on the Internet for Combating Paedophile Crime (Monitoring of Chat Rooms)* between the Federal Office of Police (fedpol) and the Security Department of Canton Schwyz contains the legal provisions under which CYCO staff can operate as undercover investigators on the Internet for the purpose of fighting paedophile crime[4]. Thus, CYCO conducts covert investigations explicitly by order and under the supervision of the cantonal police of Schwyz. This ensures the continuity of preventive undercover investigations for the purpose of monitoring online paedophile crime. On 14 January 2011, the competent court in Canton Schwyz appointed six CYCO staff members as undercover investigators. On 11 January 2012, two further staff members were named and the current arrangement was extended to 14 July 2012.

Following the decision of the court in Canton Schwyz, CYCO implemented various technical and operational start-up measures, such as training CYCO staff and defining procedures with the cantons and with other fedpol units. Implementation took a certain amount of time and was dependent on the resources available.

Sixteen cases were processed in 2011 under the agreement. Investigations led to the following measures:

- Five house searches, including questioning of suspects
- Questioning of a suspect
- Four cases currently still under review by public prosecutors
- One case dismissed by public prosecutor
- Four cases were not pursued any further because suspect could not be identified or initial suspicion was not borne out
- One case still being investigated by CYCO

The material seized during the house searches was still being evaluated at the end of 2011.

[4] Operations under Article 9d of the Ordinance of the Canton of Schwyz on the Cantonal Police, dated 22 March 2000 (PolV – SRSZ 520.110).

5. Selected case studies

CYCO processed and co-ordinated a wide variety of cases during 2011. The following case studies are intended to complement the statistics and facilitate a qualitative insight into CYCO's activities.

While monitoring P2P networks, CYCO identified a person in the first quarter of 2011 who was downloading child pornographic pictures and videos, and making them available to others. During the ensuing house search by the cantonal police, the suspect not only admitted to the charge of child pornography, but also to having sexually abused small children on several occasions. The suspect, who was not previously known to the police, was working as a child carer in a day nursery at the time, and his youngest victim was only three years old. CYCO's monitoring of P2P networks helped to expose a paedophile criminal and thus prevent further child abuse.

In another case, a foreign law enforcement agency came across information during covert investigations, indicating that a Swiss national was planning to fly to Great Britain with the intention of sexually abusing a boy there. The information was transmitted to CYCO whose findings revealed that the suspect had already been convicted for sexual crimes against children. Thanks to the close co-operation between the two countries and the e-mail service provider, who facilitated the person's identification, the Swiss man was arrested on entering Great Britain. Material found in his luggage confirmed that the man had, indeed, intended to sexually abuse a child: besides a hotel reservation in his and a child's name, police seized a video camera and a notable quantity of recording tapes. This case illustrates that close and timely co-operation between the countries and the Internet service provider concerned is essential for successful prosecution. Without the covert operations by the foreign law enforcement agency, the paedophile would not have been arrested before committing his crime.

CYCO received an online report containing information about a forum where one user was offering his 13-year old daughter for sexual abuse. CYCO was able to identify the man, who was subsequently questioned by the cantonal police. During questioning the police discovered that the man had no daughter: the statements he had made on the forum had been pure fantasy, lacking any connection to reality. The police subsequently focussed their investigations on the numerous people who had responded by e-mail to the offer and expressed an interest in the girl. Two CYCO investigators assisted the cantonal police in identifying the suspects. This joint operation led to the arrest at the beginning of 2012 of several people in Switzerland, all of whom were arrested on the occasion of a feigned meeting with the 13-year old girl, which had been set up by the police.

CYCO also dealt with other types of Internet crime. For example, in autumn 2011 criminals infected the computers of numerous Internet users in Switzerland through video streaming websites, exploiting vulnerabilities in the software and in the security system of the private computers. The attacks were remarkably complex and sophisticated: the computers were blocked by a malware, demanding via a pop-up window a cash payment before allowing the user to re-access the computer. The fictional sender of the message was Switzerland's Federal Department of Justice and Police, whose corporate logo and website the criminals had copied. Criminal acts similar to this one are committed at regular intervals, the criminals simply substituting the fake website for another and targeting a different group.

A further case, brought to CYCO’s attention using the online reporting form, involved a supposedly HIV-infected man who was offering his services on various forums to infect others with AIDS. Determining in whose jurisdiction the case should come under was difficult, but through CYCO’s monitoring activities sufficient evidence was eventually gathered to appoint the case to the appropriate canton. The culprit was subsequently charged.

6. Recipients of forwarded case files

A total of 263 incident files, resulting from reports submitted by the public using the online reporting form and from CYCO's own monitoring activities, were forwarded to cantonal law enforcement agencies in 2011. Although this represents a slight decrease over the previous reporting period (2010: 299 incident files), it is too early to speak of a reversal of trend.

