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 2013

CELEBRATING 10 YEARS OF CYCO

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

Published: 27 March 2014

Source of illustrations: Thinkstock / CYCO

FOREWORD

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

Nothing is permanent except change, said the Greek philosopher, Heraclitus. *Never give up! Stagnation is regression!* We have all heard these sayings, and they are particularly relevant to CYCO for two reasons: firstly, because one Internet year encompasses four human years (according to a study by ibusiness.de) and, secondly, because CYCO can look back on 10 years of cybercrime experience. And, visionary and upfront as it has been since the beginning, CYCO must keep looking ahead and moving forward with this in mind.

Today, eight out of ten Swiss use the World Wide Web several times each week. This has led to the emergence of whole new areas of crime and new fields of operation, both for the police and the judiciary; police and judiciary with resources to deal with an offline population of eight million. What then are the repercussions for these two institutions faced with more than 2.7 billion people throughout the world accessing Swiss computer systems at the click of a mouse? And what will happen if, as Europol predicts, this figure increases to 3.5 billion by 2017, even if only a fraction of the users has malicious intentions?

In 2013 the first home-appliance botnet was discovered. The wide-scale cyber attack was carried out using the “Internet of Things” – a new term in the tech industry that refers to a concept whereby every household device is connected to the Internet. What will be the consequences on each and every one of us, on Switzerland as an economic centre and on law enforcement agencies if by 2020 around 200 billion such appliances or “things” are connected to the Internet?

With its transfer from the intelligence service to the Federal Criminal Police, CYCO has been successfully transformed into a cybercrime police unit and is recognised by international agencies such as Europol’s European Cybercrime Center (EC3) and INTERPOL’s Global Complex for Innovation (IGCI) in Singapore as a valuable partner. The course has been set for close international co-operation in fighting this new form of crime. Switzerland has the know-how, the resources and an optimum starting point for fighting cybercrime.

At national level, by the end of 2016, CYCO is required to submit to the Federal Council a strategy to implement Measure 6 of the National Strategy on Protecting Switzerland from Cyber Threat (NCS). This measure involves compiling an overview of national cases and a strategy to co-ordinate inter-cantonal case clusters. The challenge is twofold. On the one hand, in an age when budget cutbacks are an abiding topic, implementation must be economically viable and on the other hand, the strategy must be acceptable to all parties involved so as not to endanger the project by overlooking matters of jurisdiction between national and cantonal law enforcement agencies. We must not pass up the opportunities that the M6 NCS Project offers to all for the sake of safeguarding federalism. Indeed, the project even underpins our federalist structure.

There is much to be done. CYCO is committed to addressing the challenges of the coming decade, as always by looking ahead and moving forward into the (digital) future!

Table of Contents

1. A brief overview of 2013

- In 2013, the Cybercrime Coordination Unit Switzerland (CYCO) received 9,208 Suspicious Activity Reports on Cybercrime (CySARs) via the online reporting form. This represents an increase of 11.7 per cent over the previous reporting year.

- The proportion of CySARs relating to *property offences* rose again in 2013, to nearly 61 per cent of total reporting volume. Once again, CYCO received more CySARS from this category than from the category *offences against sexual integrity*, thus continuing the trend of the previous reporting period.

- CYCO submitted 356 crime reports to the competent national or international authorities as a result of the criminal relevance of the CySAR.

- By actively monitoring peer to peer networks, CYCO identified 238 people who were sharing child pornography.

- As a result of its preventive preliminary undercover investigations and investigations conducted under the provisions of the Criminal Procedure Code (CrimPC), CYCO submitted 17 crime reports to the competent cantons and a further 176 crime reports to foreign law enforcement agencies.

- CYCO began work on implementing Measure 6 of the National Strategy on Protecting Switzerland from Cyber Threat, preparing a detailed project analysis and defining the project organisation.

- On the occasion of its tenth anniversary, CYCO joined two social media platforms; Facebook (www.facebook.com/cybercrime.ch) and Twitter (@KOBIK_Schweiz).

2. A ten-year review

2000–2002: An idea emerges

In June 2000, the Conference of Cantonal Police Commanders of Switzerland (CCPCS) appointed the BEMIK Working Group[1] to examine the feasibility of establishing a national bureau to monitor cybercrime. The working group, headed by the current deputy director of fedpol, Adrian Lobsiger, identified urgent police co-ordination requirements and proposed a number of specific measures, voting unanimously in favour of establishing a national cybercrime co-ordination unit.

Based on the working group's findings, in the spring of 2001 the Federal Department of Justice and Police (FDJP) and the Conference of Cantonal Justice and Police Directors (CCJPD) resolved to work together to fight cybercrime. To this end, they signed an administrative agreement, defining the mandate, structure and funding of a national co-ordination unit.

KOBIK
SCOCI
CYCO

The CCJPD committee and plenary voted unanimously in favour of adopting the administrative agreement, following which the president of the CCJPD invited the cantons on 4th February 2002 to allocate sufficient funds in the 2003 budget. With the exception of Zurich, all cantons confirmed their participation in the project. On 20th February 2002, the Federal Council confirmed its intention of launching a national cybercrime coordination unit with the cantons with the aim of fighting cybercrime more effectively.

1st January 2003: CYCO goes into operation

On 1st January 2003, CYCO went into operation, beginning with an online complaints form in four languages on www.cybercrime.admin.ch (see image on the right). The website also provided background information on CYCO and on cybercrime in general. The new coordination unit received wide attention in the electronic media and in IT print media, which included various background articles and interviews. A first review after 6 months concluded that CYCO had got off to a good start and this was communicated in a press release.

[1] Intercantonal Working Group on Combating the Misuse of Information and Communication Technology (BEMIK working group)

May 2003: Active monitoring begins

At the beginning of May, CYCO began its monitoring activity, focussing on peer to peer (P2P) networks. Monitoring entails searching these file exchange networks for illegal content shared by users with a Swiss IP address. After completing the preliminary work, the case is forwarded as a crime report to the competent cantons.

9th January 2004: CYCO publishes its first annual report

The first annual report was a short review of CYCO's history, the establishment of the steering committee and staff recruitment. The report also included statistics on reporting volume and monitoring. The statistics showed that in its first year CYCO received 6,457 CySARs from the public and submitted more than 100 crime reports to the cantons as a result of monitoring the Internet.

2004: The first reorganisation

To harmonise and strengthen the CYCO's team management, CYCO's clearing unit was moved from the Federal Criminal Police Division (FCP) to the Service for Analysis and Prevention (SAP).

2005: Integration into the MELANI/Cybercrime Section

The CYCO clearing and analysis units were merged into one unit as part of the 2004 reorganisation. This unit was subsequently incorporated into the new MELANI Cybercrime Section.

Following the decision by Canton Zurich to participate in the project and contribute to the costs, CYCO's Monitoring Unit was increased to 9 staff members.

2005–2006: Work on prevention is strengthened

As part of a 2005 national campaign to stop child pornography, CYCO began working closely with Swiss Crime Prevention (SCP), participating in various training courses and symposiums. This phase eventually led to the DNS Blacklist project in 2007. CYCO also became a partner to Microsoft Switzerland's prevention programme *Security for Kids*.

2006: Agreement with the national police of Liechtenstein

Under an agreement in 2006 with the national police of Liechtenstein, CYCO extended its services to the Principality of Liechtenstein.

2007: Launch of the DNS Blacklist project

The DNS Blacklist project was launched in 2007 and is based on voluntary co-operation between CYCO and the largest Swiss Internet providers. Using the Child Sexual Abuse Anti-Distribution Filter software, CYCO keeps an updated list of web-sites containing child pornography based on information it receives from the public. CYCO makes this blacklist available to Internet providers, who in turn block access to the sites in question according to their general terms and conditions and conditions.

2007: New reporting volume record

In its fifth year of operation, CYCO registered a marked increase in reporting volume. With more than 10,000 CySARs in 2007, it introduced a triage system and consolidated its position as national point of contact for cybercrime matters. The increase in reporting volume was a result of growing economic crime and a few particularly active citizens who submitted dozens of CySARs each month. After five years, CYCO made a positive review of its activities and was thus equipped for future challenges in its position as national competence centre for cybercrime.

2008: CYCO undergoes transformation

In view of the impending integration of CYCO into the Federal Criminal Police Division planned for the following year, the Coordination Unit reorganised its staff and updated its technical equipment, modernising its IT structure and improving its hard- and software.

2009: CYCO is incorporated into the Federal Criminal Police Division

On 1st January 2009, CYCO and MELANI were officially separated. CYCO was incorporated into fedpol's Federal Criminal Police Division and MELANI (which had been part of fedpol's SAP Division) was incorporated into the newly established Federal Intelligence Service (FIS). As a result, CYCO began to perform more and more operational tasks and police duties, such as co-ordinating national and international investigations, and exchanging police data. These additional tasks required a reorganisation of the Coordination Unit. Also, the two monitoring and clearing sections were merged into a new CYCO Operative Section.

2010–2011: Increasing monitoring activity

CYCO increased its active monitoring of file exchange networks, which led to a rise in the number of crime reports sent to the cantons. During 2010, the Coordination Unit was especially active in the field of preliminary undercover investigations.

A legislative loophole in cantonal provisions which had arisen following the enactment of the new Criminal Procedure Code (CrimPC) meant that from 1st January 2011 most cantonal police officers were no longer permitted to conduct preventive preliminary undercover investigations of suspected paedophile criminals on the Internet. A few cantons such as Schwyz, Aargau and Obwalden recognised the need to act early and adapted their police legislation accordingly, with effect from 1st January 2011. Together with the CCJPD, the FDJP found a solution that enabled CYCO to expand its preventive monitoring of online paedophile crime following new statutory provisions. Under an agreement with the Security Department of Canton Schwyz, CYCO was permitted to carry out preventive monitoring of the Internet on behalf of the cantons and thus to monitor chat rooms. CYCO's undercover investigations of this type are currently still based on this agreement as well as on authorisation from the Compulsory Measures Court of Canton Schwyz. This ensures that paedophile criminals cannot operate in a legislative vacuum on the Internet.

2011: National File and Hash Value Collection (NFHVC)

In the years leading up to 2011, a group (later to become the NFHVC Working Group) had been working on establishing a national database of child pornographic images and hash values. CYCO restarted work on the project in 2010 and made considerable progress. In 2011 the cantonal police forces were instructed on the use of the database and CYCO received the first picture archives.

2011–2012: National Cyber Defence Strategy (later to become the National Strategy on Protecting Switzerland from Cyber Threats)

Since May 2012, CYCO has had a seat on the National Cyber Defence Strategy project team, representing the interests of the cantonal and national law enforcement agencies in the implementation of cyber defence strategy.

