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

Cybercrime Coordination Unit Switzerland CYCO

Annual Report 2012

FOREWORD

by Christoph Neuhaus, Cantonal Councillor and Chairman of the CYCO Steering Committee

“Where there is light, there is also shadow”, as the saying goes. There is also strong shadow in the areas of the Internet that are hard to access, where criminals are involved in especially shady activities. This precisely where the Cybercrime Coordination Unit Switzerland (CYCO) must shine light into the darkness, act and remain active, expose criminal conduct and bring those responsible to justice. As the national point of contact for people who wish to report suspect Internet content, CYCO is unfortunately experiencing a veritable boom in its activities. Last year 55% more cases were reported than in the previous year. For the first time, more reports were received of economic crimes (37%) than reports on illegal pornography (33%).

CYCO continues to carry out its key assignments competently, but it also striking out in new directions. For example, a first Cybercrime Forum for public prosecutors offices and CYCO has been held. One of the aims of this event was to resolve current uncertainties in the prosecution service over at public prosecutors offices on how to deal with cybercrime and in relation to the technical options.

However, CYCO not only deals with reports from the public. By patrolling the internet irrespective of any specific suspicions, it also helps to prevent crime in the less accessible regions of cyberspace. Every year the CYCO Steering Committee reviews the focus of internet searches. In 2012, the priority was once again combating paedophile crime on the Internet. When determining these priorities, however, the Steering Committee also expressly stated that CYCO must not neglect economic offences and cybercrime in the narrower sense. This is a strategy that has been endorsed by the latest figures. CYCO and its activities have become indispensable.

Cybercrime Coordination Unit Switzerland (CYCO)
Nussbaumstrasse 29
3003 Bern
www.kobik.ch
www.cybercrime.ch

Published: 23rd April 2013

Table of Contents

1. A Brief Overview of 2012

- In 2012, the Cybercrime Coordination Unit Switzerland (CYCO) received 8,242 online complaints. This represents an increase of 55 per cent over the previous year.

- Thirty-nine per cent of these complaints concerned the category of *property offences*. This was the first time that CYCO had received more complaints relating to economic crime than to the category of *illegal pornography (*33% of complaints), despite a marked increase in the number of reports in this latter category when compared with 2011.

- A total of 383 complaints led directly to an incident file being sent to national or international authorities and organisations due to the criminal relevance of the complaint

- By actively monitoring P2P networks, CYCO identified 417 people who were exchanging child pornography.

- Covert investigations resulted in 33 cases of criminal charges being filed against suspects by the cantons.

- The National Image Hash Value Database (NDHS) came into operation in October 2012 following successful completion of all test runs and system adjustments.

- On 27 June 2012, the Federal Council approved the National Strategy to Protection Switzerland against Cyber Risks, a project that CYCO was actively involved in. Through this strategy, the Federal Council, working with federal and cantonal authorities, industry and internet operators aims to minimise the cyber risks that critical infrastructures in Switzerland face on a daily basis.

2. CYCO, the Coordination Unit

The Cybercrime Coordination Unit Switzerland (CYCO) is Switzerland's central contact office for anyone wishing to report suspicious content on the Internet. Following an initial analysis and securing of the relevant data, reports filed using the online complaints form (www.cybercrime.ch) that contain evidence of a criminal offence are forwarded to the appropriate law enforcement agencies in Switzerland or abroad.

2.1 Reports received

In 2012, CYCO received **8,242** online complaints concerning suspicious web content. This represents a marked increase of 55 per cent over the previous reporting period (2011: 5,330 reports). This increase, however, does not allow us to draw any conclusions on trends in cybercrime or the volume of illegal content on the Internet; nevertheless, it does say something about the public's awareness of and willingness to report cybercrime.

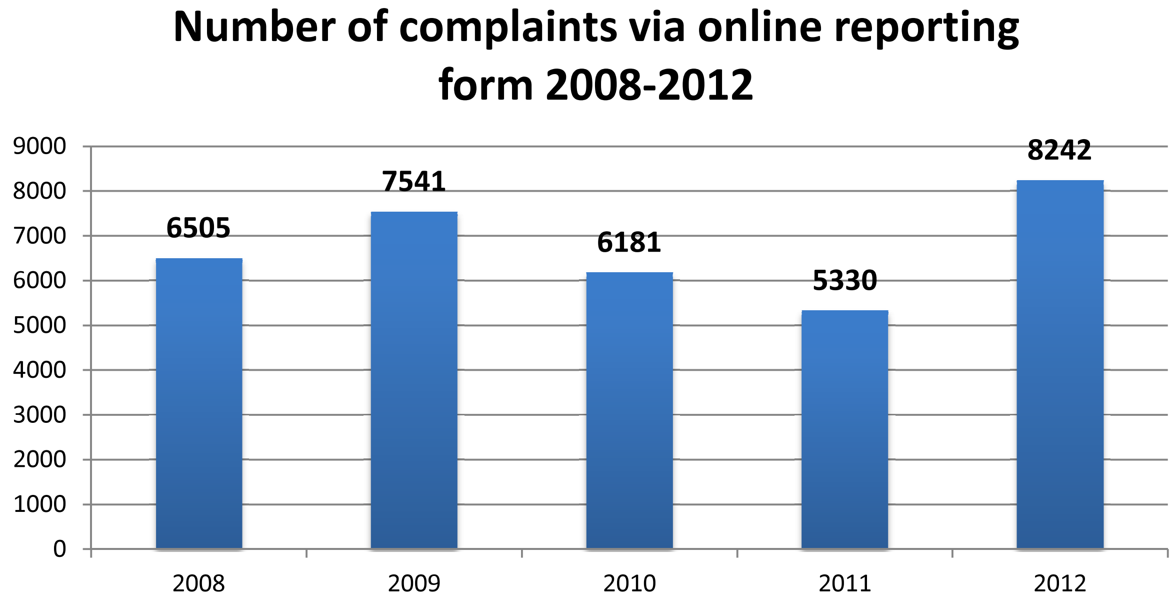


Figure 1: Comparison of the number of reports received from 2008-2012 via www.cyco.ch

There are several possible reasons for the increase in reports using the complaints form, such as the media attention that has been given to specific cases or the cybercrime alerts that CYCO regularly issues.

The number of reports received was very steady in the first four months of 2012. Various specific incidents of limited duration that affected large sections of the population in the summer and autumn triggered a substantial increase in reports (see Figure 2).

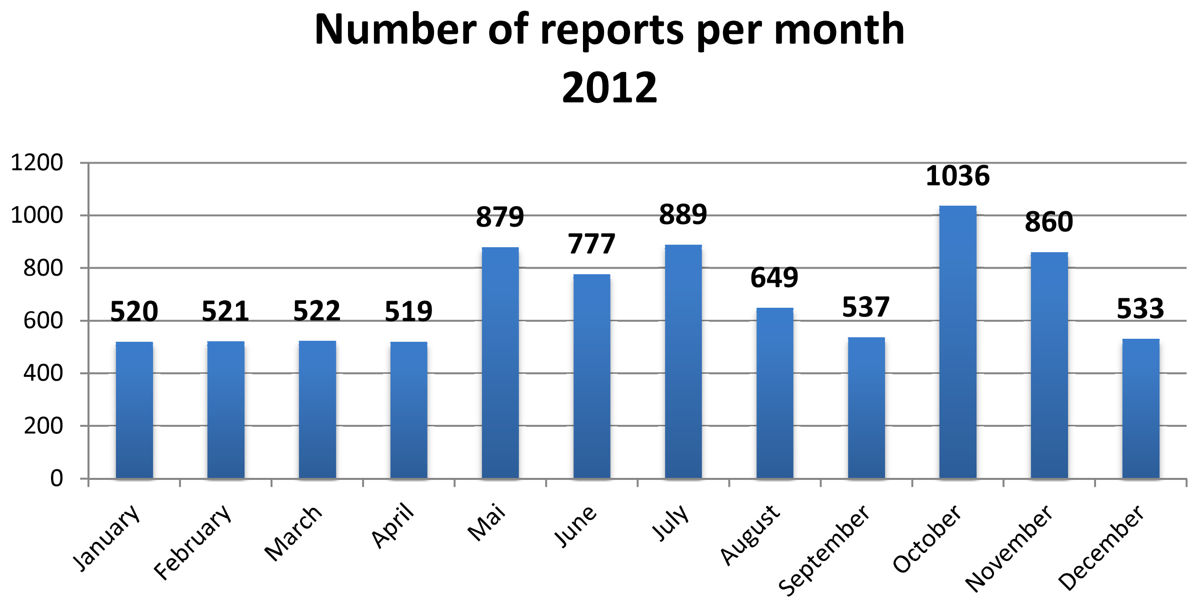


Figure 2: Comparison of online complaints received via www.kobik.ch according to month (Total = 8,242)

2.2 What exactly was reported?

The reports that CYCO received using the complaints form related to a variety of topics and were generally of a high quality. More than 80 per cent (6,639) of the complaints received in 2012 concerned criminally relevant matters. The offences reported were primarily illegal pornography, depictions of violence, racism, extremism, defamation, threats, phishing, fraud, and unauthorised access to a data processing system, damage to data and misuse of a data processing system. Many reports were of offences that are only prosecuted if a criminal complaint is made by the person affected by the criminal conduct. In these cases, CYCO refered the matter to the local police.

For the first time since CYCO began its work in 2003, more complaints concerned the category *property crime* than any other (Articles 137-172ter of the Swiss Criminal Code (SCC)). The number of complaints in this category has been steadily rising in the last few years, while the number of complaints concerning *criminal offences against sexual integrity* (Art. 187-212 SCC) has remained constantly high.