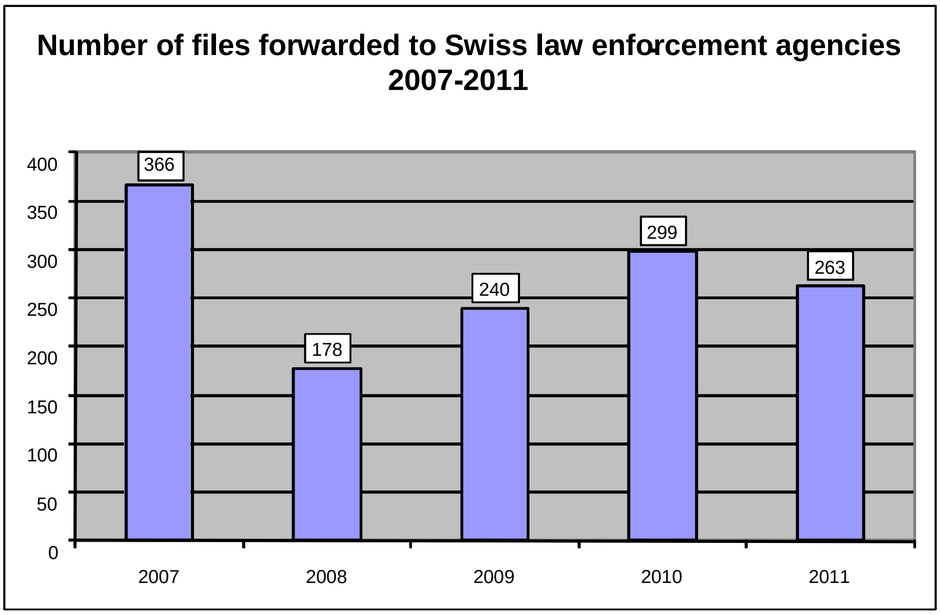

Diagram 7: Incident files forwarded by CYCO to cantonal law enforcement agencies

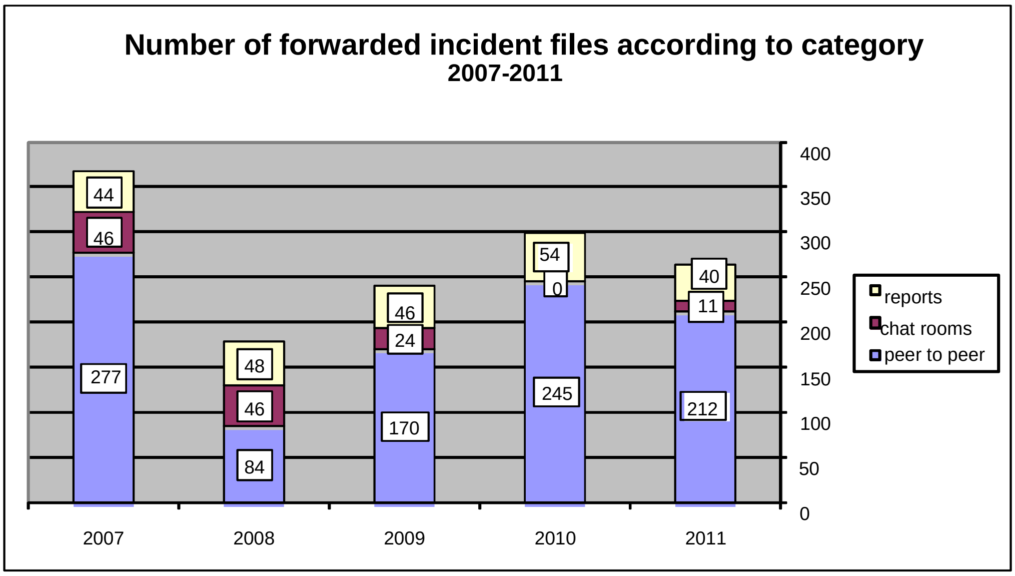

Diagram 8: Forwarded incident files according to category

Diagram 8 shows on which category the incident file was based. The decline in overall reporting volume is partly due to the decrease in the number of files from the category *reports.* This category comprises incident files that were based on an online report sent by a member of the public to CYCO.

The number of forwarded incident files from the category *P2P* also fell in the year under review, from 245 cases in 2010 to 212 cases in 2011. This represents a decline of 14 percent. A detailed analysis of this statistic shows that the decline was due to a decrease in reports particularly in the months of July, August and September; the months when systematic and technical procedures relating to the P2P-scan project were being improved and expanded.

Eleven cases concerned sexual acts with children (Art. 187 SCC) and were identified by CYCO during covert investigations in *chat rooms*.

As in previous years, CYCO forwarded most incident files to the most densely populated cantons such as Bern, Zurich and Vaud (see diagram 9). Some incident files were forwarded in-house to fedpol's own operative sections *General, Organised and Financial Crime, Sexual Offences against Children/Pornography,* or *National Security Investigations*.