On 27th June 2012, the Federal Council approved the strategy, now renamed *National Strategy on Protecting Switzerland from Cyber Threat*. The strategy aims to minimise through co-operation the cyber threat to the private and public sector, as well as to operators of critical infrastructures. The strategy is expected to be fully implemented by 2017.

January 2012: Council of Europe Convention on Cybercrime

By ratifying the Council of Europe Convention on Cybercrime Switzerland is committed to international efforts to combat Internet crime. The provisions of the Convention came into force in Switzerland on 1st January 2012. The necessary legislative amendments were enacted by the Federal Council at the same time.

October 2012: Roll-out NFHVC

The National File and Hash Value Collection came into operation in October 2012, following successful completion of all test runs and system adjustments.

December 2012: Switzerland joins the Global Alliance against Child Sexual Abuse Online

CYCO specialists provided Federal Councillor Simonetta Sommaruga with support on the occasion of Switzerland joining the Global Alliance in Brussels.

January 2013: European Cybercrime Centre at Europol

CYCO has been an active member of Europol's Focal Points CYBORG and TWINS since 2011. Both Focal Points[2] have been newly incorporated into the European Cybercrime Centre (EC3), which began work on 1st January 2013. EC3 is hosted by Europol in The Hague and focuses on fighting cyber crime by supporting EU member states in building operational and analytical capacity for investigations and co-operation with international partners.
Its mandate is to tackle cybercrime by organised groups, online child sexual exploitation, and attacks against critical infrastructure and information systems in the EU member states. Its analyses and assessments help identify and combat potential threats.

2013: Implementing the National Strategy on Protecting Switzerland from Cyber Threat

As part of implementing Measure 6 of the National Strategy, the FDJP and the cantons are required to present a strategy paper by the end of 2016 containing a comprehensive overview of cases and details of the co-ordination of inter-cantonal case clusters. The paper aims to clarify interfaces with other players involved in reducing the cyber threat, co-ordinate situation analyses, and define the resources and legislative amendments necessary at cantonal and federal level for implementing the strategy paper. In 2013 CYCO prepared a detailed project analysis and defined the project organisation.

December 2013: CYCO joins Facebook and Twitter

CYCO has had a Facebook and Twitter account since 22nd December 2013.

[2] Focal Points are departments within Europol that specialise in co-ordinating and analysing international case clusters. The Focal Points were developed from the former Analysis Workfiles (AWF).

3. CYCO, the Reporting Office

CYCO is Switzerland's central contact point for anyone wishing to report suspicious content on the Internet. When a CySAR is filed using the online reporting form (www.cybercrime.ch), CYCO analyses it for criminal relevance and secures the necessary data. If there are indications for a criminal offence, CYCO sends a crime report to the appropriate law enforcement agency in Switzerland or abroad.

3.1. Reporting volume

From 1st January to 31st December 2013, CYCO received a total of 9,208 CySARs. This is an increase of 11.7 per cent over the previous reporting period (2012: 8,242 CySARs).

The number of CySARs does not allow drawing any conclusions on cybercrime trends or the volume of illegal content on the Internet. It only reflects the public's awareness of and willingness to report it to the authorities.

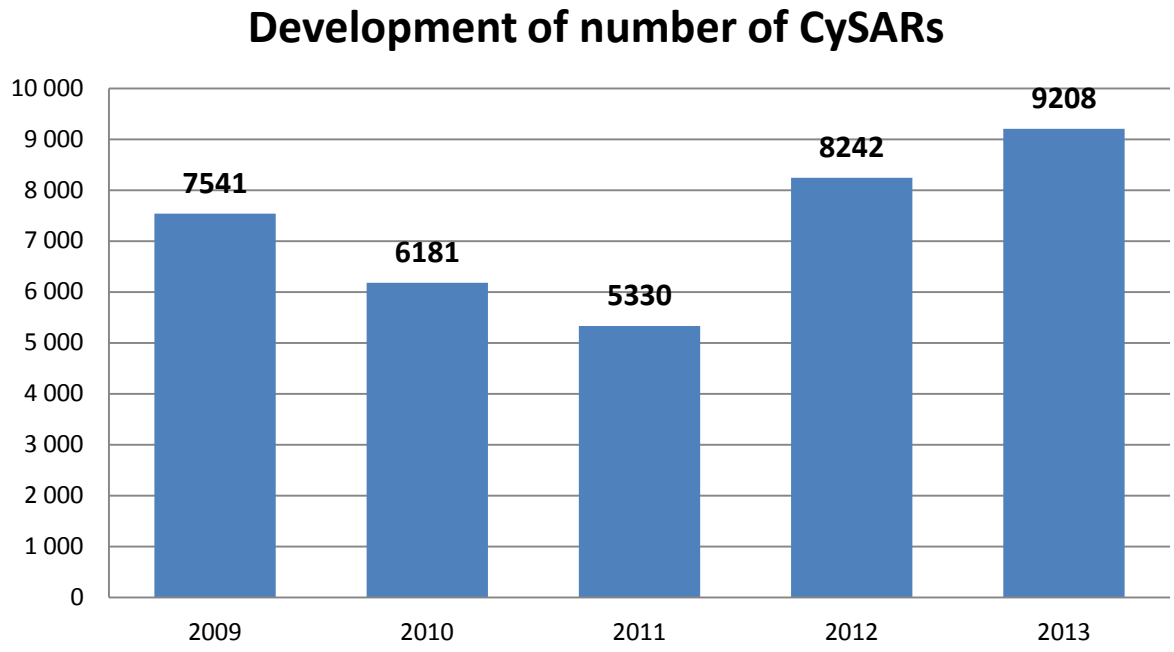


Figure 1 : Development of the reporting volume over www.cybercrime.ch

On average CYCO received 767 CySARs each month, although there were noticeable fluctuations in May (1,083 CySARs) and in September (585 CySARs). These fluctuations can result from specific incidents such as a press release by CYCO.

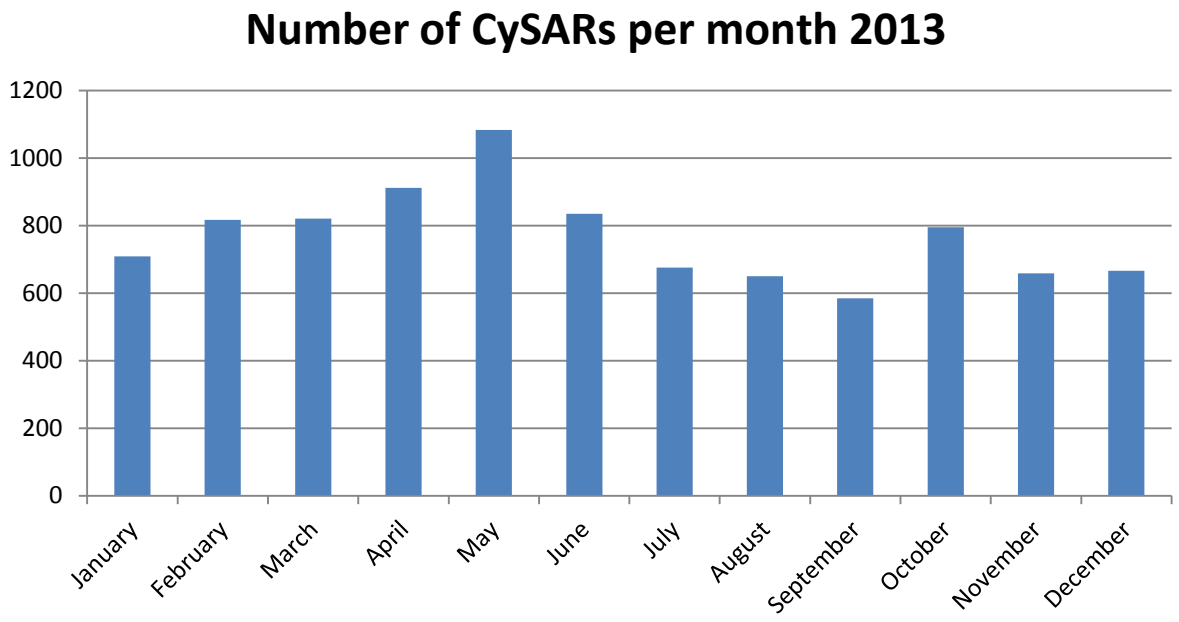


Figure 2 : Reporting volume per month via www.cybercrime.ch (total 9,208 CySARs)

3.2. Subject matter of CySARs

Eighty-six per cent of the CySARs received by CYCO in 2013 showed a relevance to the Swiss Criminal Code. The remaining CySARs related to violations against the Unfair Competition Act[3] (290 CySARs), the Copyright Act[4] (24 CySARs), the Civil Code[5] (40 CySARs), the Narcotics Act[6] (14 CySARs) and the Anti-Money Laundering Act[7] (7 CySARs). Around ten per cent of the CySARs contained no criminally relevant matter at all.

The offences reported in the CySARs can be divided into two categories. The first involves cybercrime in a narrow sense, i.e. criminal offences committed either by using Internet technology or by exploiting vulnerabilities in the system. Such offences include hacking, Distributed Denial of Service attacks (DDoS) or the production and circulation of malware. These offences are made possible by the Internet and are directed against Internet technology. Cybercrime in the broader sense, on the other hand, exploits the Internet as a means of communication, for example by using e-mail or data exchange for inappropriate or harmful purposes such as sending spam, operating scams on advertising platforms or distributing illegal pornography.

Much of the subject matter of the CySARs did not relate to offences prosecuted *ex officio* and therefore required the victim to contact the competent cantonal police office and file a criminal complaint.

---

[3] Federal Act of 19 December 1986 on Unfair Competition (UCA), SR 241

[4] Federal Act of 9 October 1992 on Copyright and Neighbouring Rights (CopA), SR 231.1

[5] Swiss Civil Code of 10 December 1907 (CC),SR 210

[6] Federal Act of 3 October 1951 on Narcotics and Psychotropic Substances (NarcA), SR 812.121

[7] Federal Act of 10 October 1997 on Combating Money Laundering and the Financing of Terrorism in the Financial Sector (AMLA), SR 955.0

The proportion of CySARs relating to property offences rose again in 2013, continuing the trend from the previous year. In 2013, 60.7 per cent of CySARs involved *property offences* (Art. 137–172ter of the Swiss Criminal Code SCC). In second place, with 20 per cent of the total number of CySARs, were *offences against sexual integrity* (Art. 187–212 SCC). This represents a marked decrease of 40.3 per cent over the previous reporting period.