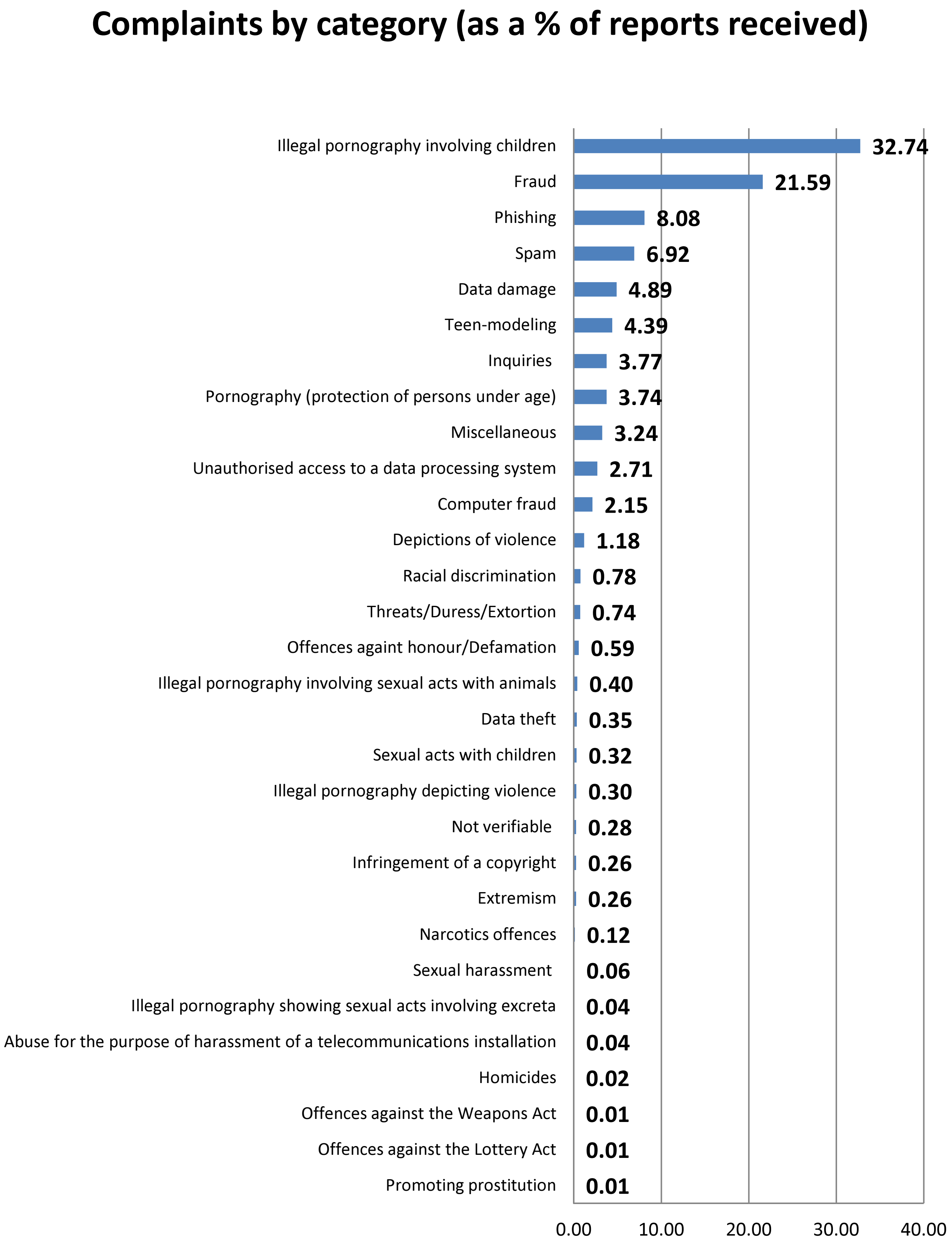


Figure 3: Percentage share of the categories of reports received in 2012

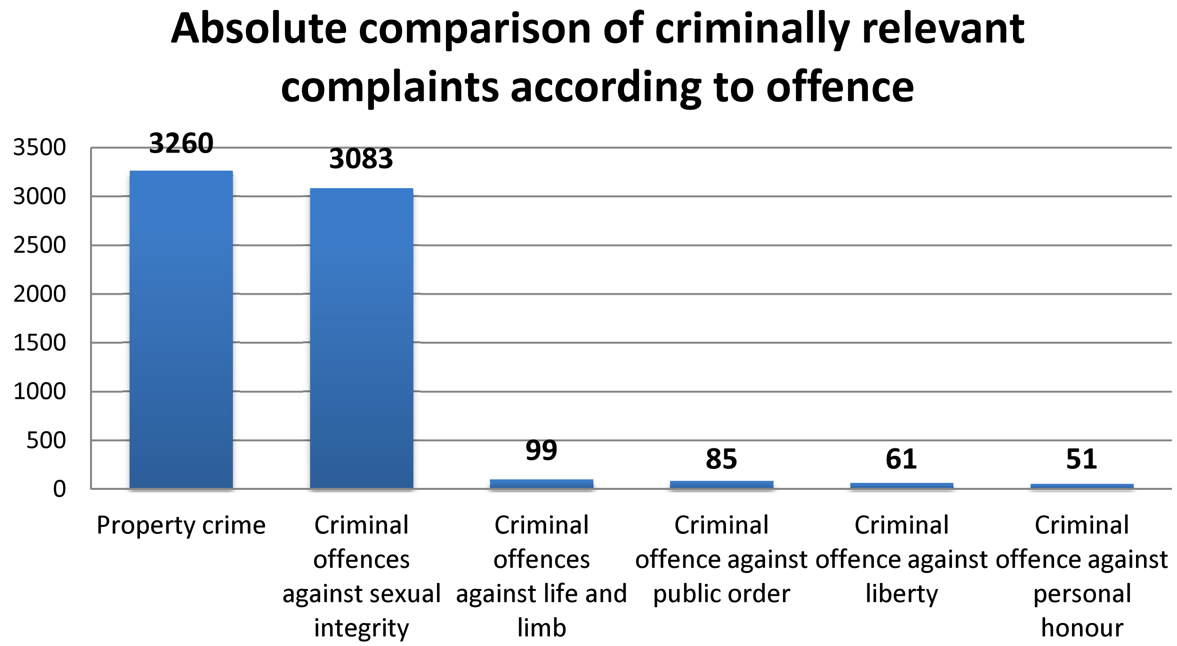


Figure 4: Comparison of criminally relevant complaints according to category of offence (total = 6,639)

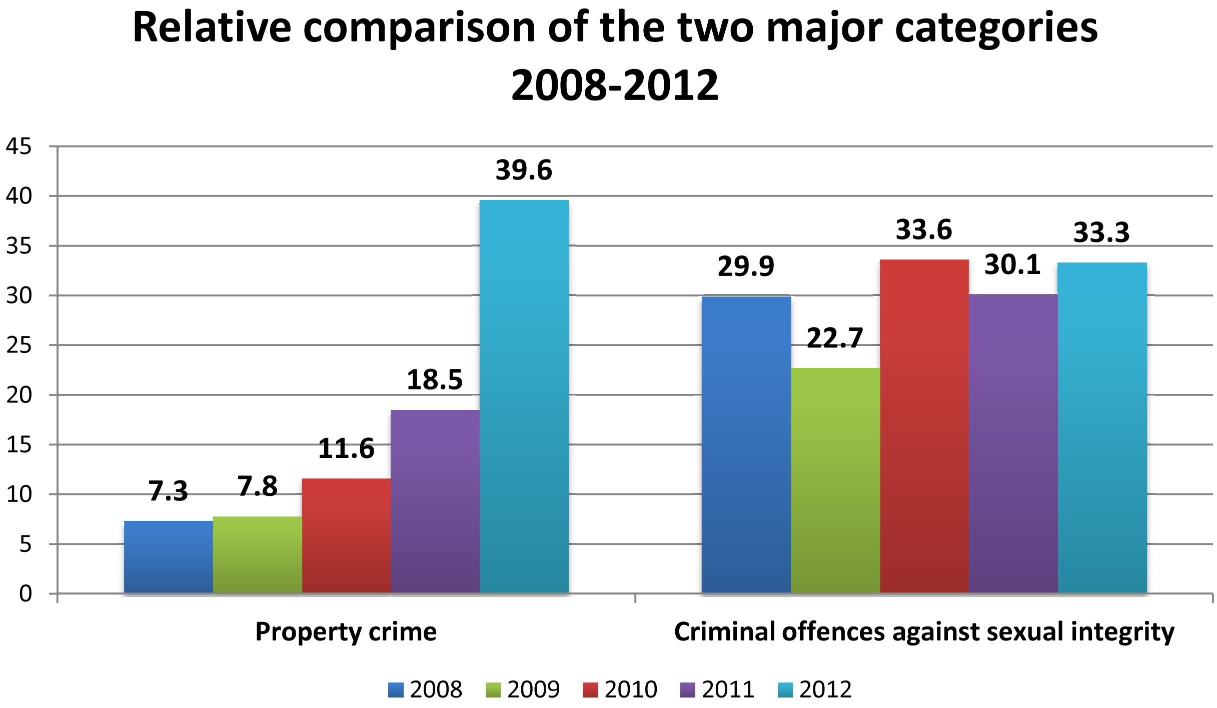


Figure 5: Relative comparison of the two major categories 2008-2012

a) Property offences

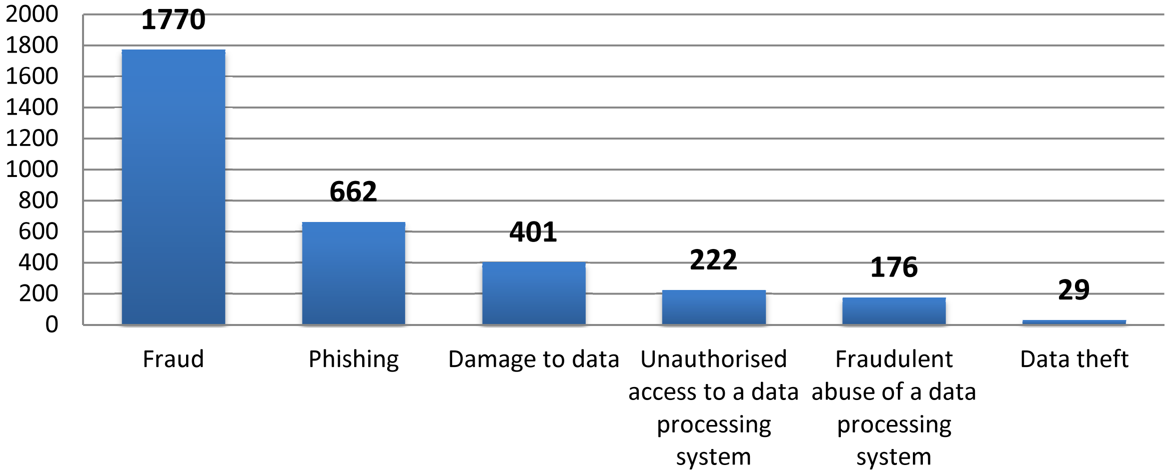


Figure 6: Comparison of property offences according to subcategories (total = 3260)

The category *property offences* was headed in 2012 by the subcategory *fraud,* with a total of 1,770 complaints. Most of the complaints concerning fraudulent offers in classified advertisements or via online auction platforms: victims were tricked into making advance payments for goods or services that they never received. There was also an increase in the number of cases where fraudsters, posing as buyers, maintained they were currently abroad and therefore required payment of additional fees or customs duties before completing the transaction. The fraudsters never intended to purchase the article offered for sale, but were only after the money for the alleged fees and duties. Real estate websites are particularly susceptible to this kind of scam.

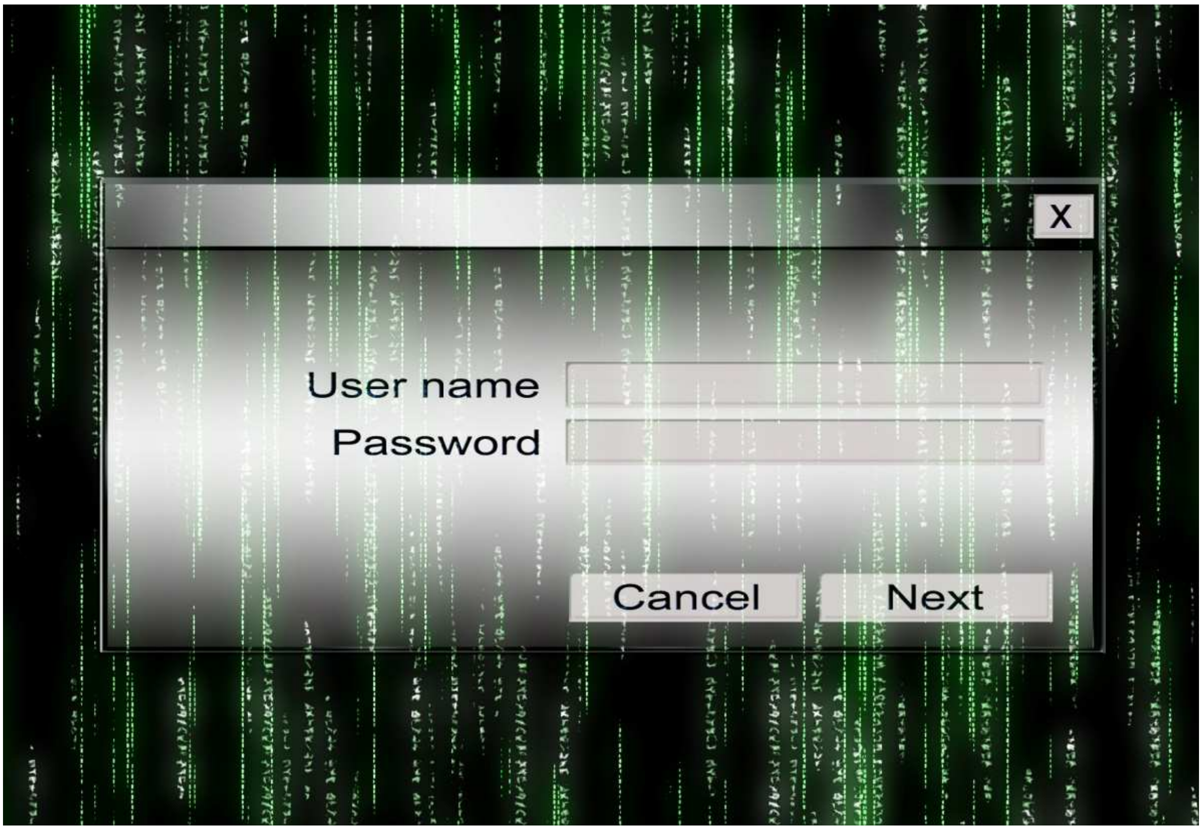
Traditional advance payment scams, where the victim is promised that large winnings will be released on payment of a small fee, were again rife in 2012. This type of fraud is often carried out by means of spam e-mails.