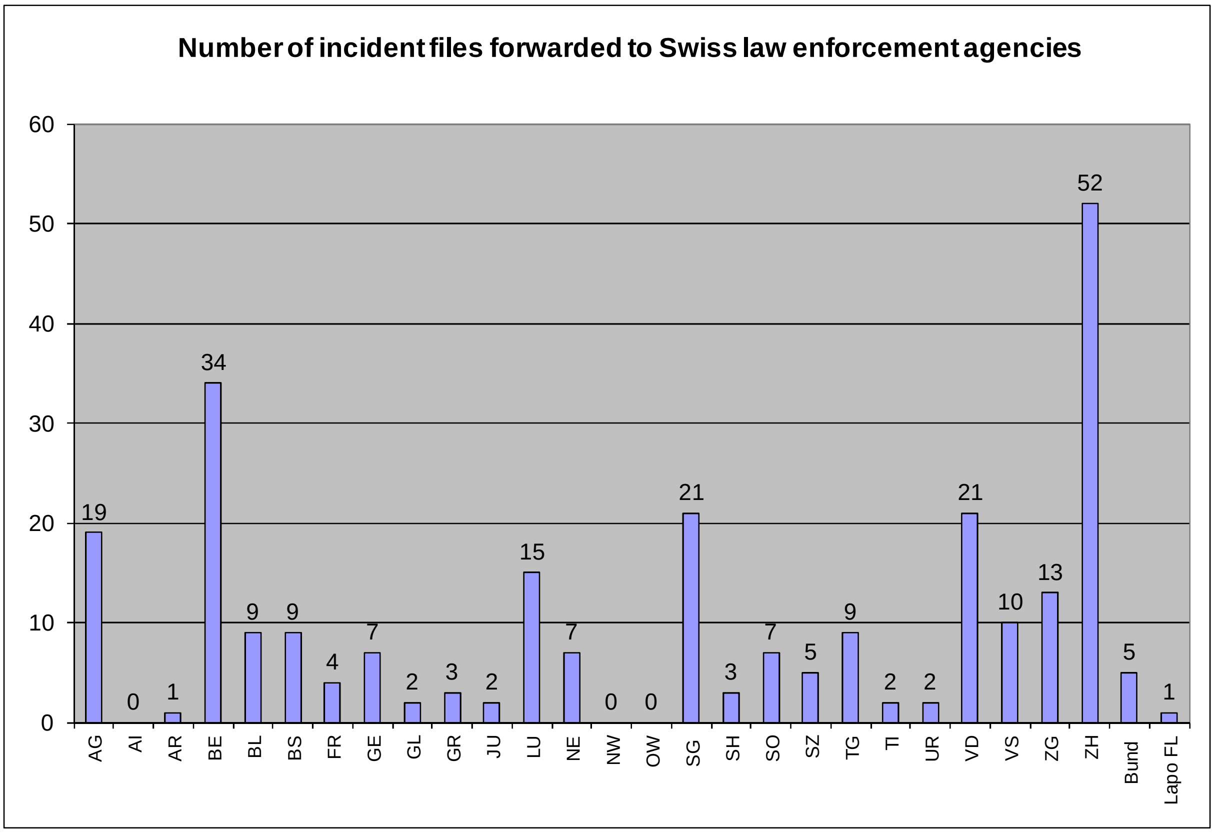

Diagram 9: Total number of incident files forwarded to Swiss law enforcement agencies (federal and cantonal) and the authorities of the Principality of Liechtenstein FL (total = 263 files)

Over 50 cases were forwarded to foreign law enforcement agencies via Europol and INTERPOL. Most of these cases concerned websites containing child pornography or involving other types of cybercrime, all of which had been brought to CYCO's attention using the online reporting form. In addition to the cases forwarded through INTERPOL or Europol, CYCO also reported websites containing illegal subject matter directly to the appropriate Internet service provider with a request to delete the material in question.

7. Responses from the cantons

If CYCO has a strong suspicion that a criminal offence is being committed, it forwards the file for further processing to the cantons (see diagram 7). 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.

Analysing the responses from the cantons is an important tool for determining the efficiency of CYCO's work and the quality of its incident files. The large majority of incident files (74 percent) resulted from active monitoring of P2P networks and thus concern people who are actively exchanging illegal material containing child pornography.

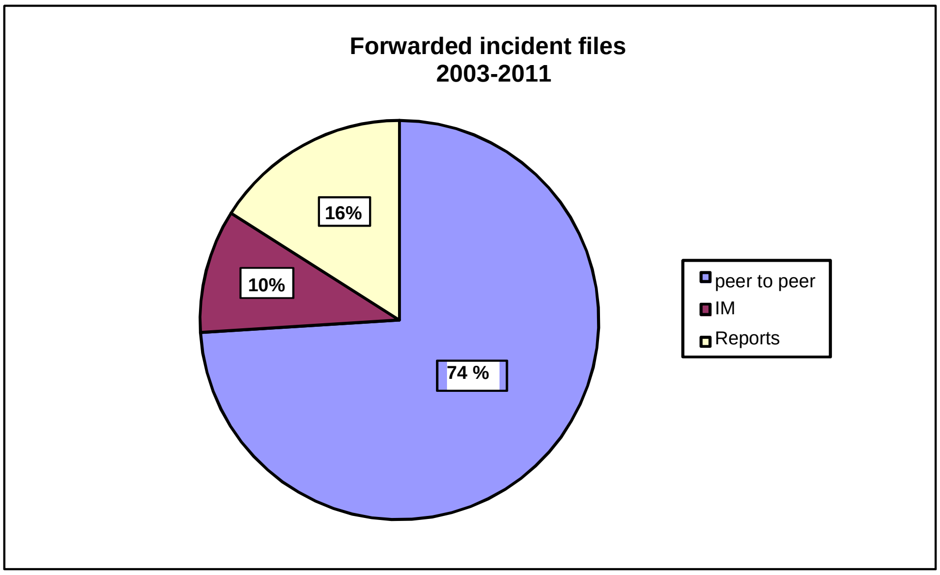

Diagram 10: Total number of incident files forwarded to cantonal law enforcement authorities since 2003[5]

[5] IM = Instant Messaging. This is a method of communication where several participants communicate simultaneously by text message (chatting).

7.1 Responses from the cantonal police

As seen in diagram 11, 91 percent of all cases forwarded by CYCO resulted in a house search by the cantonal police. Reports based on the category p*eer-to-peer* led to a house search in more than 98 percent of the cases, whereas cases from the category *reports* seldom triggered a house search (see diagram 10).

Ninety-five percent of house searches were based on an incident file from the category *peer-to-peer*.