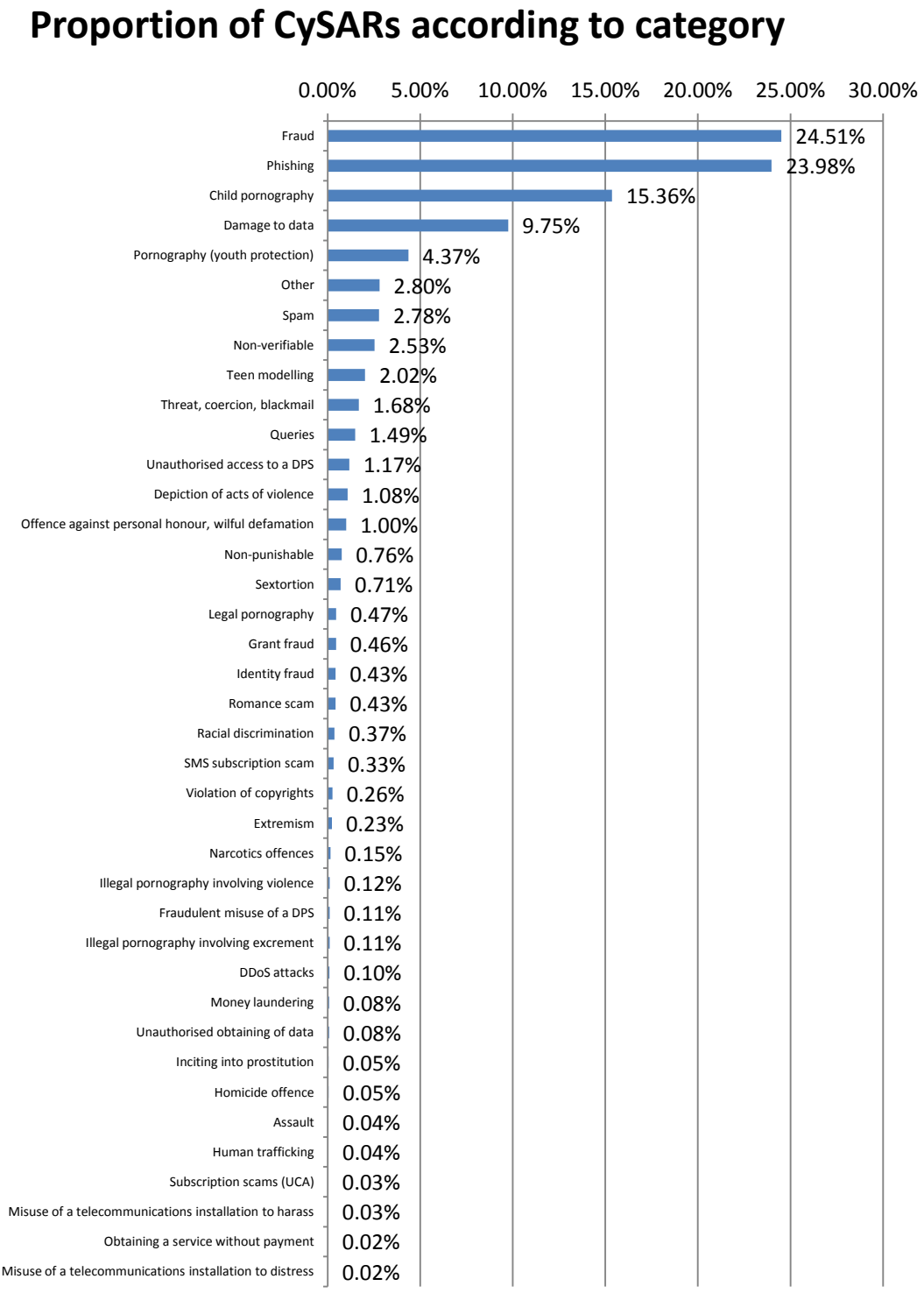


Figure 3 : Proportion of CySARs according to category 2013

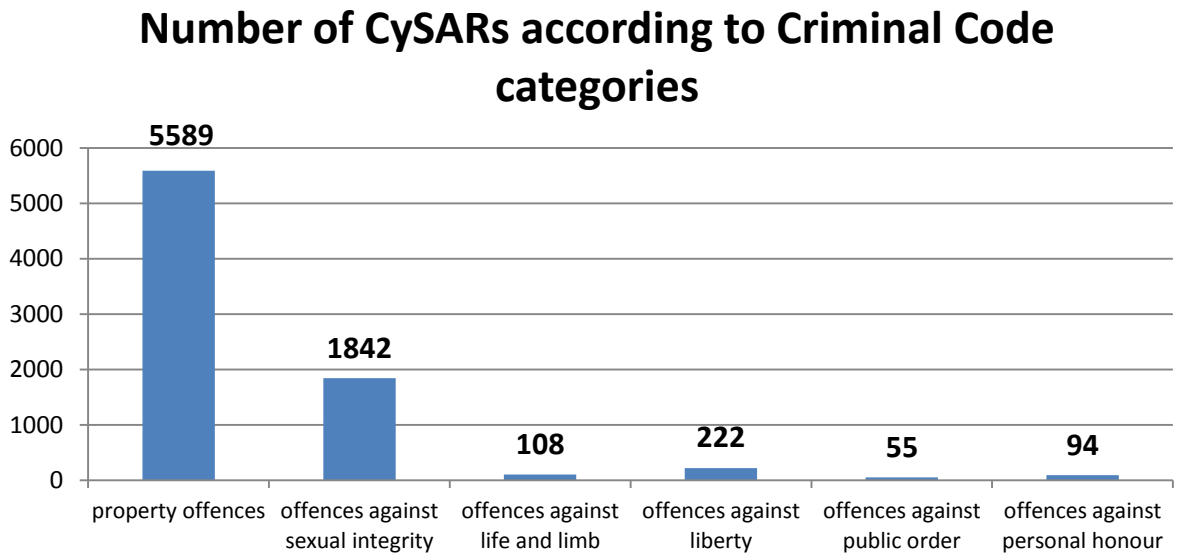


Figure 4 : Number of CySARs according to categories of the Criminal Code (total 7,910 CySARs)

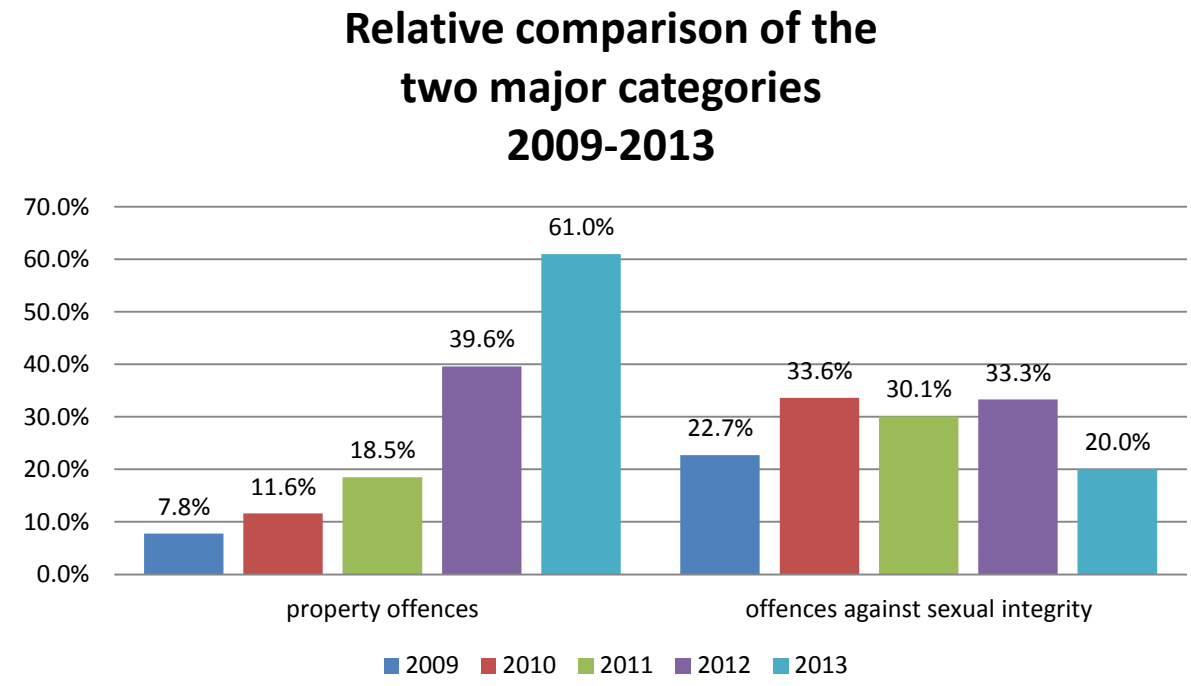


Figure 5 : Relative comparison of the two major categories 2009–2013

3.2.1. CySARs concerning property offences

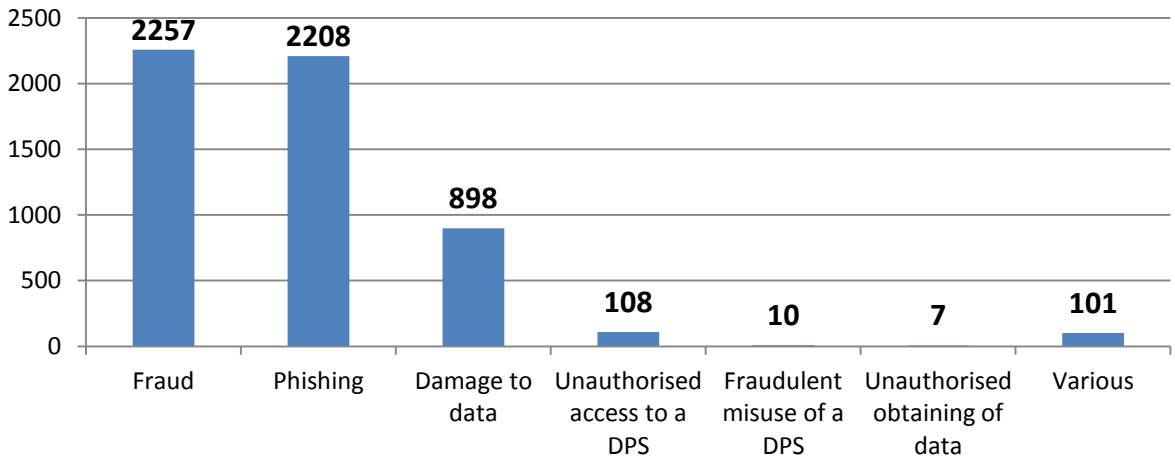


Figure 6 : Number of CySARs concerning property offences (total 5,589)

Most of the reports filed in 2013 – 5,589 CySARs amounting to 60.7 per cent of the total reporting volume – concerned *property offences*, whereby the sub-category *fraud* made up 25 per cent of total reporting volume (2,257 CySARs).