For the first time in 2012, reports concerning phishing attacks were not registered under the sub-category *spam,* but under a separate sub-category, *phishing*. The reason for this is that the focus of spam reports has shifted from unsolicited bulk advertising via e-mail (7% of reports) to phishing attacks: 8 per cent of the reports submitted to CYCO in 2012 concerned attempts to access sensitive data by means of e-mail or telephone calls. The data sought included credit card numbers, bank account numbers, access data to e-mail accounts and e-banking information. Taken together, these two sub-categories accounted for 15 per cent of reports received in 2012, the same proportion as the category *spam* alone in 2011*.* The fall in reports received from the category *spam* does not necessarily mean that the volume of spam e-mail has actually decreased. It is just as likely that the general public is becoming indifferent to spam and therefore reports fewer incidents to CYCO, or that improved spam filters can now identify and block undesired e-mail early so that the user is less aware of them.

In relative terms there was a further increase over 2011 in the number of complaints concerning **Internet crime in the stricter sense** of the word. This comprises the categories *unauthorised access to a data processing system* (Art. 143bis[112] SCC), *damage to data* (Art. 144bis SCC) and *computer fraud* (Art. 147 SCC) (see Figure 3).

Numerous complaints were made by people whose e-mail accounts had been hacked by fraudsters (*unauthorised access to a data processing system).* The hackers then used the victim's address book to request money from their e-mail contacts by posing as the account holder and pretending to have fallen into financial difficulties while on a trip abroad.

A further example from the category ***unauthorised access to a data processing system*** is the hacking of company or association websites in order to obtain sensitive data on the organisation or on its website users. Data stolen in this way may include e-mail addresses, passwords for online bank accounts or credit card numbers, which are sold on by hackers in the appropriate marketplaces. Apart from stealing data, the hackers often also deface the website or even delete whole databases or web pages.



Source: Gerd Altmann /Pixelio

CYCO also received complaints concerning threatened or completed **Distributed-Denial-of-Service attacks (DDoS)** on web shop operators. The perpetrators sent e-mails threatening that the online shop website would be paralysed for several hours by an exceptionally large number of enquiries if the operator did not pay a "ransom".

One particular attack concerned victims whose computers had been frozen by malware following an e-mail supposedly sent by the Federal Office of Police or the Swiss copyright organisation, SUISA. The mail accused the account holder of illegally downloading material from the Internet, and promised that the computer would be unblocked if the account holder paid a penalty of around a hundred francs. If the account holder refused to pay the sum required, the e-mail threatened criminal proceedings.

b) *Criminal offences against sexual integrity*

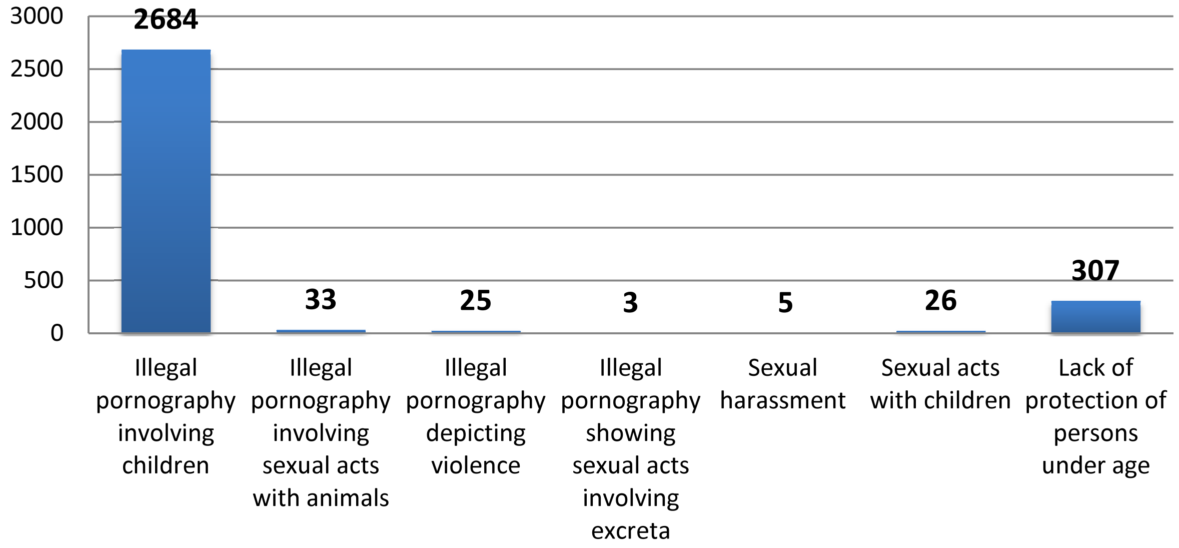


Figure 7: Comparison of sexual offences (total = 3083)

The proportion of complaints from the category *criminal offences against sexual integrity* was slightly higher again in 2012 than in 2011. Most of the complaints in this category concerned the distribution of child pornography on the Internet. CYCO also received 307 complaints concerning pornographic websites that were insufficiently protected against access by minors. However, in absolute terms, it was the first time that there were fewer complaints concerning *criminal offences against sexual integrity* than *property offences.*

Source: S. Hofschlaeger /Pixelio

c) Other criminal acts

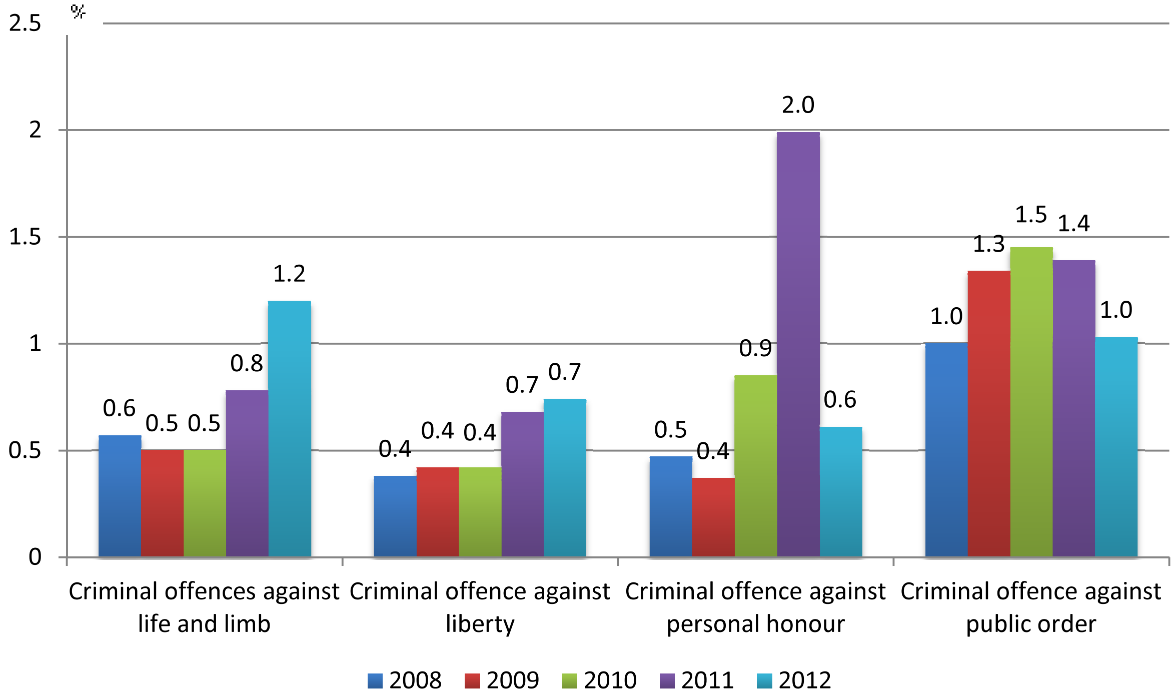


Figure 8: Relative comparison of reports concerning other criminal acts under the Swiss Criminal Code 2008-2012

As in previous years, CYCO also received complaints of other criminal offences. The marked upward trend in 2011 in the number of complaints concerning *personal honour offences* was not repeated in 2012, suggesting that there was no recognisable trend in this area. The reason for this decline may be more responsible social media use following increased public awareness of cyberbullying.

d) Conclusion

Two tendencies were observed:

Firstly, the number of complaints concerning *property offences (economic offences)*—especially fraud and phishing attacks—has been rising continually over the past few years. This development has been accompanied by a rise in the reports received from the category *fraudulent misuse of a computer* for the purpose of obtaining sensitive data or extracting payment from victims.

Secondly, although the number of complaints concerning *criminal offences against sexual integrity* was again high in 2012, with 3,083 reports (2011: 2,150 reports), this category was outstripped in relative terms by the category *property offences* (see Figure 4).

2.3 Products

Based on the reports that CYCO received via the online complaints form, various work was done and measures taken. Here is a summary of the most important figures and information

- All 8,242 online complaints submitted to CYCO in 2012 were analysed within an appropriate timeframe with regard to their criminal relevance jurisdiction.
- CYCO replied individually to more than 2,200 of the 8,242 complaints.
- CYCO forwarded 38 incident files for follow-up action directly to the competent canton or authority due to the criminal relevance of the complaint.
- 345 complaints were forwarded to foreign law enforcement agencies (via Interpol or Europol) or to organisations working in a related field (e.g. INHOPE).
- Hundreds of complaints were forwarded directly to national or foreign Internet service providers, requesting deletion of the unlawful content in question or requesting Internet protocol (IP) information.
- A number of reports were forwarded to fedpol's Federal Criminal Police Division for follow-up action by the competent investigations section (*General, Organised and Financial Crime Section, Criminal offences against sexual integrity against Children and Pornography Section, or National Security Section).*

2.4 Case study

CYCO received several complaints in 2012 concerning people voicing thoughts of suicide on the Internet. One particular complaint was from a French IT company whose in-house abuse prevention team had become aware of a user posting suicidal remarks in the chat room of a popular online game. The company decided to submit an online report to CYCO because the user's IP address was registered in Switzerland. On receipt of the report, CYCO made inquiries with the Internet service provider and was quickly able to identify the address of the Internet connection and alert the competent cantonal police. Only hours after the comments had appeared on the Internet, the cantonal police were able to personally contact the girl and her parents. It turned out that fears for the girl's safety were not unfounded and she subsequently received the necessary counselling. This case underlines the importance of co-operation between the private sector and law enforcement, both at a national and international level.

3. Active searches by CYCO (Monitoring)

Besides handling online complaints from the public, CYCO also conducts its own independent search for suspect content on the Internet. By monitoring less accessible areas of the Internet, CYCO contributes to cybercrime prevention. The CYCO Steering Committee redefines its monitoring priorities each year. As in previous years, the priority for 2012 was combating paedophile crime on the Internet. However, the Steering Committee also expressly required that CYCO should not neglect other fields, such as property offences and Internet crime in the stricter sense (i.e. *unauthorised access to a data processing system, damage to data* and *computer fraud*).