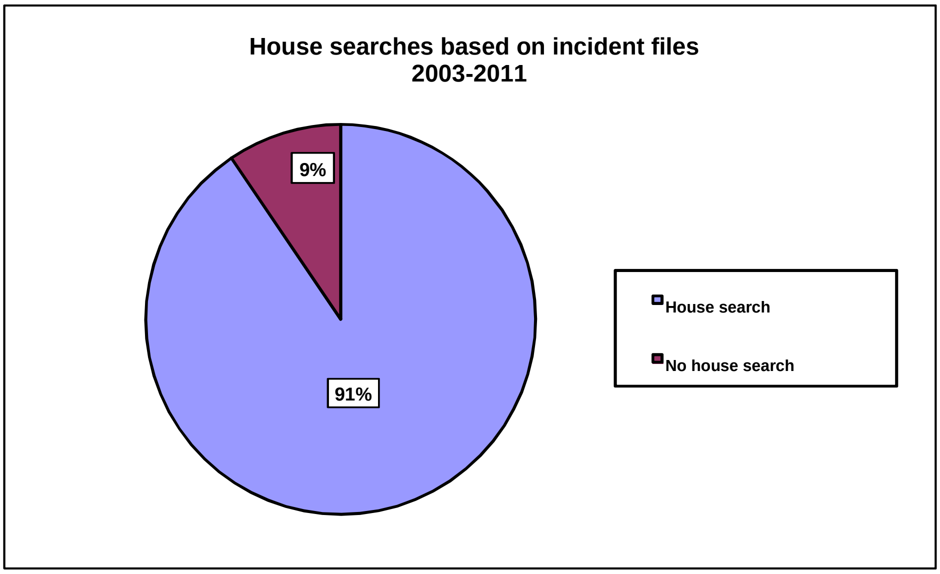

Diagram 11: House searches (791 responses)

Eighty-four percent of house searches conducted as a result of incident files yielded illegal material. Only 16 percent of house searches yielded no criminally relevant material. There are many reasons why a house search may be unsuccessful, and it is not always easy for law enforcement agencies to identify the reasons.

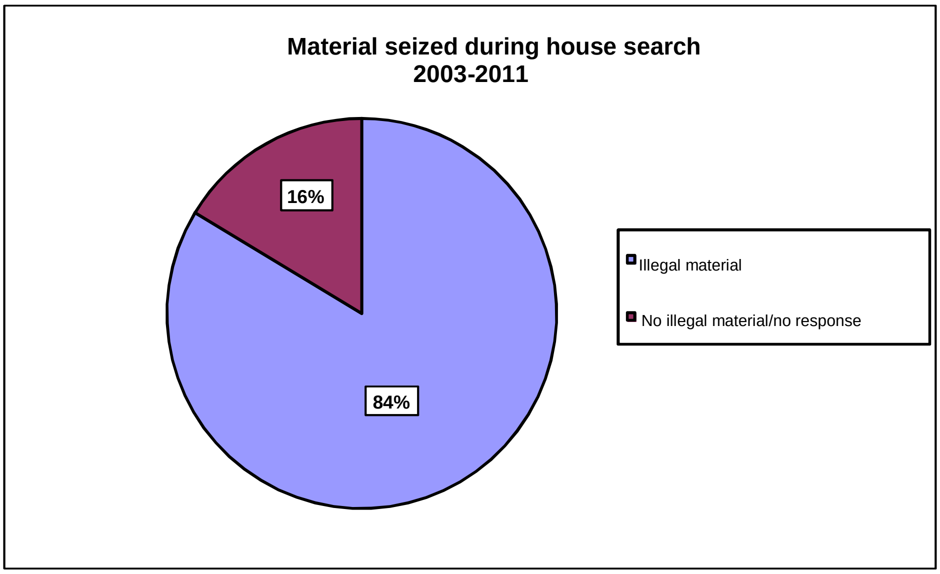

Diagram 12: Seizure of illegal material (716 house searches)

Ninety-four percent of the illegal material seized related to child pornography. This high percentage is not surprising considering that CYCO focussed its monitoring of P2P networks on this crime and the majority of incident files was based on these monitoring activities. It is also worth mentioning that in more than half of the cases other elements of illegal pornography (see Art. 197 SCC) came to light (see Diagram 13). For example, in half of the house searches law enforcement agencies seized pornography involving animals.

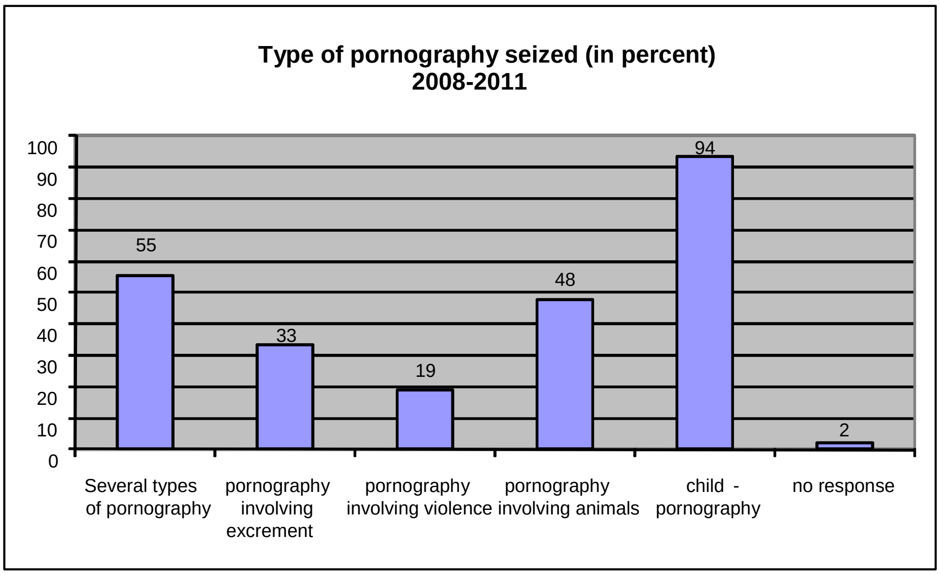

Diagram 13: Type of material seized (251 responses)

Of the house searches that yielded illegal material, 80 percent yielded illegal video data and 63 percent illegal picture data. Numerous house searches yielded both kinds. In total, the house searches conducted in 2011 resulted in the seizure of tens of thousands of video images and hundreds of thousands of picture images.