The types of fraud reported to CYCO in 2013 were numerous. The number of CySARs concerning attempted fraud against buyers and sellers on auction and classified advertising websites increased. CYCO noticed that fraudsters intensified their efforts to lend credibility to their attempted fraud, for example by creating bogus websites for fictitious transport companies along with whole package tracking systems, with the purpose of deceiving victims for as long as possible into believing that purchased or dispatched items were on their way. Fraudsters were also up to date on current developments and exploited situations such as the latest housing shortage in major Swiss conurbations, which gave rise to fraudulent advertisements on real estate websites requesting upfront payment for cheap rental accommodation in Zurich and Basle which in reality did not exist.

In 2013, there was a marked increase in the number of reported phishing attempts: CYCO received 2,208 CySARs in this category (2012: 662 CySARs), which represents more than a threefold increase over the previous reporting period. Most of the CySARs in this category related to fraudsters sending spam to potential victims with the purpose of luring them onto websites offering well-known Internet services and then inducing them to disclose their user data (e.g. user name, password, etc.). Approximately one-fifth of phishing CySARs concerned attempts to obtain access data to the services of Swiss banking institutions.

There was a renewed increase in the number of CySARs involving cybercrime in the narrow sense: CYCO received over 20 per cent more reports on offences in this category than during the previous reporting period. In particular the category *damage*

to data recorded a noticeable increase of 124 per cent (898 CySARs) over 2012. One modus operandi frequently reported in this category was the organised but random channelling of malware – such as ransomware – to the computers of private individuals or companies. A computer infected with ransomware is blocked for further use. To have the restriction lifted the victim is required to pay a "ransom" in the form of a promotional code from an anonymous payment services provider.

In the second half of 2013 a new kind of ransomware known as CryptoLocker appeared, resulting in a rise in corresponding CySARs. When activated, the malware encrypts computer files, rendering them inaccessible. The malware then displays a message which offers to decrypt the data if a payment is made.

More and more small and medium-sized businesses (SMBs) fell victim to targeted attacks against their websites or telecommunication infrastructure. For example, criminals gained unauthorised access to modern Voice-over-Internet-Protocol (VoIP) systems to conduct telephone calls to countries in Africa, and Central and South America, causing costs of several thousands of Swiss francs to the targeted companies. A further angle of attack was client data such as e-mail addresses, telephone numbers and invoice data, which criminals accessed through security vulnerabilities in company websites. Although victims did not suffer any direct financial damage, the security breaches caused follow-up costs to secure the data, install back-ups and rectify the vulnerabilities. As a result, companies could possibly lose their clients' trust. Also, the stolen data is often used to commit other types of fraud such as identity theft, or to infiltrate e-mail accounts with the purpose of committing scams like advance-fee fraud.

3.2.2. CySARs concerning offences against sexual integrity

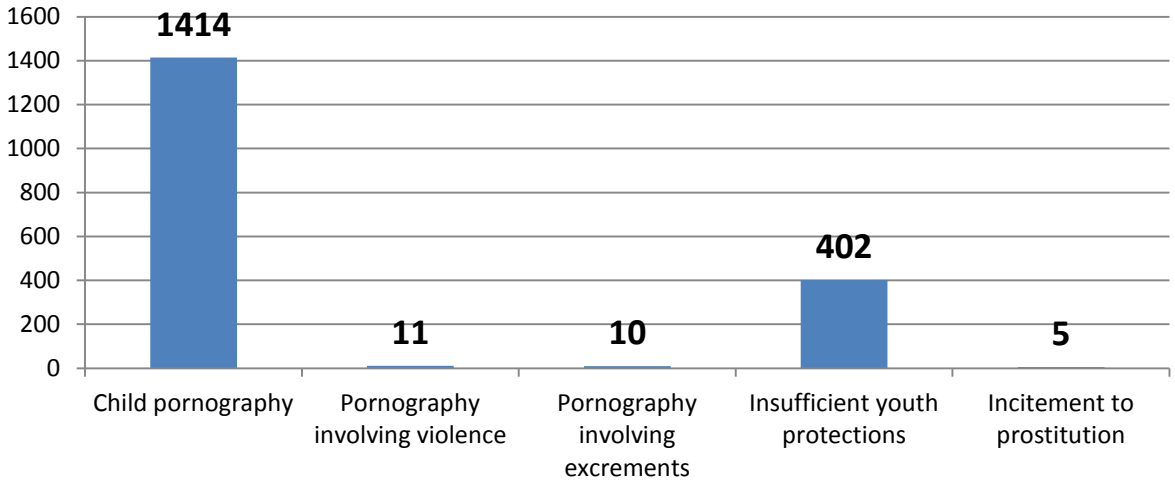


Figure 7: Number of CySARS concerning offences against sexual integrity (total 1,842)

The number of reports concerning offences against sexual integrity fell by nearly 40 per cent, from 3,083 CySARs in 2012 to 1,842 CySARs in 2013. Whereas CYCO received approximately one-third more reports concerning pornographic websites where youth protection was insufficient (2013: 402 CySARS, 2012: 307 CySARs), it received 47 per cent fewer reports concerning websites containing child pornography (2012: 2,684 CySARs, 2013: 1,414 CySARs).

3.2.3. Further offences

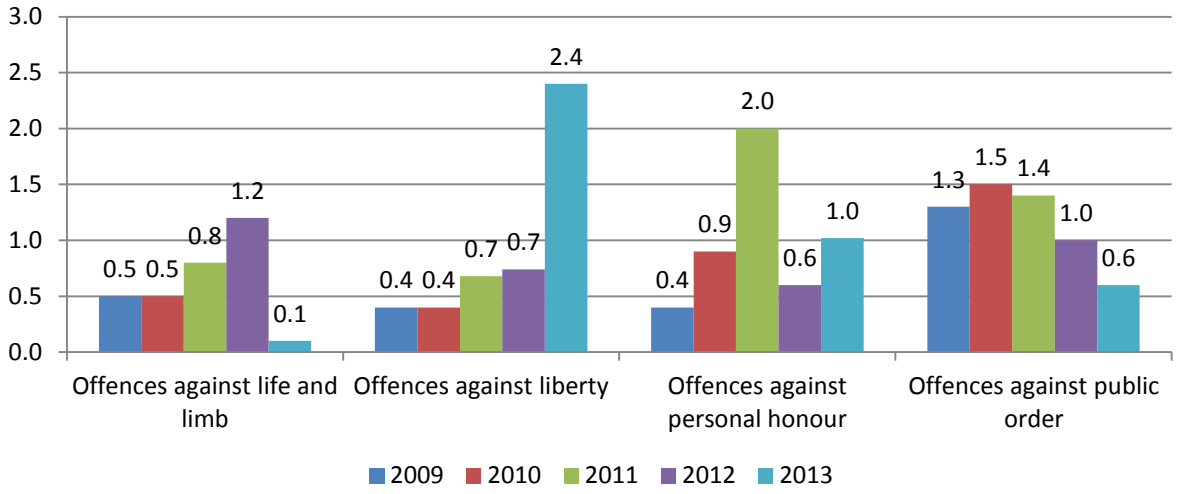


Figure 8: Relative comparison of other offences related to SCC, reported to CYCO 2009-2013

Approximately four per cent of the total reporting volume concerned offences against life and limb, liberty, public order and personal honour. The 2.4 per cent of CySARs concerning offences against liberty mostly involved cases where a person had been contacted – usually by a woman – via an online dating or social media platform and seduced into performing sexual acts in front of a camera. The victim had then been blackmailed into paying a ransom so that the videos would not be published on the Internet. The number of CySARs concerning offences against personal honour was again small, as during the previous reporting period.

3.2.4. Conclusion

The number of CySARs concerning offences against property increased once again in 2013, rising by one-third and thus continuing the trend started during the previous reporting period. At the same time, the number of CySARs concerning offences against sexual integrity fell by one-third. For the first time, the number of CySARs concerning the categories *phishing* and *fraud* (offences against property) was higher than the total number of CySARs concerning offences against sexual integrity.

3.3. Facts and figures

Here is a summary of the most important facts and figures concerning the CySARs submitted to CYCO in 2013:

- All 9,208 CySARs were analysed with regard to their criminal relevance within an appropriate time-frame.
- CYCO replied individually to 3,457 of the 9,208 CySARs.
- CYCO sent 35 crime reports directly to the competent canton or authority on account of the criminal relevance of the CySAR.
- 321 CySARs were forwarded to foreign law enforcement agencies (via INTERPOL or Europol) or to non government organisations working in a related field (e.g. inhope).
- Numerous CySARs were forwarded to fedpol's Federal Criminal Police Divisions (General, Organised and Financial Crime Section and Paedophile Crime and Pornography Section).
- CYCO published nine alerts on its website (www.cybercrime.ch) on the most frequently reported types of offence. By forwarding these alerts to MELANI, Swiss Crime Prevention and the media, CYCO succeeded in alerting large sections of the general public to the latest cyber threats.

3.4. Case study

CYCO was informed by a Swiss web hosting service provider about an unidentified user who was using the provider's services to operate an online shop selling stolen credit card data. The web hosting service provider sent CYCO the stolen information and log files, which were forwarded to Europol. The latter's European Cybercrime Center (EC3) analysed the data and contacted the appropriate lending institution to have the relevant cards inactivated.

4. Monitoring

Besides handling online reports (CySARs) from the public, CYCO also conducts its own independent search for suspicious content in less accessible areas of the Internet (preventive monitoring), thus contributing to cybercrime prevention. The CYCO Steering Committee redefines its monitoring priorities each year. As in previous years, the priority for 2013 was combating paedophile crime on the Internet. However, in view of the rising number of reports on economic crime, the Steering Committee emphatically stated that CYCO should not neglect its monitoring of offences against property and Internet crime in the strict sense. In practice, this decision impacted particularly on CYCO's activities in the field of co-ordinating national and international investigations (see Chapter 5.2).

As a result of CYCO's monitoring activities, 423 crime reports were compiled in 2013. This is a decrease of six per cent over the previous reporting period.