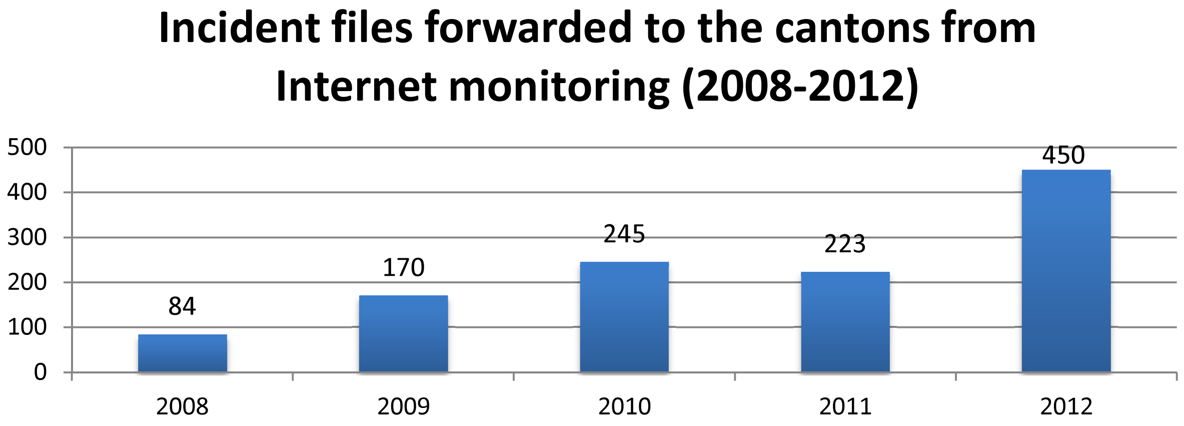


Figure 9: Number of incident files resulting from active Internet monitoring (2008-2012)

CYCO's monitoring activities are twofold: they comprise searching P2P networks for illegal pornography and conducting covert investigations. In 2012, CYCO forwarded 450 incident files to the cantons for follow-up action as a result of both types of Internet monitoring. This represents a twofold increase over 2011.

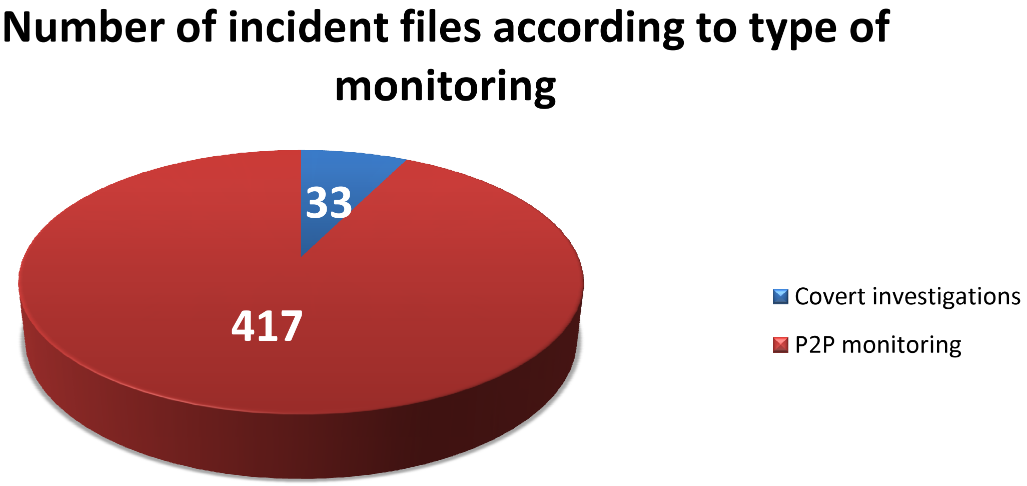


Figure 10: Number of incident files according to type of monitoring (total = 450)

3.1 Active search of peer-to-peer networks (P2P)

Most of the incident files opened in 2012—417 out of 450—were a result of monitoring P2P networks for Internet users who were actively exchanging child pornography in Switzerland. In comparison with 2011, the number of incident files rose by 214, representing a 95 per cent increase. P2P networks continue to be one of the most widely-used means of exchanging illegal data relatively anonymously on the Internet. However, the marked increase in the number of incident files is primarily due to continued development of software used by CYCO, and to in-house process optimisation.

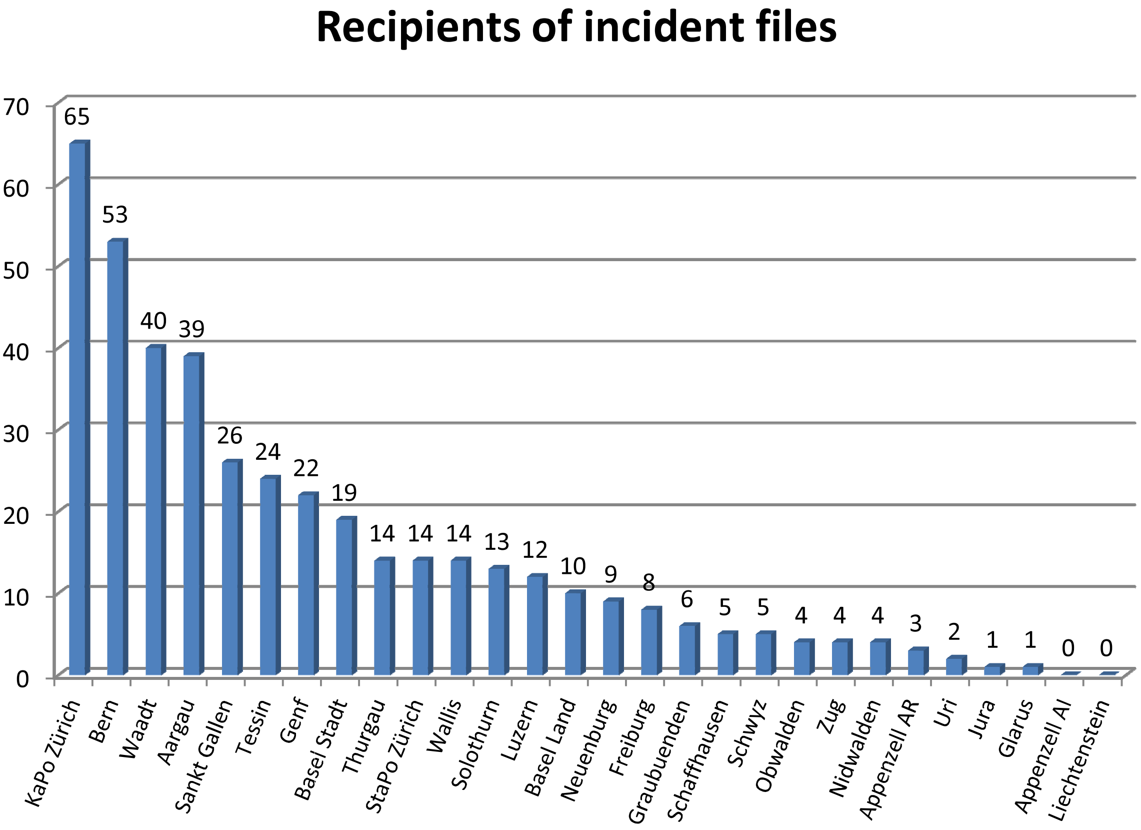


Figure 11: Distribution of incident files according to canton (total = 417)

As in the previous years, most of the incident files that CYCO forwarded went to the most populous cantons, Zurich, Bern and Vaud (see Figure 11).

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

3.2 Preventive covert investigations

Source: Alexander Klaus /Pixelio

The other area of Internet monitoring is preventive covert investigations.

The *Agreement on Cooperation in Police Investigations of the Internet for Combating Paedophile Crime (Monitoring of Chat Rooms)* between CYCO, 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 for the purpose of fighting paedophile crime on the Internet[1]. Hence, CYCO conducts covert investigations explicitly by order and under the supervision of the Cantonal Police of Schwyz. This ensures a continuity of centralised preventive undercover investigations at federal level for the purpose of monitoring online paedophile crime.

As a result of CYCO's undercover investigations, 33 incident files were forwarded to the competent cantonal authorities. Of these 33 cases, thirteen resulted from undercover investigations in children's chat rooms. All these cases concerned attempted sexual acts with children or the distribution of pornography to minors, or both.

The remaining 20 files were a result of undercover investigations on private P2P file-sharing sites. In contrast to classic P2P networks, data is not shared on an open public network. Because data exchange takes place directly between two computers, the legal provisions on undercover investigations apply. Up to now, investigations into private P2P networks have been limited because this field of law enforcement is extremely time-consuming and requires considerable resources. As many of the 20 suspects were repeat offenders and already known to the police—either in connection with illegal pornography or criminal offences against sexual integrity—CYCO's decision to extend undercover investigations to private P2P file-sharing networks has proven to be justified.

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

3.3 Feedback from the cantons

Source: Thorben Wengert /Pixelio

If there is a well-founded suspicion that a criminal offence has been committed, CYCO forwards the case to the competent cantonal authority for follow-up action (see Fig. 11). To gain an overview of the action taken by the cantonal authorities, CYCO requests information from the cantons on the progress made with incident files (i.e. on what police measures have been taken and on the outcome of court proceedings.

Analysing these responses is an important means of reviewing the efficiency of measures, and assessing the quality of incident files and complaints filed with the cantonal police. The majority of incident files (417) were opened as a result of monitoring P2P networks and therefore relate to people who were actively engaged in exchanging child pornography.

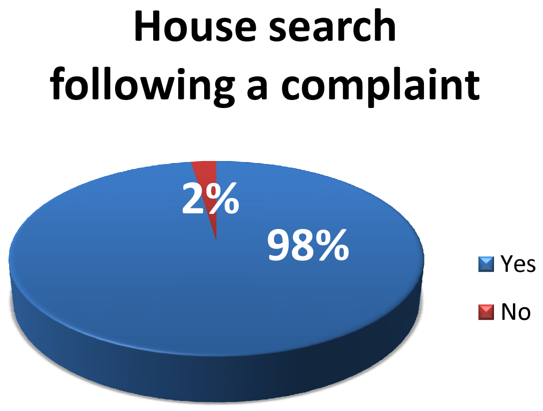


Figure 12: House searches 2012

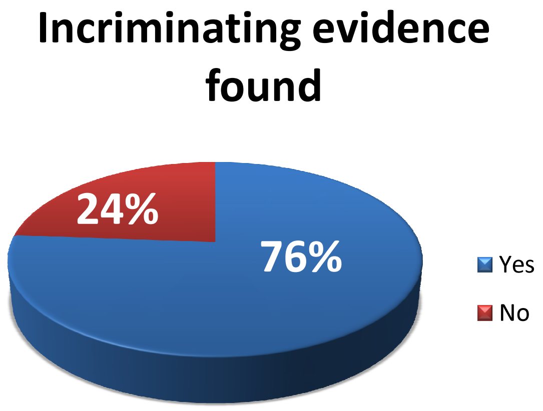


Figure 13: Incriminating evidence 2012

As the diagrams above show, police carried out a house search in 98 per cent of all cases CYCO forwarded to the competent cantonal authority.

a) Feedback from the cantonal police

The police seized incriminating evidence in 76 per cent of all house searches conducted on the basis of an incident file from CYCO. Where a house search does not turn up any incriminating evidence, it is difficult to pinpoint the reason: open and unprotected wireless networks or outsourcing data to cloud services often make it difficult to secure evidence and clearly identify the suspects.

Also, cantonal law enforcement agencies have a better chance of seizing incriminating evidence if they can conduct a house search soon after receiving the incident file from CYCO, because this reduces the risk that computers are substituted or data carriers are deleted by the suspects in the time it takes the police to respond.

Ninety-seven per cent of the incriminating evidence seized in house searches concerned child pornography. This high figure is not surprising, as CYCO searches P2P networks for this type of pornography and most incident files are opened following these monitoring activities. It is also worth mentioning, however, that in more than half of these cases the police identified further offences relating to illegal pornography under Article 197 of the Swiss Criminal Code (see Figure 14). By way of example, in nearly 50 per cent of all house searches police also seized pornography relating to sexual acts with animals.