7.2 Responses from the cantonal judiciary

In 90 percent of the 589 responses from the cantonal judiciary, the case in question resulted in a conviction.

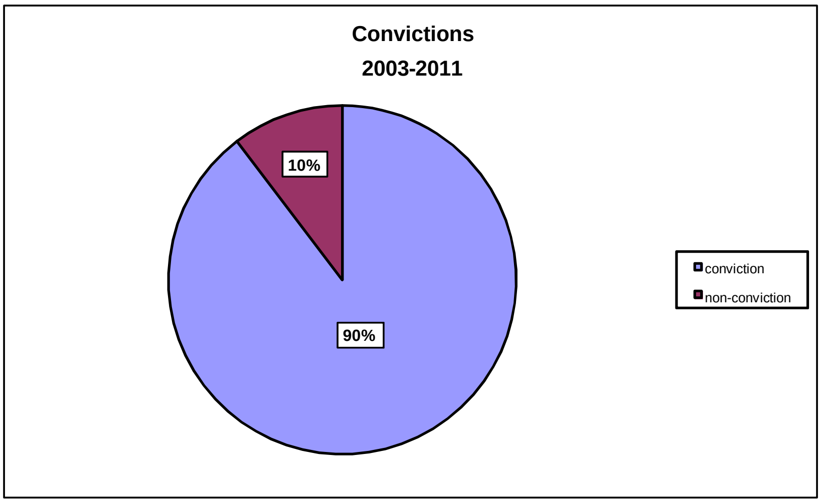

Diagram 14: Percentage of convictions based on 589 responses from cantonal judiciary

Most convictions were for the possession of hardcore pornography (Art. 197 SCC), especially for the acts defined under Article 197 paragraph 3 and 3bis[6]. In a few cases there were convictions for violations of Article 187 paragraph 1 SCC (sexual acts with children).

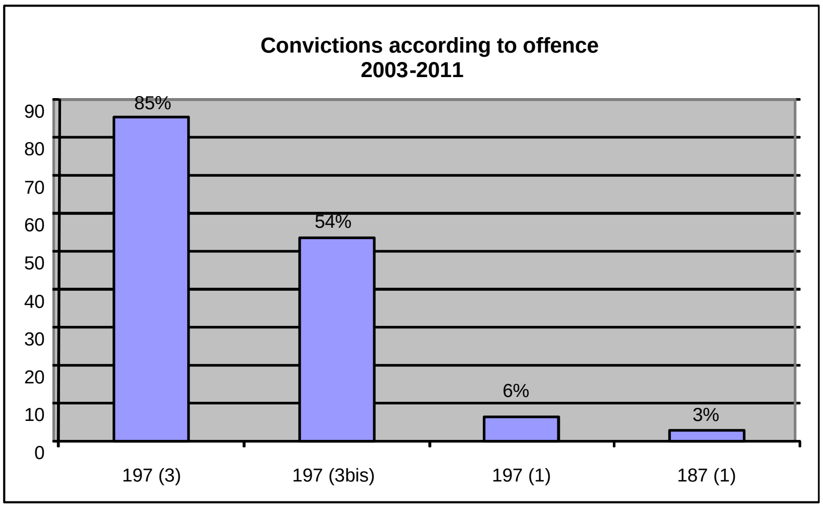

Diagram 15: Convictions according to offence (total 532 convictions)

[6] Paragraph 3. Any person who produces, imports, stores, markets, advertises, exhibits, offers, shows, passes on or makes accessible to others articles or representations as described in Paragraph 1 above that depict sexual acts involving children or animals, human excrement, or acts of violence shall be liable to a custodial sentence not exceeding three years or to a monetary penalty. The objects shall be seized.
Paragraph 3bis. Any person who acquires, possesses or procures via electronic media articles or representations as described in Paragraph 1 above that depict sexual acts involving children or animals or sexual acts involving violence shall be liable to a custodial sentence not exceeding one year or to a monetary penalty.

In most cases, the person was convicted to a monetary penalty (i.e. a penalty that involves the payment of a sum of money to the state and that is specified as a number of daily penalty units, depending on the blameworthiness of the offender, and the financial level of which is based on the personal and financial circumstances of the offender). In many of these cases, the convicted person also received a fine. In 91 percent of the convictions, the monetary penalty was suspended. In only a few cases was the person sentenced to communal work or ordered to undergo therapy. The severest penalties such as a custodial sentence or an unconditional monetary penalty were only pronounced on habitual offenders.

In approximately two-thirds of the cases the fine amounted to less than CHF 1,000, and in 16 percent of cases to between CHF 1,000 and CHF 2,000. Only 18 percent of the fines were higher than CHF 2,000. Forty-eight percent of the monetary penalties were fixed according to a maximum of 50 daily penalty units; in 35 percent of the cases the monetary penalty was fixed at between 51 and 100 daily penalty units. Only in 17 percent of the cases was the monetary penalty fixed at over 100 daily penalty units. In 24 percent of the cases the daily penalty unit was fixed at between CHF 1 to CHF 50, in 38 percent of the cases between CHF 51 and CHF 100, and in 38 percent of the cases at over CHF 100.

The fines mostly ranged between CHF 500 and CHF 3,000. The highest fine was CHF 6,000. Generally, the convict also has to pay the costs of the proceedings, which are often many times higher than the actual fine. Fines were mostly fixed at between 20 and 200 daily penalty units at between CHF 20 and CHF 200.