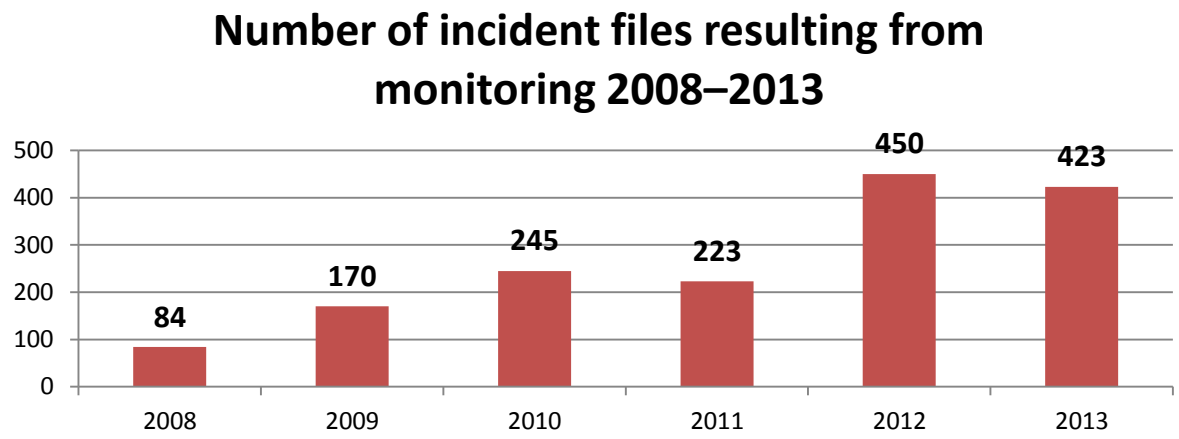


Figure 9 : Number of crime reports from active monitoring of the Internet by CYCO 2008-2013

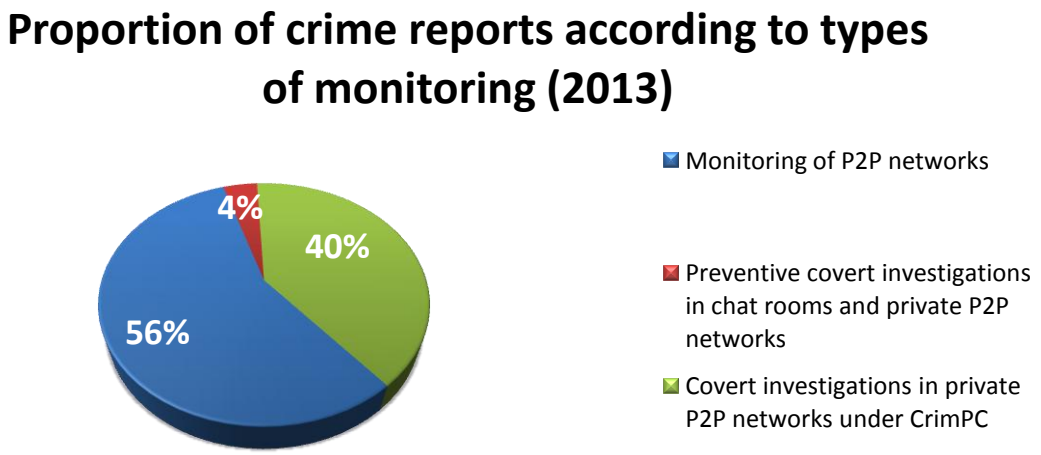


Figure 10 : Proportion of crime reports according to type of monitoring (total 423)

4.1. Monitoring peer-to-peer networks (P2P)

Of the 423 crime reports compiled as a result of CYCOs active monitoring, 238 resulted from CYCO's monitoring of open P2P file-sharing platforms and involved Internet users who were actively exchanging child pornography as defined under Article 197 paragraph 3 SCC. In comparison to 2012 (450 reports), this represents a decrease of 47.1 percent (falling to the same level as in 2011) despite the fact that CYCO continued to monitor the Internet with same intensity and according to the same criteria as during the previous reporting period.

Although CYCO specifically searches for users in Switzerland, it also identified offences committed by ten people beyond Swiss borders. The findings were transmitted via INTERPOL to the competent authorities of the countries concerned.

4.2. Preventive preliminary undercover investigations

The *Agreement on Co-operation in Police Investigations of the Internet for Combating Paedophile Crime (Monitoring of Chat Rooms)* between CYCO, the Federal Office of Police 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 online paedophile crime[8]. Hence CYCO conducts preventive preliminary undercover investigations explicitly by order and under the supervision of the cantonal police of Canton 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 investigations, 17 crime reports were sent to the competent cantonal authorities. Of these 17, three were a result of undercover investigations in chat rooms exclusively reserved for children. All three cases involved attempted sexual acts with children as defined under Article 187 SCC.

The remaining 14 crime reports resulted from undercover investigations of closed-source P2P file-sharing sites. In contrast to classic P2P networks, data is not shared in an open network, but encrypted and shared directly between computers. This means that the legal provisions on undercover investigations apply. Most crime reports compiled as a result of undercover investigations of non public file-sharing sites involve the possession and distribution of illegal pornography as defined under Article 197 paragraph 3 or 3bis SCC.

4.3. Undercover investigations under the Criminal Procedure Code

For the first time in its ten-year history, CYCO was requested by cantonal public prosecutors' offices to conduct undercover investigations under the Criminal Procedure Code. The investigations in private filesharing networks were carried out under Article 285a et seq. CrimPC and resulted in 168 crime reports being sent to the competent police authorities in Switzerland and abroad.

[8] Operations as defined under Article 9d of the Law of 22 March 2000 of the Canton of Schwyz on the Cantonal Police (PolV – SRSZ 520.110).

Due to the global nature of private P2P networks it is difficult to focus only on Swiss users. During the investigation, two Swiss users were identified; the remaining 166 crime reports were transmitted to law enforcement agencies abroad as part of the international exchange of police information.

4.4. Feedback from the cantons

If there is a well-founded suspicion that a criminal offence has been committed, CYCO sends a crime report to the competent cantonal authorities for follow-up action To gain an overview of the action taken by the cantonal authorities, CYCO requests updates from the cantons on the progress of the case (e.g. on what police measures have been taken and the outcome of court proceedings).

To gain a better overview of recent developments, the following data only includes feedback from the cantons from 2013. Most of the crime reports transmitted to the cantons in 2013 were based on the active monitoring of P2P networks in 2012 (417 files) and involved people who were actively engaged in sharing child pornography. 98 percent of all crime reports submitted to the competent cantonal authority led to a house search.

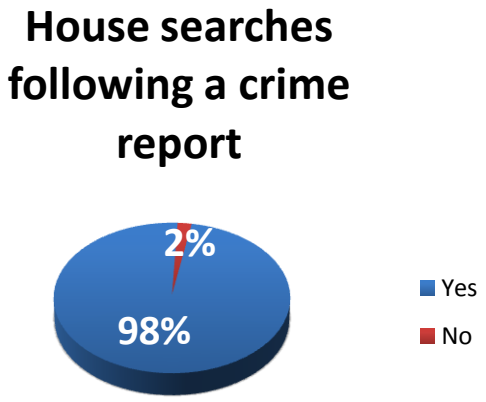


Figure 12 : House searches 2013

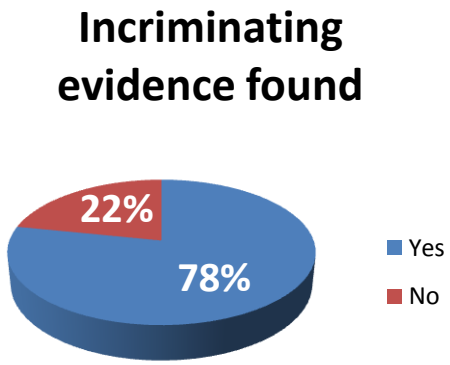


Figure 13 : Incriminating evidence found 2013

4.4.1. Feedback from the cantonal police

Police found incriminating evidence in 78 per cent of all house searches. In cases where a house search did not turn up any incriminating evidence, it is difficult to pinpoint the reasons: unencrypted and therefore unprotected wireless networks or outsourcing data to cloud services often make it difficult to secure evidence and to clearly identify suspects.

93 per cent of the cases where incriminating evidence was seized related to child pornography. This high figure is not surprising since CYCO searches P2P networks specifically for this category of offence and most crime reports result from these monitoring activities. It is also worth mentioning that in more than half of these cases the police identified further offences relating to illegal pornography as defined by Article 197 SCC (see Figure 14). By way of example, in more than 50 per cent of all

house searches, the police also seized pornography relating to sexual acts with animals.