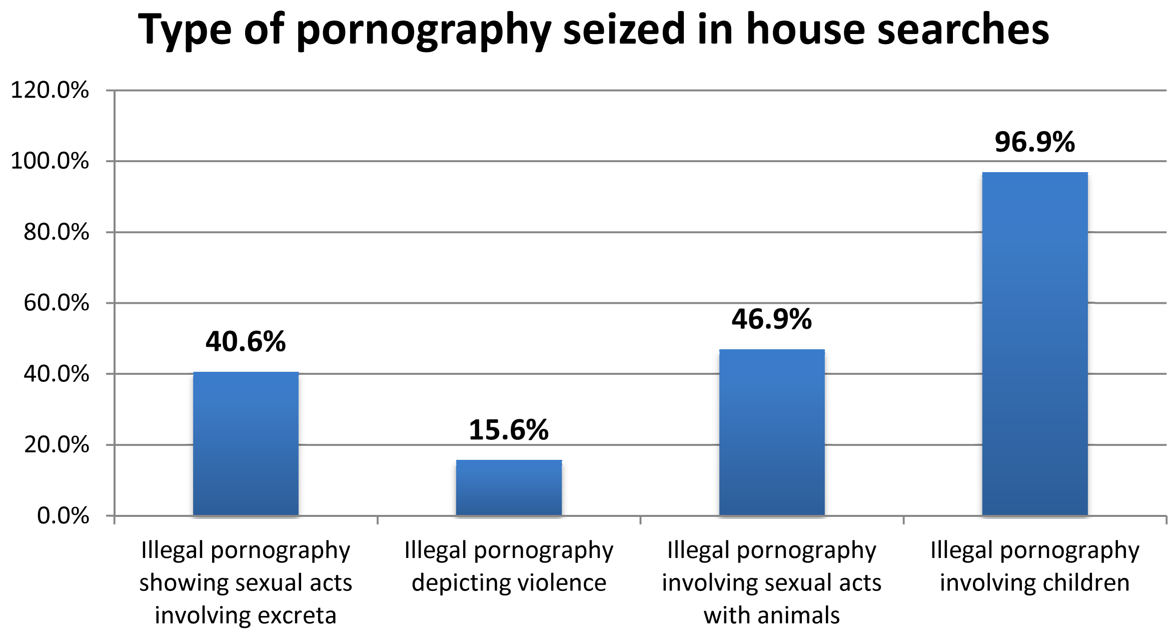
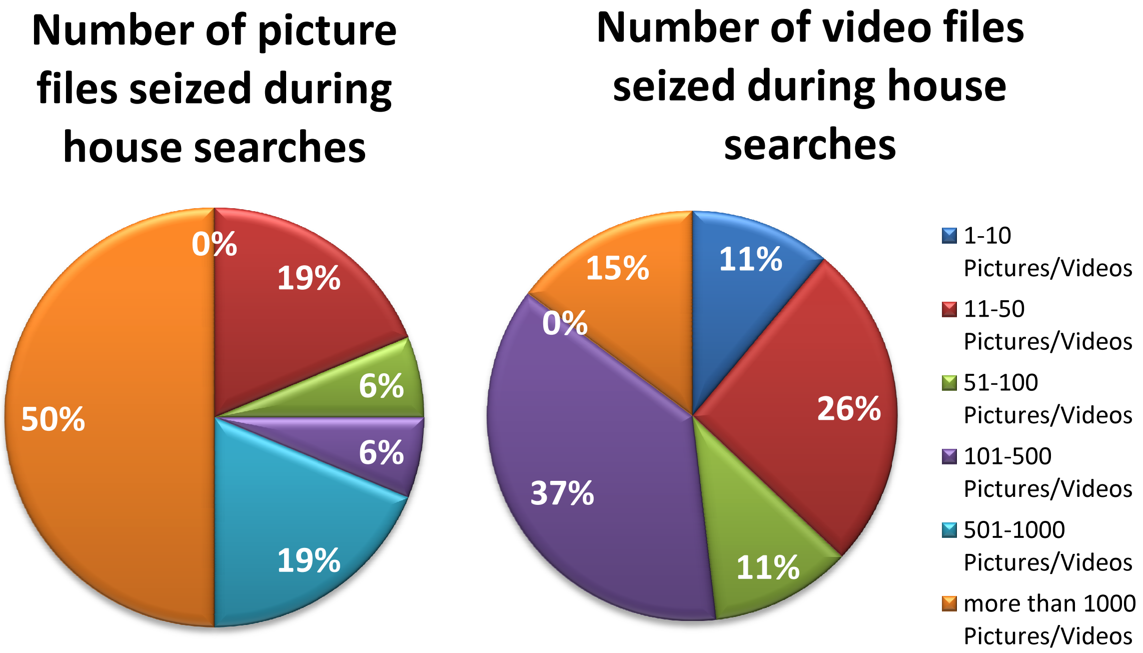


Figure 14: Type of pornography seized in house searches 2012

Feedback from cantonal police authorities also shows that video files were seized in 94 per cent and picture files in 66 per cent of the house searches. Numerous house searches led to both kinds of files being found and seized. In total, the house searches led to the seizure of several million illegal picture and video files.



Figures 15 and 16: Overview of the number of seized picture and video files

b) Feedback from the cantonal courts

In 90 per cent of the cases in which the cantonal courts provided CYCO with feedback, criminal proceedings had led to a conviction.

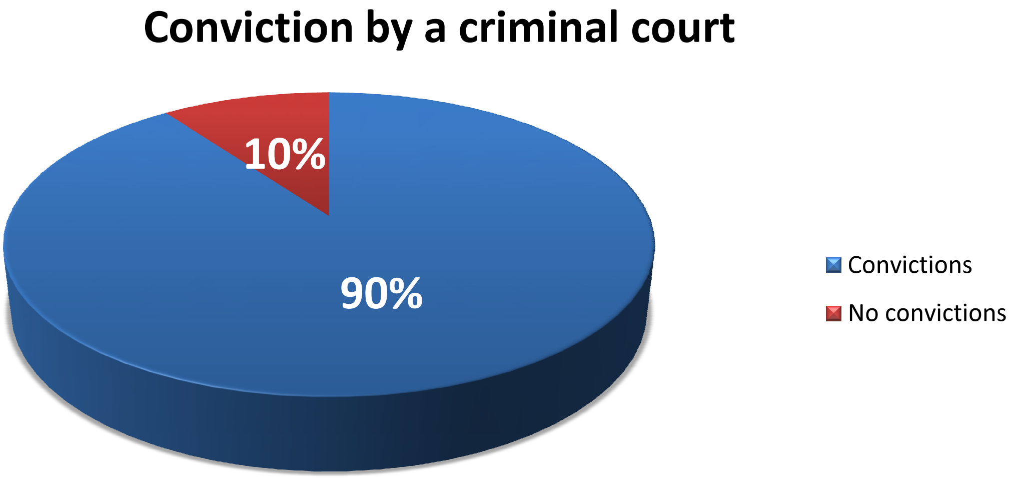


Figure 17: Conviction by a criminal court 2012 in relative terms of the number of responses from cantonal judicial authorities

Most convictions were for offences concerning hardcore pornography (Art. 197 SCC), especially for the acts defined under Article 197 sections 3 and 3bis of the Swiss Criminal Code (pornographic representations depicting sexual acts with children or animals, or involving excrement or violence).

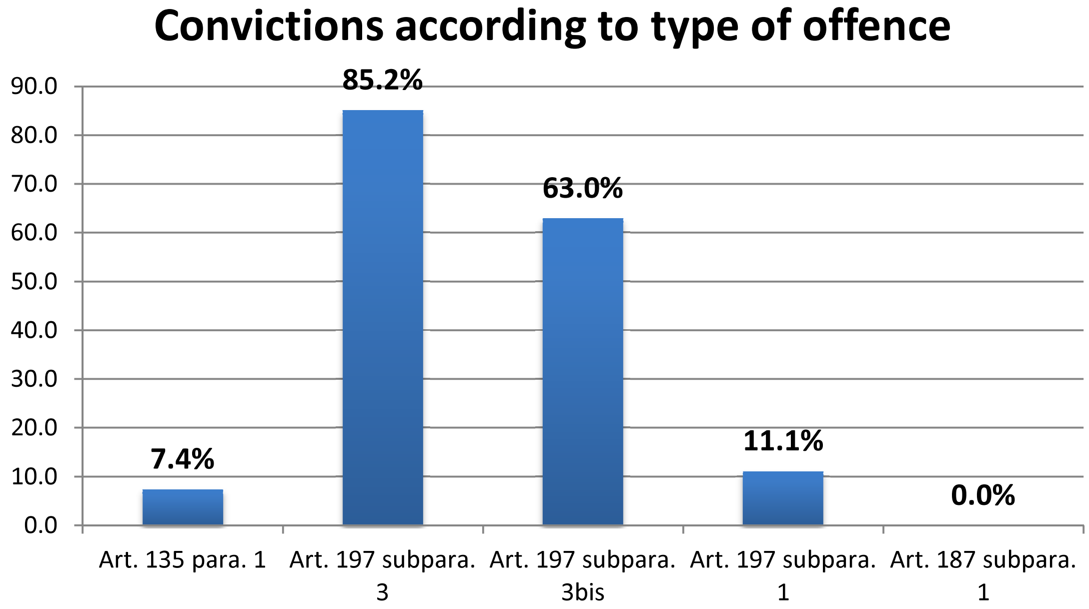
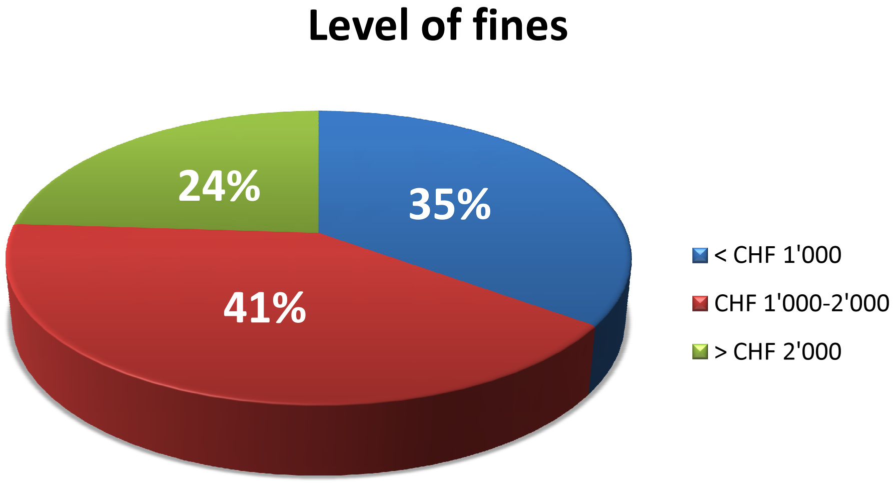


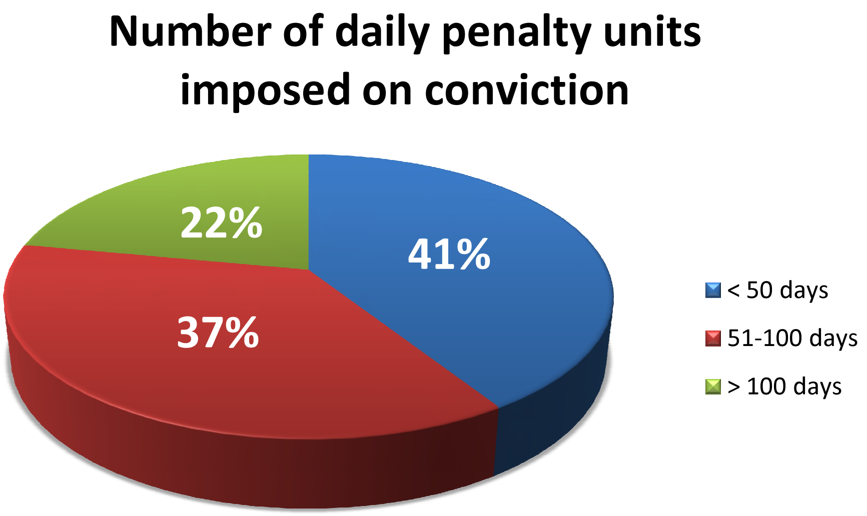
Figure 18: Relative comparison of convictions according to type of offence 2012

In all the convictions reported to CYCO in 2012, the offender was given a **monetary penalty** (i.e. a penalty that involves the payment of a sum of money to the state and that is defined as a number of daily penalty units, depending on the culpability of the offender, and the financial level of which is based on the personal and financial circumstances of the offender). In 63 per cent of these cases, the offender also received a **fine**. In **96 per cent of the convictions, the monetary penalty was combined with probation.** None of the offenders were sentenced to community service, ordered to undergo therapy, given a custodial sentence or received a monetary penalty not combined with probation, in accordance with a trend that has been evident for the past few years.