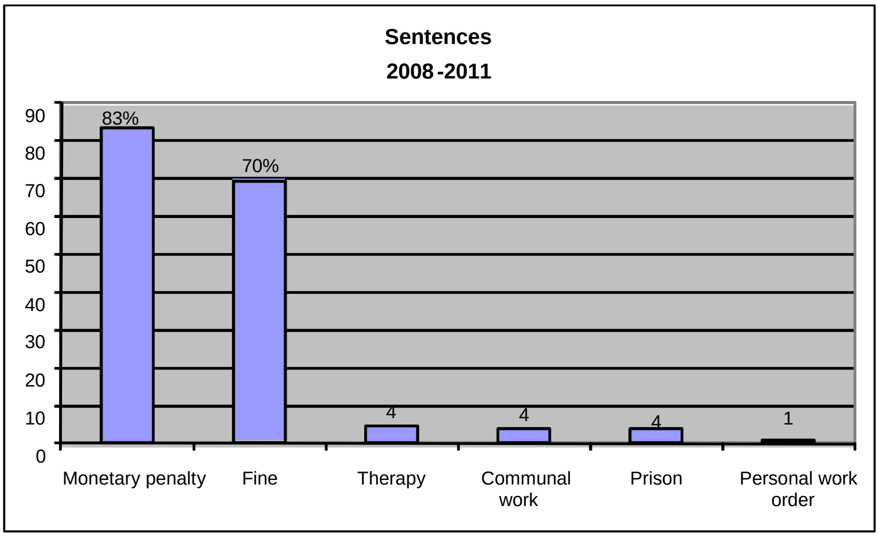

Diagram 16: Sentences (242 responses)

8. Working groups

8.1 National

In 2011, CYCO was represented in various national working groups on crime prevention:

Child Abuse Working Group: CYCO is an active member of the national Child Abuse Working Group, together with fedpol's Paedophile Crime and Pornography Unit, NGOs, cantonal representatives and Swiss Crime Prevention

Media Protection and Media Literacy for Young People: CYCO is a member of the steering group, which is responsible for developing the programme, and of the support group, which is responsible for 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. The highlight of the programme was the "Media Skills Day", which took place for the first time on 27 October 2011 in Freiburg.

Swiss Crime Prevention: CYCO has represented fedpol since 2011 in this new commission, established to develop projects and tools for preventing crime in the cantons and to evaluate their implementation.

Security and Confidence Action Plan: CYCO continued to be involved in developing the "Security and Confidence Action Plan" (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.

IT Investigators and *Monitoring Telecommunications*: thanks to CYCO's participation in the "IT Investigators" and "Monitoring Telecommunications" working groups, it was able to stay abreast of technical developments and law enforcement in 2011.

8.2 International

Since 2011, CYCO has been a new member of Europol‘s *Analysis Work Files (AWF) Cyborg* whose goal is to combat transnational cybercrime, placing special emphasis on phishing, botnets and hacking.

CYCO is also involved in the *CIRCAMP project* to fight the distribution of child pornography on the Internet.

As in previous years, CYCO continued to be represented in the *European Financial Coalition* working group in Brussels.

CYCO also participated in the Council of Europe's *Cybercrime Convention Committee (T-CY)*, based in Strasbourg. In 2011, the Convention celebrated its tenth anniversary and the entry into force of the Convention in Switzerland on 1 January 2012.

9. Projects

9.1. Co-operation with Swiss Internet access providers to filter websites containing child pornography

Since 2007, CYCO has assisted the major Swiss Internet service providers in blocking foreign websites containing child pornography, which have not been blocked despite having being reported to the appropriate foreign law enforcement agency. CYCO sends Internet providers a regularly updated list of websites that contain child pornography. Based on their corporate ethics and general terms and conditions[7], Internet service providers block access to the illegal websites and redirect the user to a « *Stop* page ».

As part of this project to block websites – in which several other countries also participate - CYCO collaborates closely with INTERPOL, and this co-operation was further strengthened in 2011. INTERPOL has compiled a «worst of» list, which serves as a basis for Switzerland's list, which is supplemented by websites discovered from CYCO's own monitoring activities. INTERPOL's list is updated on a daily basis and is integrated into CYCO's list. CYCO also reports new websites to INTERPOL to supplement its own «worst of» list.

9.2 National Data and Hash Value Database (NDHS)

Data (e.g. pictures, videos, etc.) seized during investigations into child pornography offences is transmitted to CYCO by the cantonal authorities. CYCO subsequently generates a hash value[8] for each piece of data and stores the value in the National Data and Hash Value Database. The list of hash values is made available to the cantonal authorities over the JANUS community[9]. The competent cantonal authorities also generate a hash value for the data they seize. The hash values generated by CYCO and the cantonal authorities can be compared for matches. This enables investigators to identify duplicate images without having to view the content, a procedure that is time-saving and, in particular, reduces emotional stress.

CYCO made considerable progress with the project. The planning phase was completed in collaboration with the cantons, and fedpol set up the necessary infrastructure. Representatives from all cantons were trained in the use of the database, and CYCO received the first set of images and videos from the cantons

The time required to classify and verify data has been considerably shortened thanks to an image identification software developed by a Swiss company in collaboration with fedpol. The software will also be used to assist in operations.

[7] General terms and conditions (GTC)

[8] Clearly definable parameter of an image (digital fingerprint)

[9] Intranet, that provides police corps throughout Switzerland with information

9.3 National Strategy for the Protection of Switzerland against Cyber Attack (previously known as the National Strategy for Cyber Defence)

On 10 December 2010, the Federal Council appointed the Federal Department for Defence, Civil Protection and Sports (DDCPS) to develop a national strategy on cyber defence and named Major General Kurt Nydegger as project manager. The aim of the strategy is to protect critical infrastructures in Switzerland against cyber attack. The strategy must contain precise information on the implementation of measures and their consequences in terms of time, costs, capabilities, legal implications and resources. The Federal Council is expecting a definite national cyber defence strategy containing various options in the first quarter of 2012. CYCO has been on the project team since May 2011 and will represent the interests of federal and cantonal law enforcement agencies on implementation of the strategy.