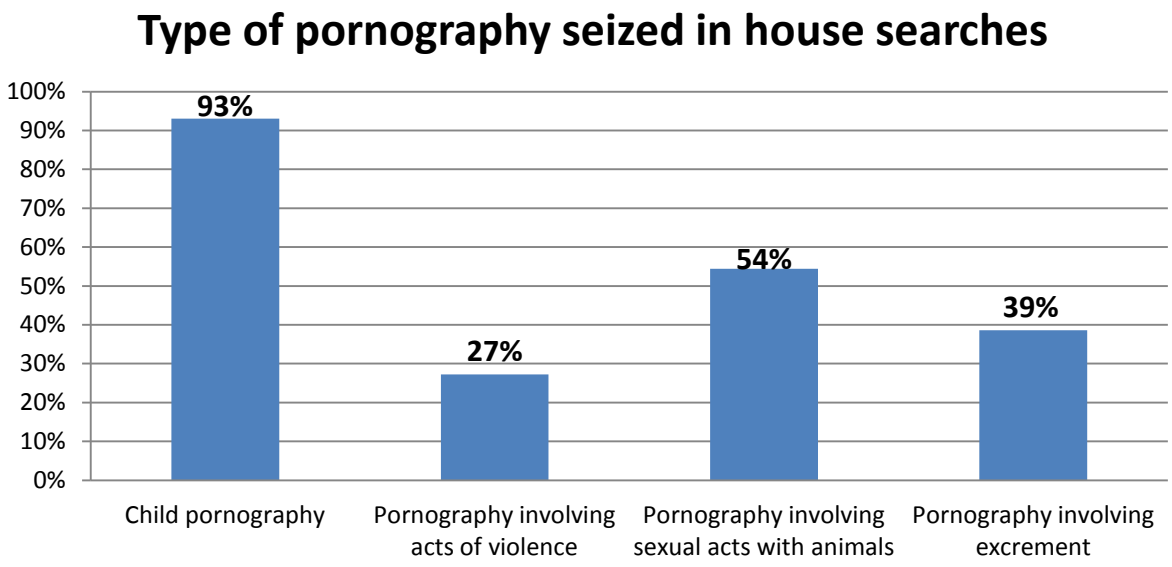
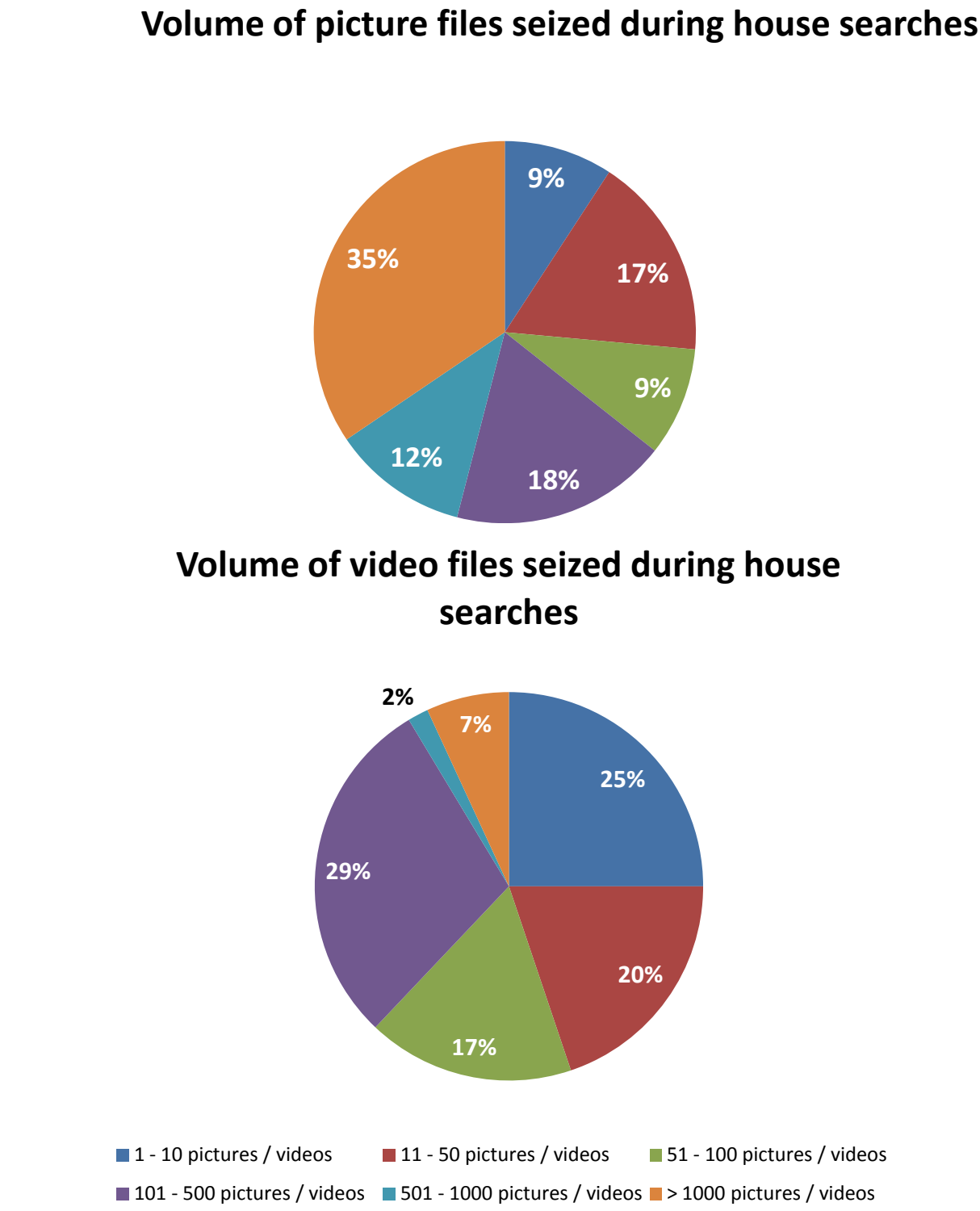


Figure 14 : Type of pornography seized during house searches in 2013

Feedback from the cantonal police also revealed that video files were seized in 94 per cent and picture files in 66 percent of all house searches. In total, the house searches led to the seizure of several million illegal picture and video files.



Figures 15 and 16 : Volume of picture and video files seized during house searches

4.4.2. Feedback from the cantonal judiciary

In 91 per cent of the cases in which the cantonal judiciary provided CYCO with feedback, criminal proceedings had led to a conviction.

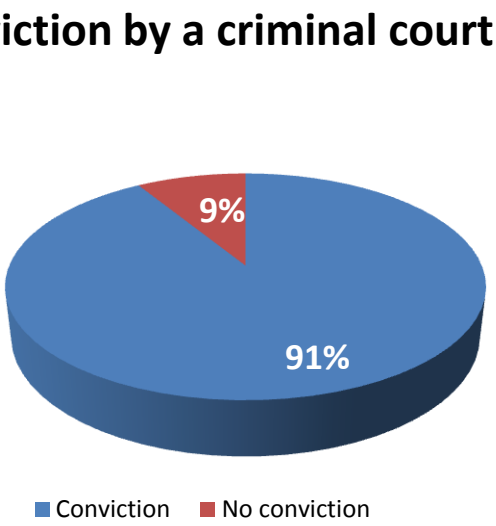


Figure 17 : Proportion of convictions in 2012 based on feedback from the cantonal judiciary

Most convictions were for offences concerning illegal pornography, in particular for the acts defined under Article 197 paragraphs 3 and 3bis SCC.

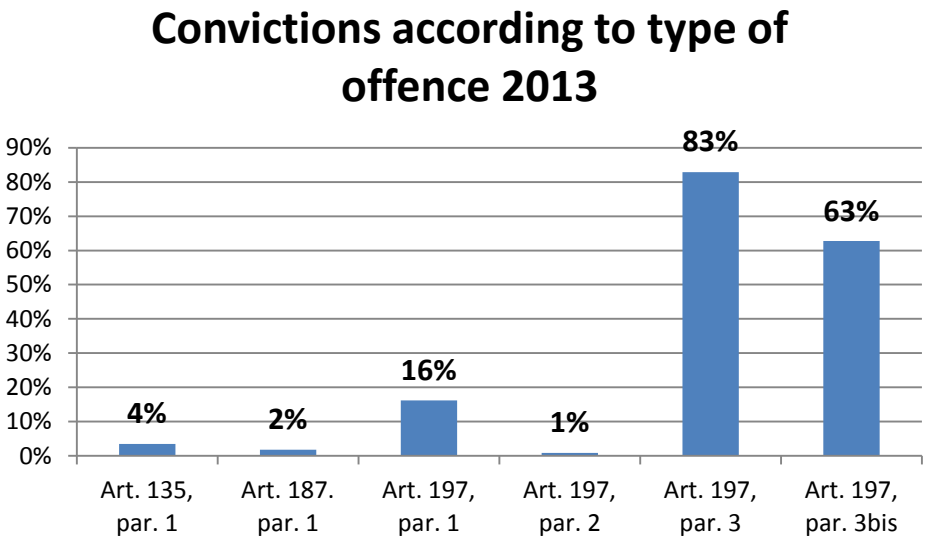


Figure 18: Relative comparison of convictions according to type of offence 2013

In 85 per cent of the convictions reported to CYCO in 2013, a monetary penalty was imposed on the offender (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 amount of which is based on his or her personal and financial circumstances). In 77 percent of these cases the offender also received a fine. In 91 per cent of the convictions the monetary penalty was combined with probation. In four per cent of the convictions, the offender was ordered to undergo ther-

apy, was sentenced to perform community service, was given a custodial sentence or received a monetary penalty not combined with probation.

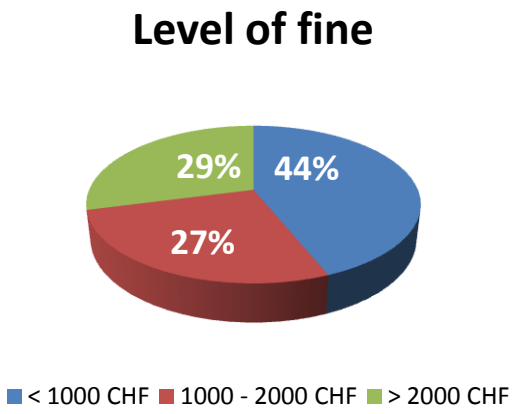


Figure 19: Level of fine imposed (in CHF)

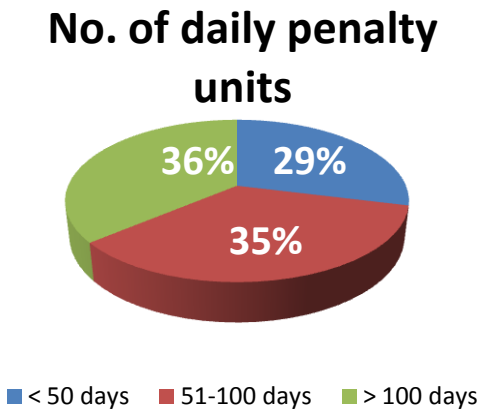


Figure 20: Number of daily penalty units imposed

In approximately fourty-four per cent of the convictions the fine amounted to less than CHF 1,000. In twenty-seven per cent of the convictions the offender was fined between CHF 1,000 and CHF 2,000. Only twenty-nine per cent of the fines were higher than CHF 2,000.

Twenty-nine per cent of the monetary penalties were fixed at 50 or less daily penalty units. In thirty-five per cent of the convictions the monetary penalty was fixed at between 51 and 100 daily penalty units. In thirty-six per cent of the convictions the monetary penalty was fixed at more than 100 daily penalty units.

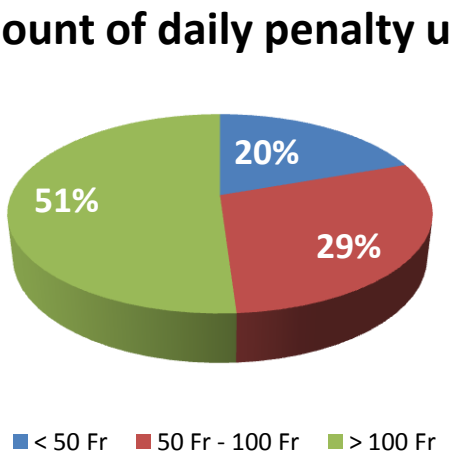


Figure 21 : Amount of daily penalty unit imposed (in CHF)

In twenty per cent of the convictions the daily penalty unit was fixed at between CHF 1 and CHF 50. In twenty-nine per cent of the convictions it was fixed at between CHF 51 and CHF 100, and in fifty-one per cent of the convictions at more than CHF 100.

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

4.5. Case studies

During the current reporting year, the police arrested three people who were seeking sexual contacts with minors through children's chat rooms. One of the suspects even insisted on a meeting with the victim after only a few minutes' chat, stating his intention to carry out sexual acts with the "minor" who in reality was one of CYCO's preliminary undercover investigators. The cantonal police succeeded in arresting the suspect who was armed with a knife on his way to the rendez-vous to meet the alleged 13-year-old girl. This case illustrates the danger of sexual offenders who operate in children's chat rooms.