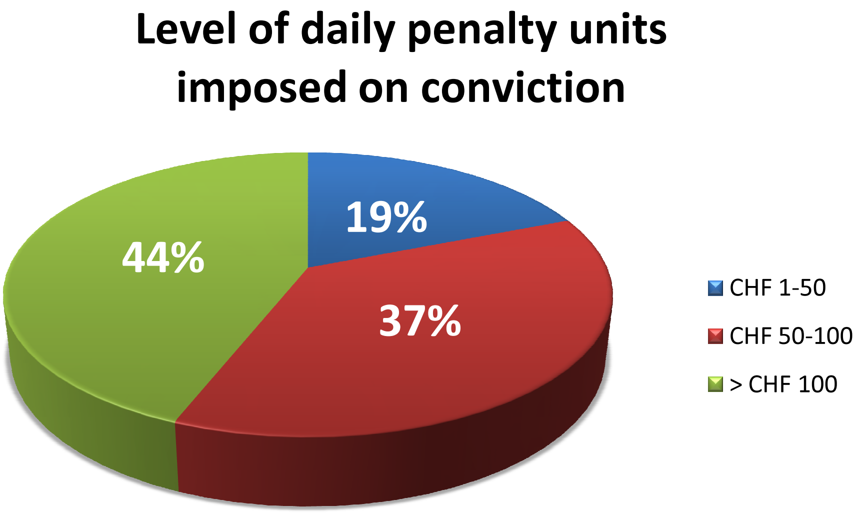


In approximately 35 per cent of cases, the fine amounted to less than CHF 1,000. In 41 per cent of cases, the offender was fined between CHF 1,000 and CHF 2,000. Only 24 per cent of the fines were higher than CHF 2,000.

Forty-one per cent of the monetary penalties were fixed at a maximum of 50 daily penalty units. In 37 per cent of the cases the monetary penalty was fixed at between 51 and 100 daily penalty units. Only in 22 per cent of the cases was the monetary penalty fixed at over 100 daily penalty units.



In 19 per cent of the cases the daily penalty unit was fixed at between CHF 1 to CHF 50, in 37 per cent of the cases between CHF 51 and CHF 100, and in 44 per cent of the cases at over CHF 100.



Generally, the convicted offender also had to pay the costs of the proceedings, which were often many times higher than the actual fine.

3.4 Case study

The following case study is derived from covert investigations conducted by CYCO in P2P networks:

Police investigations based on the CYCO incident file revealed that the person in question had, on two occasions, travelled abroad and there had sexually abused several children and filmed the abuse. The suspect then uploaded the images onto the Internet. Further investigations revealed that the man was also abusing his own three-year-old child.

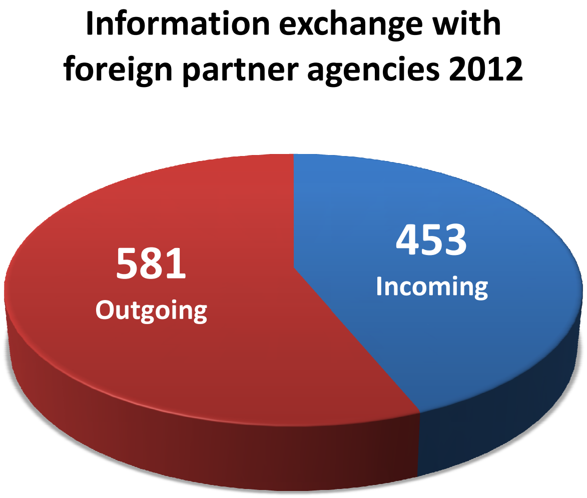
The man was not known to the police until CYCO reported him. Thanks to the professional collaboration between CYCO and the cantonal police, following by the detailed police investigation, the offender was brought to justice and his three-year-old child and other potential victims are now protected from further abuse.

This case study shows how important it is that the cantonal police systematically and thoroughly process incident files relating to criminal offences committed on P2P networks. However, this field of investigation poses a real challenge to law enforcement agencies because the number of incident files from CYCO has increased dramatically and some cantons do not have sufficient resources to deal with such time-consuming cases.

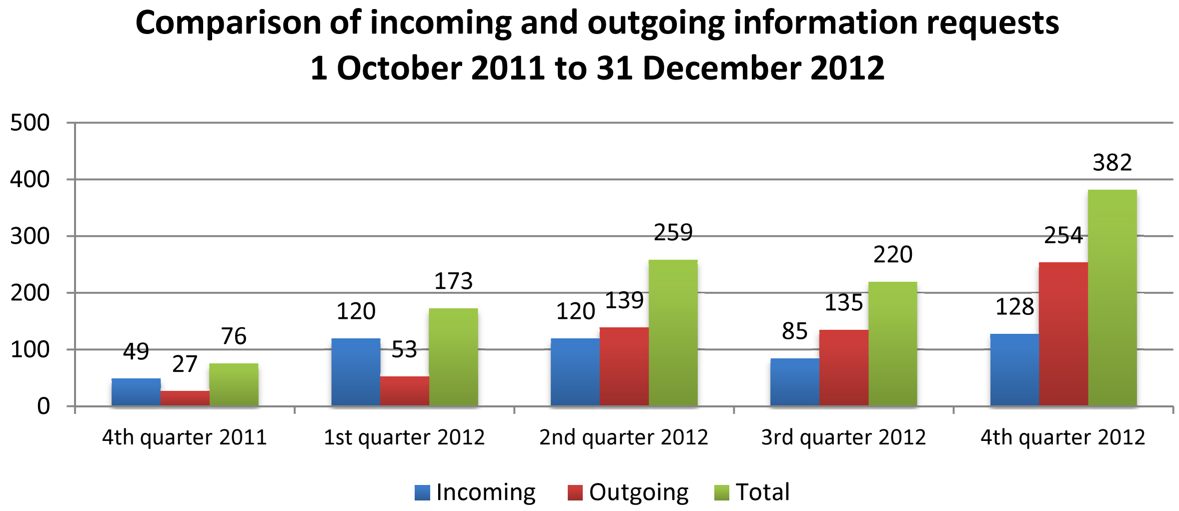
.

4. Information Exchange with Foreign Partner Agencies

Since the Council of Europe's Convention on Cybercrime came into force in Switzerland on 1 January 2012, Switzerland has been increasingly regarded by the international community as an active partner in the fight against Internet crime. This is reflected primarily in the marked increase in the volume of data exchanged with foreign police authorities on issues falling within the scope of the Convention. Other factors that have contributed to CYCO's growing status at international level and the subsequent increase in data exchange are the decision by its Steering Committee to focus equally on cybercrime in the strict sense—and hence on property crime (see chapters 2.2a and 3)—and CYCO's incorporation into the Federal Criminal Police. This latter step also means that CYCO now performs more co-ordinating tasks with regard to investigations and criminal proceedings (see Figure below).



The statistics show that CYCO received 453 requests for information from foreign partner agencies in 2012. Of this total, 128 were submitted in the last quarter alone - an increase of more than 161 per cent over the same reporting period in 2011 (4th quarter 2011: 49 incoming requests). The same trend applies to the number of information requests CYCO made to foreign partner agencies in 2012, a total of 581 (via Interpol and Europol), which has a direct correlation with the higher number of incoming requests. If we compare the number of outgoing requests in the last quarter of 2012 (254 requests) with the number in the same period in 2011 (27 requests), the figures show a dramatic increase.



4.1 Case studies

The following two cases are illustrative of information exchange between CYCO and its foreign partner agencies under the Council of Europe Convention on Cybercrime:

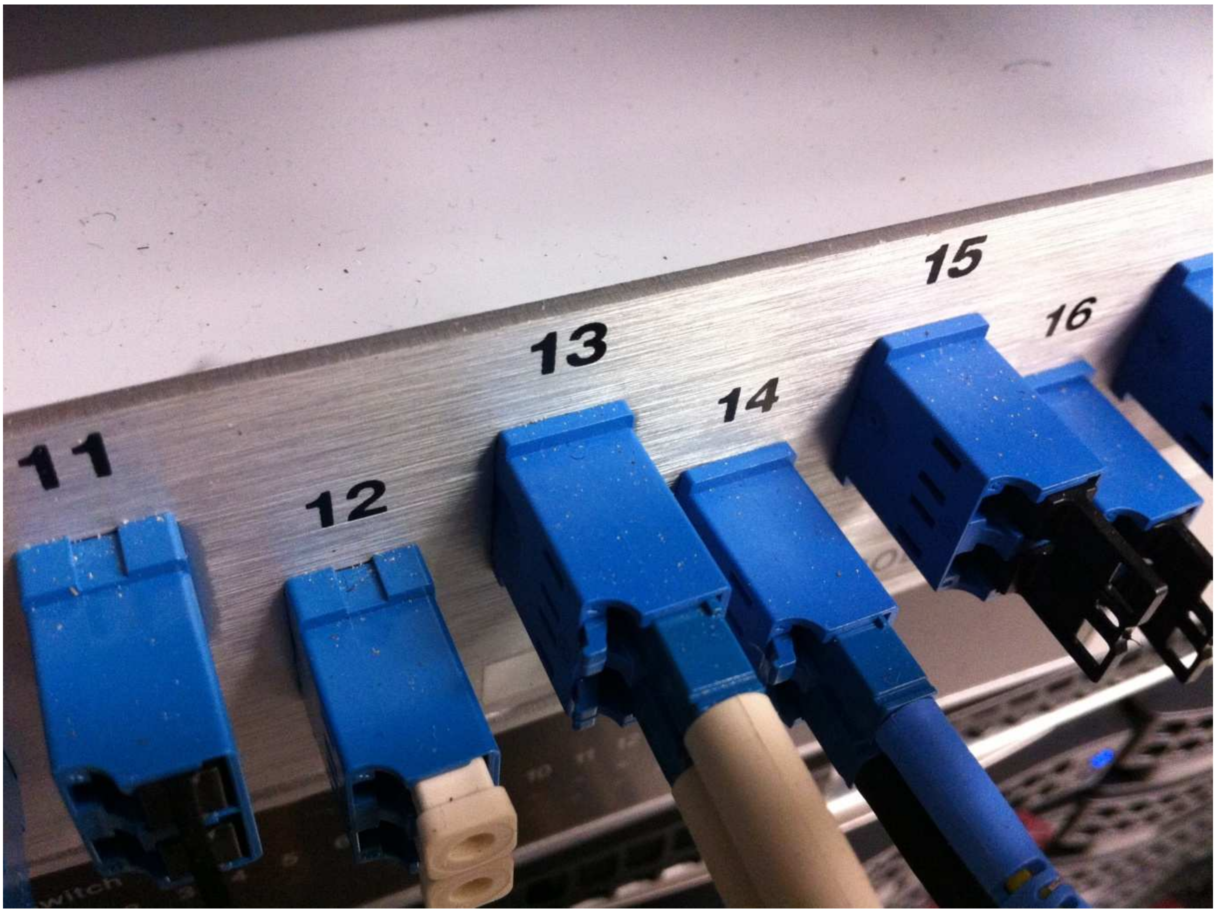
CYCO received a request for information from a foreign partner agency via its Interpol bureau concerning members of political parties in the requesting state who had received death threats via e-mail. The foreign partner agency provided CYCO with details of the sender of the death threats who had a connection in Switzerland. Thanks to procedures that had been defined earlier between CYCO and the Internet access provider in question, the incriminating data was secured within 24 hours and the Internet access provider supplied CYCO with additional information that helped identify the subscriber. CYCO forwarded the incident file to the competent cantonal police for follow-up action and, at the same time, provided the foreign partner agency with the information required for a possible request for mutual legal assistance.