10. Parliamentary procedural requests at federal level

10.1 Parliamentary procedural requests submitted in 2011:

Child and youth protection / paedophile crime

Interpellation Pasquier: Protection of children from sexual exploitation and sexual abuse
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113141

Motion Savary : Pornography on the Internet: Taking precautions.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113314

Question Bruderer-Wyss: Sanctioning sexual contacts with 16 to 18 year olds.
http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20115351

Question Rickli : Paedophile register.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20115008

Motion Schmid-Federer: Making *Grooming* a punishable offence.http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20114002

Federal Council item of business concerning the Code of Criminal Procedure, Military Code of Criminal Procedure and the Juvenile Criminal Law Act: Non-applicability of statutory limitation regarding sexual and pornographic act on children.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20110039

Others

Interpellation Amherd: Increasing monitoring of the Internet.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113862

Postulate Eichenberger-Walther: National network of police competence centres.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113642

Question Leutenegger-Oberholzer: Deploying trojans at federal level.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20115541

Question Reimann: Dubious practices by PayPal in Switzerland.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20115438

Question Schmid-Federer: Status of the prevention campaign by the Federal Social Insurance Office after one year.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20115198

Postulate Amherd : Statutory provisions for social media.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113912

Postulate Schmid-Federer : Basic law on information and communication technology.
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20113906

Petition: Prohibiting killer games
http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20112005

10.2 Legal developments

Fighting cybercrime also poses new challenges in the field of law-making and case law. This chapter looks in detail at specific national and international legal developments.

Decision no. 6B_744/2010 by the Federal Supreme Court

In 2011, the Federal Supreme Court was confronted with the question of whether child pornography held in a computer's cache is a punishable offence. In its decision of 12 May 2011 the court held that Article 197 paragraph 3bis SCC includes all electronic data and types of storage. If a user has accessed a website, the data is automatically stored on a temporary Internet file on the hard drive. This data is recalled faster if the user revisits the website. Using common and free-of-charge software (e.g. Cache Viewer or Cache Reader) the stored websites can also be accessed in offline mode. The illegal possession of hardcore pornography according to Article 197 paragraph 3bis SCC encompasses the ability and will to exercise domination. Although the average Internet user has no influence on the temporary storage of data in a cache and, therefore, this does not constitute possession that can be qualified as physical control, any person who over a period of time deliberately visits websites containing hardcore pornography does not confine himself merely to viewing the website. By repeatedly accessing such websites, the person is demonstrating his will to exercise domination. Although the data is temporarily stored automatically, it is up to the user to decide whether he deactivates or deletes the temporary Internet file, since it must be assumed that it is a generally well-known fact these days that accessed websites are temporarily stored in the cache.

Acquiring data according to Article 197 paragraph 3bis SCC is given if a user by means of a password has lasting and unlimited access to a website containing hardcore pornography and can have this data freely at his command. The same applies for the various elements of possession: the element of possession is given if access to illegal pornographic data is possible at any time, for example via a temporary Internet file. Only in this way can the legislator achieve total culpability regarding hardcore pornography.

Federal Council confirms copyright law

In November 2011 the Federal Council implemented a postulate of March 2010 from Géraldine Savary, a member of the Council of States and of the Social Democrat Party from Canton Vaud. The Council of States had commissioned the Federal Council to examine whether measures to combat the violation of copyright law were necessary. The report found that every third person over the age of 15 in Switzerland downloaded music, films and games from the Internet free of charge. It also found that, although the Internet had fundamentally changed the use and acquisition of music, films and games, it did not have a negative effect on artistic creativity. The Federal Council therefore declined to amend copyright law. For Swiss Internet users this means that they may continue to download films and songs protected by copyright without prosecution providing it is for private use.

Cybercrime convention

Switzerland has ratified the Council of Europe Convention on Cybercrime and is thus party to greater international efforts to fight computer and Internet crime. The Convention entered into force in Switzerland on 1 January 2012, at the same time the Federal Council brought the necessary legal amendments into force.

The Council of Europe Convention on Cybercrime is the first international treaty on fighting computer and Internet crime. Under the Convention member states are bound to adopt the necessary legislative measures to make computer-related fraud, data theft, computer-related document forgery or unauthorised access to a secure data processing system a punishable offence under their national law. Member states must also undertake to impose sanctions on child pornography and the violation of copyright law. Further, the Convention provides for the collection and storage of evidence in electronic form and aims to ensure that investigating authorities have fast access to electronically processed data before it is altered or destroyed during proceedings. Finally, the Cybercrime Convention aims to foster fast, effective and comprehensive co-operation between the member states.

Implementing the Convention required a small amendment to the Swiss Criminal Code and the International Mutual Assistance Act. Amendment to the Swiss Criminal Code has made the step before unlawfully accessing a secure data processing system (i.e. hacking) also a criminal offence: thus any person who markets or makes accessible passwords, programs or other data that he knows or must believe are intended to be used to commit an offence has himself also committed a criminal offence and is now liable to a punishment. The International Mutual Assistance Act was amended to in future allow the competent Swiss authority in certain cases to transmit traffic data to the requesting authority for investigative purposes before completion of the mutual assistance procedure. This data, which provides information on a communication’s origin, destination, route, time, date, size or duration may, however, only be used as evidence once the final decision on granting mutual assistance and the extent thereof has become legally valid.