A case of actual child abuse came to light after CYCO's active monitoring of the Internet revealed that illegal pornography was being shared on certain P2P networks. CYCO submitted several crime reports to the cantonal police whose inquiries revealed that a father, living together with his wife and children, had been sexually abusing his three year-old daughter for several months. The suspect had no previous criminal record. Thanks to close co-operation between CYCO and the competent cantonal police and to detailed investigations by the latter, the suspect was arrested and thus prevented from further abusing his child.

In another case of active Internet monitoring, CYCO identified a German national who was sharing child pornography on P2P networks. It subsequently sent a crime report to the German authorities via INTERPOL. The public prosecutor revealed that the suspect was the 45-year-old head of an association which claimed its work focussed on "child and youth protection from violence, pornography and cyber mobbing, as well as in the fields of film rating, youth protection software, Internet safety, computer games, smartphones and media project advice". The association was funded by the federal state in which it was located.

All these cases show how important it is for the competent police authority to deal systematically with crime reports submitted by CYCO. This poses a real challenge to some cantons because of the high number of crime reports compiled by CYCO and the insufficient resources in some cantons to deal with such time-consuming cases.

5. Exchange of police data

5.1. Incoming and outgoing requests

Since CYCO's incorporation into the Federal Criminal Police in 2009 and the Steering Committee's decision that CYCO should also focus on monitoring offences against property and Internet crime in the narrow sense, the exchange of criminal police relevant data with partners both in Switzerland and abroad has become increasingly important. CYCO has become the centre of this flow of information, supporting the cantons in their investigations by ensuring the exchange of data. Thanks to its wide contact network of partners in the private and public sectors, and of its partners in the cantons and abroad, CYCO has become a competence centre for coordinating investigations and criminal proceedings. It also functions as an interface to international organisations such as INTERPOL and Europol and especially to the European Cybercrime Center (EC3).

Since the Council of Europe's Convention on Cybercrime came into force in Switzerland on 1st January 2012, Switzerland has increasingly become an active partner at an international level in the fight against Internet crime. This is reflected in the noticeable increase in the volume of data exchanged with foreign authorities on issues falling within the scope of the Convention. The following figures clearly illustrate this point.

In 2013 CYCO received 739 requests for information from foreign partner agencies, which is an increase of 53 per cent over the previous reporting period. Similarly, there was an increase of 68 per cent in the number of requests for information CYCO made to foreign law enforcement agencies (via INTERPOL and Europol), figures climbing from 561 in 2012 to 946 in 2013. The increase in requests to its partners abroad, made on behalf of the cantons and as a result of CYCO's own investigations, bears a direct relation to the increase in the overall reporting volume.

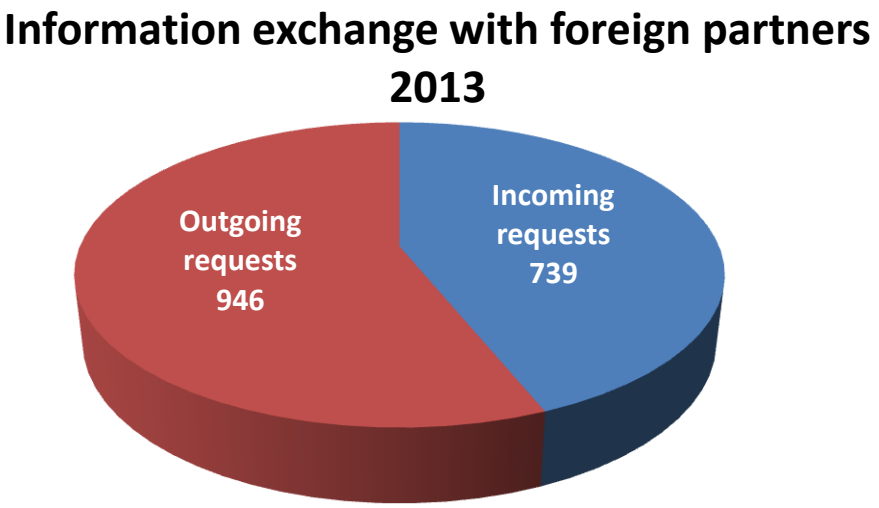


Figure 22 : Information exchange with foreign partners

A special feature of the Cybercrime Convention is the expedited preservation of stored computer data under mutual assistance (Article 29 et seq.). Under these provisions CYCO forwarded eight requests on behalf of the cantons to foreign law enforcement agencies and, conversely, received four requests from its foreign partners.

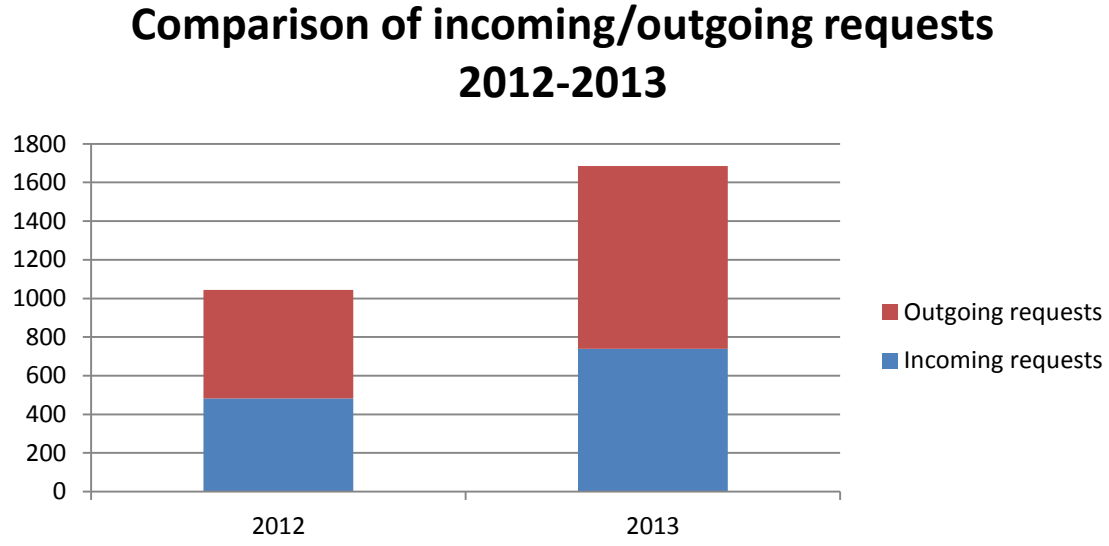


Figure 23 : Comparison of incoming and outgoing requests from/to foreign partners

5.2. Co-ordinating national and international investigations

In the frame of police data exchange CYCO undertook co-ordinating measures in 180 instances.

The type of support provided by CYCO and its role in investigative proceedings depends on the specific case and situation. CYCO performs a co-ordinating function particularly in international investigations where it acts as the national contact point for law enforcement agencies in Switzerland and abroad, and for agencies or individuals involved in investigative proceedings. In cases where the cantons are responsible, CYCO provides the competent agencies with its analytical, technical and legal expertise or with undercover investigators.

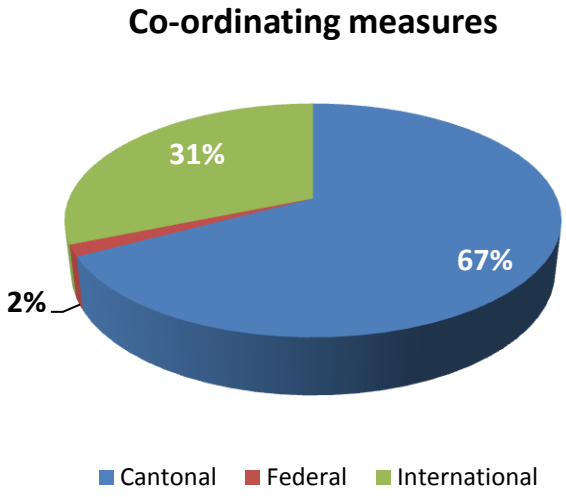


Figure 24: Relative comparison of CYCO's co-ordination measures

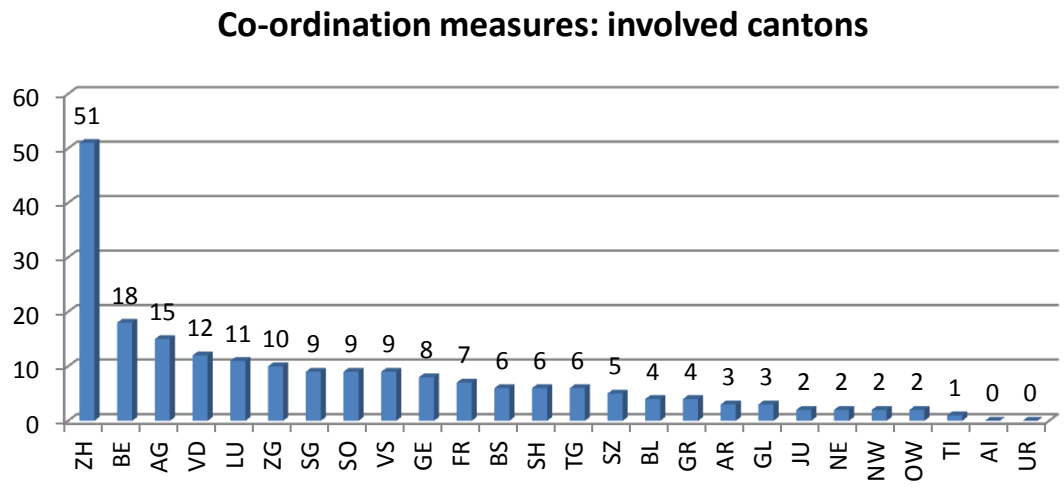


Figure 25 : Cantons affected by CYCO's co-ordination measures

Zurich was by far the most affected canton. Two reasons for this are apparent: on the one hand, Zurich is an economic centre and as such attracts many major national and international information and communication companies. On the other hand, the Canton's new Competence Centre for Cybercrime has created an ideal basis both for conducting cybercrime investigations and for making a significant contribution to international investigations.