Another case was brought to CYCO's attention by a foreign Interpol bureau. It concerned a series of e-mails designed to extort money from an international wholesaler, the content of which was always the same and appeared to have been sent by the same person. The sender of the e-mail threatened to detonate bombs at various branches of the wholesaler's chain if the money was not paid. One of the e-mails had been come from a Swiss e-mail account and had been sent personally to one of the wholesaler's branch managers. CYCO immediately ordered the Swiss provider, via the competent cantonal police, to secure the data, thus giving rapid and essential assistance to the requesting Interpol bureau in identifying the suspect.

5. Projects

5.1 National Image Hash Value Database (NDHS)

Under this project, data (e.g. picture and video files) seized during investigations into child pornography offences are categorised by the competent cantonal authorities before being transmitted to CYCO. CYCO then generates a hash value for each piece of data[2] and stores the value in the National Image Hash Value Database (NDHS). The list of hash values is then made available to the cantonal authorities. When cantonal authorities seize picture and video files, they also generate a hash value for the data. The hash values generated by CYCO and the cantonal authorities can subsequently be compared for matches. This enables investigators to compare large volumes of data and identify duplicate images without having to view the content, a procedure that is time-saving and, in particular, reduces emotional stress.



The NDHS was designed by CYCO in collaboration with the cantonal police. At the start of the project, both parties had to define the general requirements of such a system (e.g. standard categorisation).

[2] Characteristic value that can be clearly attributed to an image (digital fingerprint)

The key to realising the required software technology lay in developing an efficient solution for processing and comparing large volumes of data in database systems.

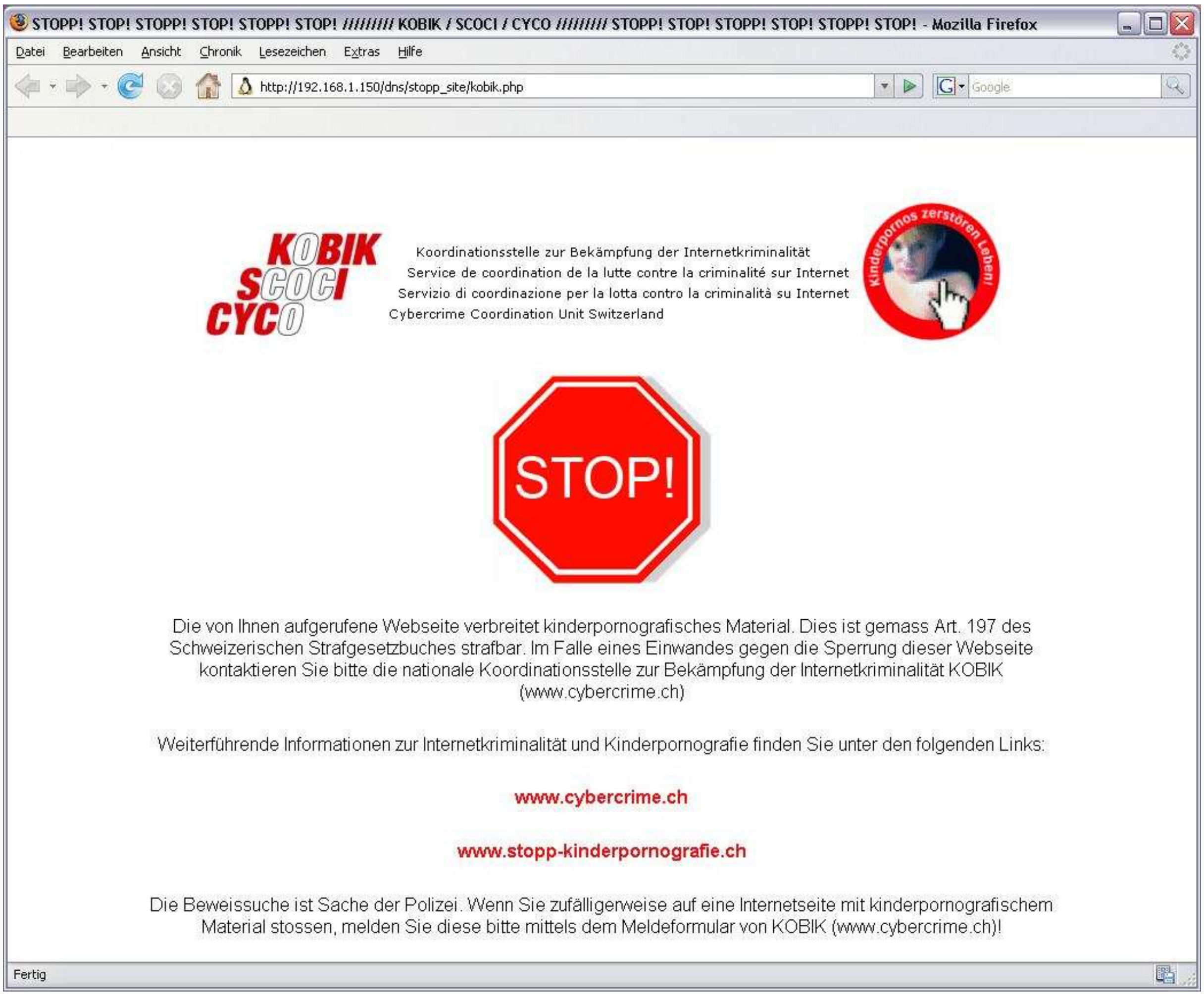
The pilot stage of the project reached a milestone in 2012; the database hardware was set up at the appointed location in February, and between April and July CYCO installed the specially-designed software and ran the first tests. The system came into operation in October, following completion of all test runs and system adjustments. Cantonal and municipal offices can now transmit their pre-categorised images to CYCO; CYCO then verifies the material, assigns the images to definite category and scans them into the database.

5.2 Project to monitor peer-to-peer networks

As part of its preventive monitoring activities, CYCO, working with the NGO Action Innocence Geneva (AIG), has in recent years developed a program that scans P2P networks for child pornography. The software is aimed at preventing the exchange of paedophile material on the Internet. The program, which is fully financed by AIG, is being continually developed in collaboration with the NGO and has been made available to other law enforcement agencies.

CYCO's preventive monitoring activities help to expose not only the "consumers" of child pornography, whose activities foster the production of more and more material, but also paedophile criminals who sexually abuse children, film the abuse and produce the images.

5.3 Co-operation with Swiss Internet access providers


STOPP! STOP! STOPP! STOP! STOPP! STOP! //////// KOBIK / SCOCI / CYCO //////// STOPP! STOP! STOPP! STOP! STOPP! STOP! - Mozilla Firefox
Datei
Bearbeiten
Ansicht
Chronik
Lesezeichen
Extras
Hilfe
http://192.168.1.150/dns/stopp_site/kobik.php
Google
KOBIK
SCOCI
CYCO
Kinderpornos zerstören Leben!
STOP!
Fertig

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

Die von Ihnen aufgerufene Webseite verbreitet kinderpornografisches Material. Dies ist gemass Art. 197 des Schweizerischen Strafgesetzbuches strafbar. Im Falle eines Einwandes gegen die Sperrung dieser Webseite kontaktieren Sie bitte die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK (www.cybercrime.ch)

Weiterführende Informationen zur Internetkriminalität und Kinderpornografie finden Sie unter den folgenden Links:

www.cybercrime.ch

www.stopp-kinderpornografie.ch

Die Beweissuche ist Sache der Polizei. Wenn Sie zufälligerweise auf eine Internetseite mit kinderpornografischem Material stossen, melden Sie diese bitte mittels dem Meldeformular von KOBIK (www.cybercrime.ch)!

Since 2007, CYCO has assisted the major Swiss Internet service providers in blocking websites containing child pornography. This project is aimed exclusively at foreign websites with child pornography content. CYCO sends the Internet service providers a regularly updated list of websites containing child pornography (. Based on their corporate ethics and general terms and conditions, Internet service providers block access to the illegal websites and redirect the user to a “Stop” page.

As part of this project CYCO works closely with Interpol. Interpol has compiled a “worst-of” list of websites with child pornography images and videos. CYCO also compiles a list of unlawful websites, which comprises Interpol’s list and websites discovered during CYCO’s own monitoring activities. Interpol’s list is updated on a daily basis and is integrated into CYCO’s list. Similarly, CYCO reports its discoveries to Interpol.

6. Working Groups, Partnerships and Contacts

6.1 National working groups

In 2012, CYCO was represented in the following national working groups on cybercrime prevention:

- *Child Abuse Working Group*: A national working group comprising representatives from CYCO, fedpol's *Sexual Offences against Children and Pornography Section,* non-profit organisations, Swiss Crime Prevention (SCP) and cantonal delegates.

- *Media Protection and Media Literacy for Young People*: CYCO is a member of the steering group (responsible for programme development) and the support group (responsible programme implementation). The programme aims to teach children and young people how to deal with modern media in a safe and responsible way, and appropriate to their age.

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

- *IT Investigators Working Group* and *Monitoring Telecommunications Working Group*: through its participation in these working groups, CYCO seeks to stay abreast of technical developments and hence foster better law enforcement.

- *Security and Confidence Action Plan*: CYCO continued to be involved in developing the "Security and Confidence Action Plan" (German *Sicherheit und Vertrauen*). Under the guidance of the Federal Office of Communications (OFCOM) this action plan highlights measures to promote the safety and confidence of the public in using modern information and communication technologies.

Source: Gerd Altmann /Pixelio

6.2 Co-operation with other federal agencies

CYCO co-operated closely in 2012 with other federal agencies on fighting cybercrime. In-house, it collaborated 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 Cooperation. Cooperation between CYCO and the *Paedophile Crime and Pornography* unit was especially intensive on account of a mutual topical interest.

In addition, a variety of contacts with cross-department federal agencies were expanded and intensified. Worth mentioning are the Reporting and Analysis Centre for Information Assurance (MELANI), the International Mutual Assistance Division in the Federal Office of Justice (FOJ), the Federal Office of Information Technology, Systems and Telecommunication (FOITT), the Federal Social Insurance Office (FSIO), the Federal Office of Communications (OFCOM) and the Federal Commission against Racism (FCR).

At various meetings with the Office of the Attorney General of Switzerland, important common processes were discussed and cooperation optimised. A specific result of this is the decision by the Federal Criminal Police to provide CYCO promptly with any information obtained in federal investigations that relates to cybercrime in the narrower sense. In this way, CYCO will be better placed to carry out its duties, such as case supervision, situation analysis of cybercrime in Switzerland or its role as an interface between the police authorities and the intelligence service via MELANI.

6.3 Exchanging experiences with the cantons

In the report year, CYCO maintained its numerous contacts with representatives of various police forces and public prosecutors offices. In addition to the normal exchange of experiences, various working sessions were held, particularly as part of covert preliminary investigations and the NDHS project.

In addition, in 2012 the first Cybercrime Forum for public prosecutors offices and CYCO was held. Its aims included resolving a number of uncertainties that public prosecutors offices had when dealing with cybercrime and its technical aspects. At the Forum a variety of experts provided the participants with a practical insight into combating cybercrime which was tailored to their needs. The enormous interest shown by public prosecutors offices in the Forum showed that the original initiative by the Office of the Cantonal Prosecutor in Zurich was justified and that extending the Forum to allow participation by other cantons was the right move.