The task of ensuring a 24/7 single point of contact as required under Article 35 of the Convention has been designated to fedpol’s Operations Centre, which is assisted by CYCO in processing inquiries as foreseen under the Convention.

11. Media coverage, training and conferences

11.1 Media coverage

CYCO and its activities enjoyed widespread media coverage in 2011, especially on CYCO's preventive undercover investigations and on some spectacular cyber attacks such as the DDoS attacks[10]. On the whole, media coverage was positive.

11.2 Training and conferences

CYCO staff participated in the following conferences, international conventions and training modules in 2011:

In Switzerland :

- IT Investigators Convention
- Media Skills Day (as part of the national *Youth and Media* programme)

Abroad :

- RIPE NCC Meeting, London
- Octopus Interface, Strasbourg
- E-Crime Congress, London
- UN Expert Meeting on Cybercrime, Vienna
- OSCE Conference on Cybersecurity and Cybercrime, Vienna
- New Technologies Symposium, Federal Criminal Office Wiesbaden
- Fighting Cybercime : cooperation between law enforcement agencies and the internet industry», Academy of European Law, Trier
- World Summit Information Society (WSIS)
- Child Sexual Exploitation Experts Conference» Europol, The Hague

[10] Distributed Denial of Service

12. Partnerships and contacts

12.1 Co-operation with other federal agencies

CYCO co-operated closely in 2011 with other federal agencies on fighting cybercrime. In-house its efforts were focussed on collaboration with the Federal Criminal Police's *Paedophile Crime and Pornography*, *IT Investigators*, *National Security*, and *Undercover Investigations* units, and with the main division for International Police Co-operation. Co-operation between CYCO and the *Paedophile Crime and Pornography* unit was especially intensive on account of a mutual topical interest and six new staff positions authorised by the Federal Council to fight cybercrime.

Throughout 2011, 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), the Federal Office for Social Insurance (FSI), Swissmedic and the Lotteries Commission (Comlot).

Existing co-operation with Swiss Crime Prevention (SCP) was further strengthened when CYCO joined the SCP's expert commission as fedpol's official representative.

12.2 Working meetings and exchanging experiences with the cantons

CYCO had contact with various cantonal police corps and public prosecutors offices. Besides the standard exchange of experience, working meetings on undercover investigations and the National Data and Hash Value project took place.

In the context of the National Cyber Defence Strategy and on account of various inquiries on cybercrime on the political level, CYCO strengthened it contacts and established a regular exchange of information with the Swiss Police IT Congress.

12.3 Co-operation with Action Innocence (AIG)

For several years CYCO has collaborated closely in fighting child pornography with the NGO[11] Action Innocence (AIG). Thanks to strong and financial support from this NGO, CYCO has been able to carry out and develop the monitoring of P2P networks successfully. Co-operation with AIG is very important because a clear majority of our monitoring activities are only possible thanks to the software made available to CYCO by AIG. Also, AIG assists CYCO by developing additional projects that are expected to be implemented as part of efforts to fight paedophile crime.

[11] Non-Governmental Organization

12.4 Co-operation with industry (Public Private Partnership, PPP)

Co-operation with industry is becoming increasingly important in fighting cybercrime. In 2011, various meetings took place between CYCO and representatives from the Internet sector and with companies involved with new technologies. New contacts forged to various Internet service providers were a positive development: such co-operation is essential for investigating suspects and dubious IP addresses as part of police investigations because fighting cybercrime requires fast and hands-on action by all those involved.

12.5 External visitors

CYCO received various external visitors in 2011, giving it the opportunity of presenting its work and drawing visitors' attention to the difficulties and correlations within the field of cybercrime. CYCO also received visits from various journalists who were granted an insight into the work performed by its specialists.

12.6 International co-operation

In addition to the above-mentioned international conferences and working groups mentioned in chapter 8.2, CYCO fostered contact with various international partners. The purpose of these exchanges is primarily to develop joint procedures to improve co-operation. International co-operation is no longer only focussed on fighting paedophile crime, but increasingly also on combating other forms of Internet crime and economic crime. Especially in the context of operations such as undercover investigations, direct exchange with foreign law enforcement agencies is of great benefit.

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 (paedophile 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 2011

It is difficult to draw conclusions about the development of Internet crime or the presence of illegal web content based on the volume of incoming reports. These statistics probably reveal more about the willingness on the part of the public to report illegal websites or society’s perception of Internet crime. There may be various reasons for the decline in reporting volume: one explanation could be that certain types of Internet crime have now become so common that they tend to be trivialised by the public, and victims therefore refrain from reporting the incident to CYCO. However, it is important that the public continue to report such incidents so that the extent of Internet crime can be registered and countermeasures can be taken. Another reason for the decrease in reporting volume may be that such subject matter is becoming less visible on the Internet to the general public: paedophile criminals are purposely retreating to closed or difficult-to-access platforms (forums, groups, social networks), which allow them to exchange child pornographic material more discretely and anonymously. This trend is likely to continue, given the rapid technological development of the Internet. For this reason undercover police investigations on the Internet for the purpose of identifying and solving crime will continue to increase in importance.

CYCO expects the number of computer-related fraud cases, committed by criminals operating from abroad, to continue rising. The rising trend has been observed for a number of years and continued in 2011. Prevention work and public awareness campaigns on the correct use of the Internet are therefore key measures in combating this form of crime. Another important tool in fighting this and other types of Internet crime is co-operation between all key players such as governments, law enforcement agencies, Internet service providers and regulators. CYCO is already a member of various national and international working groups whose goal is combating specific forms of Internet crime, and it is likely that co-operation between private and public institutions (Public Private Partnership) will become in the future an ever more important factor in combating cybercrime.