Source: Gerd Altmann /Pixelio

6.4 Cooperation with Action Innocence Geneva (AIG)

For several years, CYCO has been working closely with the NGO[3] Action Innocence Geneva (AIG) on combating the child pornography. Thanks to active support from AIG, a project supervising peer-to-peer networks has been successfully developed and run in recent years. The cooperation with AIG is highly significant, as a clear majority of the active enquiries made by CYCO is only possible thanks to the software made available by AIG. In addition, AIG supports CYCO by developing various additional projects intended for use in combating paedophile crime.

6.5 Cooperation with the private sector (Public-Private Partnership)

CYCO's cooperation with the private sector is becoming increasingly important in combating cybercrime. In the report year, various visits to or meetings with representatives of the internet industry took place. Particularly positive are the contacts made with various Internet service providers. This cooperation is decisive when investigating suspects' internet connections (IP addresses) in the course of police preliminary investigations and investigations. Combating cybercrime requires all those involved to act quickly and in concert. Due to the rise in economic crime on the Internet, in 2012 meetings were held with representatives of online sales platforms.

6.6 International cooperation

Since 2011, CYCO has been a member of Europol's "Cyborg" Focal Point (FP), whose aim is to combat supranational cybercrime. It focuses on the phenomena of phishing, botnets and hacking. In a new move in 2012, CYCO also joined the "Twins"

[3] Non-Governmental Organization / Nichtregierungsorganisation (NRO)

FP which is devoted to combating paedophile crime. Both Focal Points are integrated into the European Cybercrime Centre (EC3), which began its work on 1 January 2013.

The European Cybercrime Centre, based at Europol in The Hague aims to support EU states operationally and to provide specialist knowledge for joint investigations at EU level. Investigators will concentrate on organised crime in cyberspace. The expected priorities will be combating the sexual exploitation of children on the Internet and investigating financial crimes. In addition, the EU Cybercops aim to tackle attacks on critical infrastructures and information systems. Their tasks include analyses and evaluations in order to identify and deal with potential threat situations at an early stage.

CYCO is also involved in CIRCAMP project. This project combats the spread of child pornography on the Internet. As in previous years, CYCO was in contact with the European Financial Coalition again in 2012. The EFC, co-funded by the EU, is made up of important players in law enforcement and the private sector, who have the common goal of combating the commercial sexual exploitation of children on the Internet.

Also in the report year CYCO actively cultivated contacts with various foreign partner agencies. This exchange primarily served the joint development of processes designed to improve cooperation. For some time, cooperation has no longer been concentrated exclusively on combating paedophile crime. Combating cybercrime in the narrower sense and white-collar crime are regularly the focus for international efforts. In particular, as part of operations (e.g. covert investigations) direct exchanges with foreign prosecution authorities are highly beneficial. Here again, CYCO is developing close and promising cooperative ties to various authorities.

7. Media Appearances, Training and Conferences

7.1 Media presence

Reports on CYCO's activities appeared in numerous media reports in 2012. The media took a particular interest in (preventive) covert preliminary investigations conducted by CYCO, individual spectacular attacks on information systems (DDoS attacks[4]) and malware infections, which affected countless computer users. Taken over the year as a whole, the reports were extremely positive.

7.2 Training and conferences

In the report year, CYCO staff attended several conferences, international congresses and training courses and benefited from the opportunity to cultivate essential contacts with partners and experts.

[4] Distributed Denial of Service

8. Political Initiatives at Federal Level

8.1 Legal and political developments

Combating cybercrime also poses new challenges for the courts and for lawmakers. This Chapter will consider specific legal developments at national and international level.

Source: Gerd Altmann /Pixerio

a) Cybercrime Convention

By ratifying the Council of Europe Convention on Cybercrime, Switzerland is playing its part in increased international efforts to combat computer crime and cybercrime. The Convention came into force in Switzerland on 1 January 2012, while at the same time the Federal Council brought the required amendments of Swiss legislation into effect.

The Council of Europe Convention on Cybercrime is the first international agreement on combating computer and cybercrime. It requires the contracting states to criminalise computer fraud, data theft, counterfeiting documents with the aid of a computer or unauthorised access to a protected computer system. The contracting states must also introduce offences of child pornography and breach of copyright on the Internet.

The Convention also regulates the way in which evidence should be gathered and secured in the form of electronic data in criminal investigations. It is intended in particular to guarantee that investigating authorities can gain quick access to electronically processed data so that such data cannot be falsified or destroyed in the course of the proceedings. Finally, the Convention is intended to ensure rapid, effective and comprehensive cooperation between the contracting states.

Implementing the Convention has required minor amendments to the Swiss Criminal Code and the Mutual Assistance Act:

- In the criminal offence of unauthorised access to a data processing system ("Hacking", Art. 143bis SCC), criminal liability has been introduced at an earlier stage. Accordingly, making available or circulating passwords, programmes and other data now becomes an offence if the person concerned knows or must assume that these may be used for illegal unauthorised access to a protected computer system.

- The Mutual Assistance Act now gives the Swiss mutual assistance authority the power in certain cases to transmit traffic data to the requesting authority in order to assist with investigations before the conclusion of the mutual assistance proceedings (cf. Art. 18b MAA). These data – which provide information on the sender and recipient, time, duration, size and route of a message – may however only be used as evidence once the final ruling on granting and the extent of mutual assistance has become legally binding.

- In addition, it has been decided that the 24/7 contact point required under Art. 35 of the Convention will be provided by the fedpol Operations Centre (SPOC, fedpol OC). CYCO supports the SPOC in processing enquiries made under the Convention.

b) National strategy to protect Switzerland against cyber risks (NCS)

On 27 June 2012, the Federal Council approved the national strategy to protect Switzerland against cyber risks[5]. With the strategy, the Federal Council in cooperation with authorities, the private sector and operators of critical infrastructures intends to minimise the cyber risks that they are exposed to every day.

The strategy identifies cyber risks primarily as a feature of existing processes and responsibilities. Accordingly these cyber risks should be taken into account in existing risk management processes. In an initial step, those responsible should compile basic information on cyber risks and raise their awareness of this problem.

To this end, the Federal Council instructed the departments to set about implementing a total of 16 identified measures at their own level and together and in consultation with cantonal authorities and the private sector. The measures range from risk analyses relating to critical ICT infrastructures to increased lobbying for Swiss interests in this field at international level.

Measure 6 provides that at national level cases (criminal cases) should be supervised as comprehensively as possible and intercantonal case clusters must be coor-

[5] www.admin.ch/ch/d/ff/2013/563.pdf

dinated. The information obtained should be fed into an overall presentation of the situation. The FDJP, working with the cantons, has been asked to submit a concept for this by the end of 2016. This concept must also include a clarification of the position with regard to interfaces with other parties involved in minimising cyber risks, coordination with the presentation of the situation and the resources and legal adjustments required at federal and cantonal level in order to implement the concept. In accordance with decision of the CYCO Steering Committee and the fedpol Directorate, CYCO will act on behalf of fedpol to coordinate and supervise the coordination and completion of the implementation work on the NCS strategy.

9. Glossary

Adult check	(A proof of age system) A system used for the protection of minors. It makes it possible to prevent minors from accessing certain websites.
Chat	Electronic communication in real time, mainly via the Internet.
Cloud Computing	Cloud Computing denotes IT infrastructures (computing capacity, data storage on computers and servers) that are made available from various parts of the world via a network such as the Internet. Instead of storing system applications and data on a small number of local computers, the processing load is shared by as many computers as possible in order to achieve the optimum use of resources and is thus provided by a multitude of servers around the world (a “cloud system” as it were). A high performance bandwidth is one of the basic requirements for cloud computing.
Cyberbullying	Cyberbullying involves using modern communications media such as mobile phones, chat, social Internet networks such as Netlog or Facebook, video portals or forums and blogs to publish defamatory texts, pictures or films in order to denigrate, humiliate or harass people. Attacks are normally made repeatedly and/or over a long period of time and victims are characterised by their particular helplessness.
One click hosting	One click hosting offers users the opportunity to save providers’ files (mainly video and audio files) directly and without any prior registration process. The user receives a URL where the file can be clicked on and downloaded.
Peer-to-Peer	In a peer-to-peer network members can access shared files and can also exchange the files with third parties.
Phishing	Method for trying to obtain data (passwords, user names, etc.) from an Internet user by using falsified www-addresses.
Hardcore pornography	Sexual acts involving children (synonym: child pornography), animals or human excrement, or sexual acts involving violence (Art. 197 Sec. 3 SCC).
Hash values	Characteristic value that can be clearly attributed to an image (digital fingerprint)
Proxy	Communication interface between the client and a server in an IT network, via which, for example, a website can be accessed.
Redirect service	A service that turns long URLs into short ones that are easy to remember. The browser is instructed to retrieve the content of the specified page immediately via an abbreviated URL.
Spam	Spam is undesirable correspondence, normally transmitted electronically, that are sent to the recipient unsolicited. Spam is often sent for advertising purposes, but also from time to time in order to introduce malware into a user system.
Streaming	Transmission of audio or video files. Files are downloaded via a computer network into a system, not in full but continuously. As a result, the full download of the file is not necessary, as it is possible to “listen in”.
URL	Uniform Resource Locator. An address consisting of characters and numerals (commonly known as an Internet address).

10. Trends and Potential Threats in 2013

Based on the reports that CYCO has received, very few if any conclusions can be drawn as to how cybercrime or illegal content on the Internet will actually develop. At best, trends can be identified with regard to the willingness of public to report incidents and the perception of cybercrime in society.

Trojan horses targeting banks: It cannot be excluded that that the "Blitzkrieg" operation announced by Russian groups, which will apparently be mainly directed against American banks, will also lead to attacks on Swiss banks. It is suspected that the attacks will primarily consist of intercepting login data using Trojan horses. As most banks in Switzerland have multi-level authentication mechanisms, the risk of direct financial losses due to fraudulent transactions is low, but cannot be excluded.

Mobile Malware: In 2012 there was an explosion in the number of malware variants, which primarily infect Android smartphones. Experts expect that the number will continue to rise. The consequences for victims are additional costs due to the use of Internet bandwidth, as infected devices can be used for DDoS attacks, along with unsolicited mailing of spam texts. It should also be expected that personal data, such as the content of address books, passwords, etc. will be unlawfully gathered and sold on to other criminals.

Malware: Here too a further increase in the number of the cases can be expected. The focus continues to be spying out bank data, credit card numbers and passwords. Secondary targets are address book data, which can be used to create bogus identities for fraud attempts, and the development of a botnet for DDoS attacks. New infection routes can also be expected, for example via add-ons for browsers or web apps for social media sites. It is also conceivable that security loopholes in cloud services will be exploited in order to install malware in target computers.

Data theft: As a wide variety of cases have shown, even small websites are not safe from attackers. Client data such as addresses have become an increasingly valuable target for hackers, as they make social engineering considerably easier and accordingly can be used to commit other frauds. In addition, e-mail addresses can be sold at lucrative prices on the relevant forums. As cyber criminals specialise in specific services, such as procuring and selling data, in future smaller targets could also become of interest for such attacks and be targeted.

Scams: With the increasing spread of the Internet in Africa and the growth of (by western standards) low-earning middle classes in countries such as Nigeria, South Africa or Morocco, experts fear that fraudulent offers will again proliferate on classified advertisement and auction pages in coming years. There is talk of a doubling of the number of advertisements by 2015.

DDoS attacks: In 2012 a variety of DDoS attacks were launched for extortion purposes and also for politically motivated ends. It must be assumed that in 2013 these types of attacks will continue. The major powers are already developing military and intelligence service reserve units to defend critical infrastructures against DDoS and other hacking attacks. This shows that large-scale DDoS attacks are being taken very seriously as a threat scenario.

Whatever the form of cybercrime may be, it can only be combated and a solution found through cooperation between all those involved (governments, prosecution authorities, internet providers, internet service providers and regulators). CYCO already takes part in various national and international working groups that aim to combat phenomena relating to specific crimes. It must be expected that cooperation between private and public institutions (public-private partnerships) to combat cybercrime will play an increasingly important role.