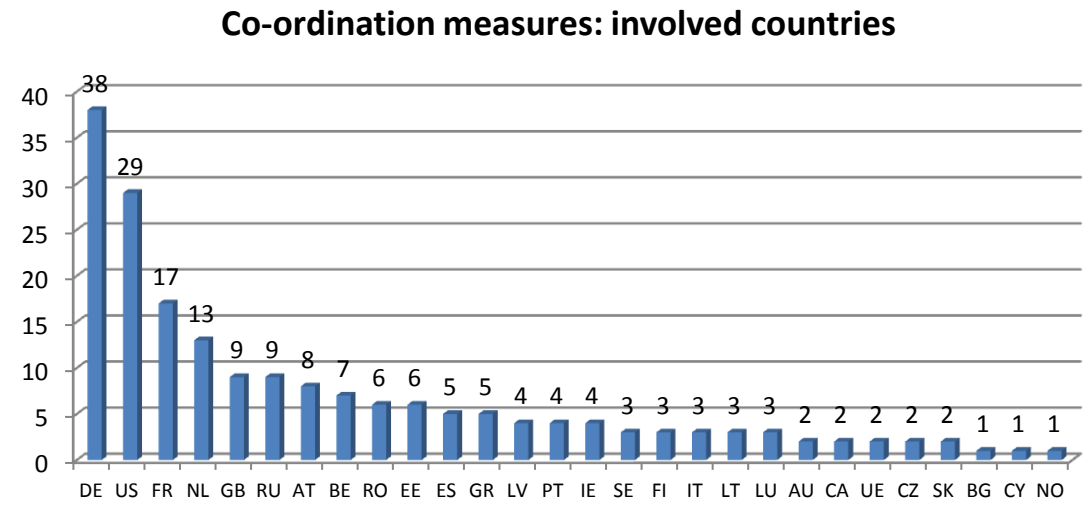


Figure 26: Countries affected by CYCO's co-ordination measures

In international investigations CYCO is the national contact and liaison between national and international parties to the proceedings, ensuring that Switzerland has a comprehensive overview of the respective case and data, and is in a position to take the appropriate measures if required.

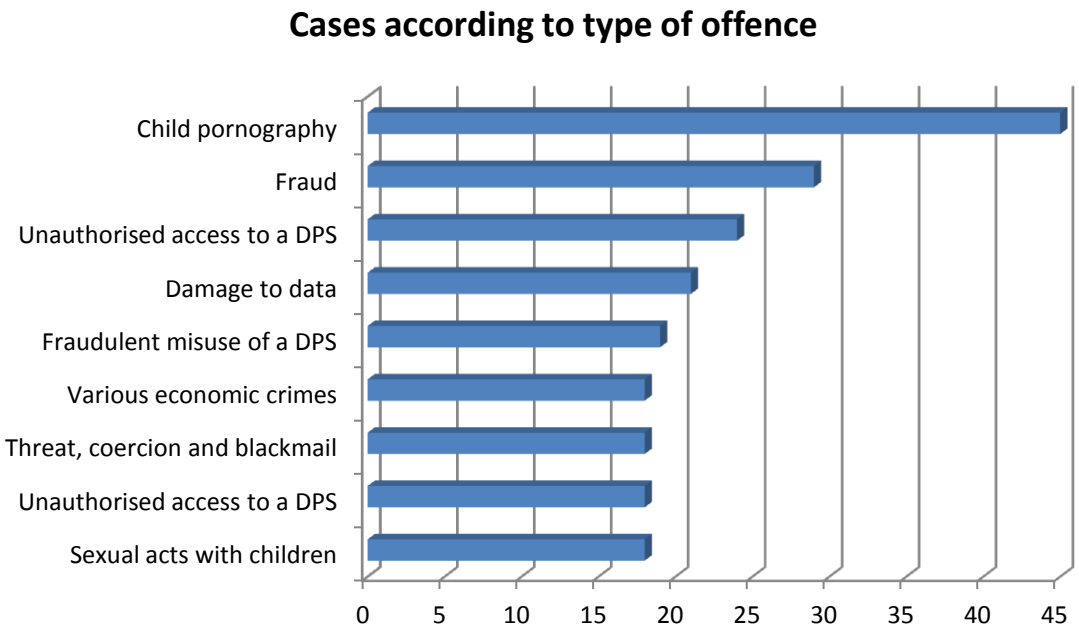


Figure 27 : Number of co-ordinated cases according to type of offence 2013

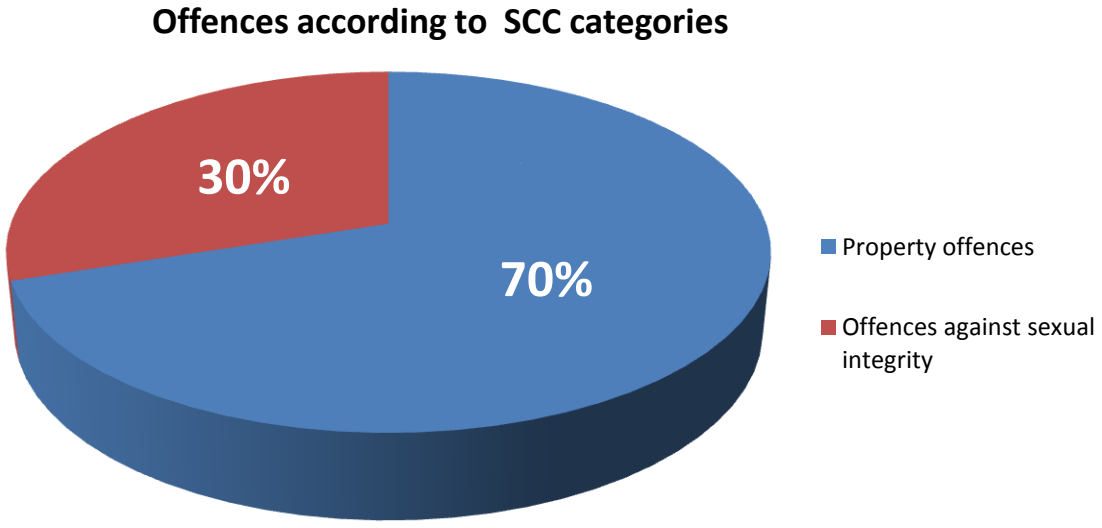
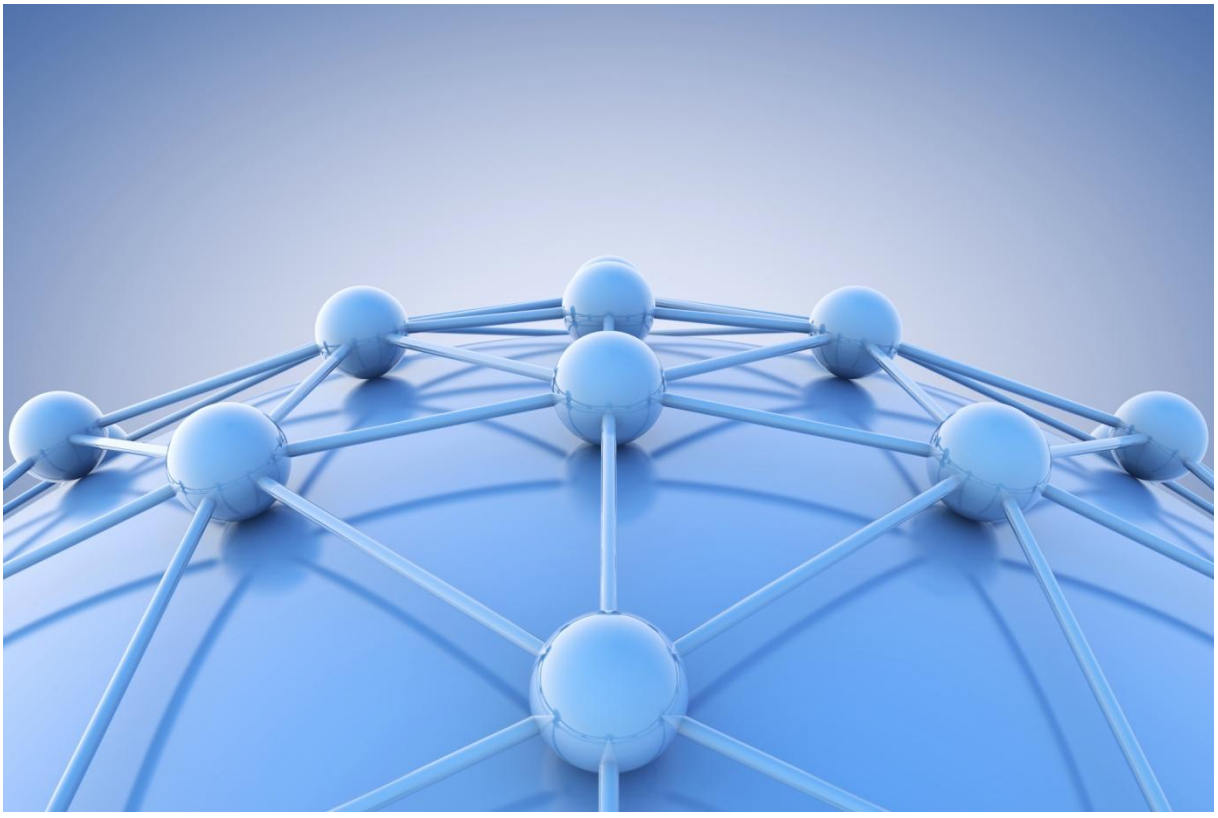


Figure 28 : Proportion of co-ordination measures according to type of offence 2013

5.3. Case studies

CYCO received a report from the Federal Criminal Office of Wiesbaden concerning the infiltration by unknown persons of the computer system of a large telecommunications service provider. The hackers had accessed stolen data via a server in Switzerland. Within hours CYCO contacted the Cybercrime Competence Centre in Zurich and secured the connection data and content under Article 29 of the Cybercrime Convention. A first analysis of the recovered data enabled investigators to track the hackers back to Germany. Two days later investigators carried out a further back-up and a new analysis of the server and discovered that the hackers had already tried to cover up their tracks and destroy most of the evidence. Had the data not been seized immediately (as had been the case), it would have been nearly impossible to identify the perpetrators.



In another occasion, CYCO was involved in co-ordinating an international request for mutual assistance relating to the take-down of the Liberty Reserve payment network by the United States Secret Service (USSS). CYCO was called in to co-ordinate matters between the Federal Office of Justice, the USSS, the Office of the Attorney General of Switzerland as well as the Swiss Federal Criminal Police. Prior to the take-down, CYCO had been requested by the USSS to contact the involved parties and to conduct preliminary inquiries, this because the time between receipt by the Federal Office of Justice of the request for assistance and execution would otherwise have been too short. Thanks to CYCO's co-ordination and liaison work, the parties concerned were able to focus on their core preparatory tasks and seize the server as had been requested.

6. Projects

6.1. National Strategy on Protecting Switzerland from Cyber Threat (NCS)

On 27th June 2012 the Federal Council approved the National Strategy on Protecting Switzerland from Cyber Threat (NCS), which aims to minimise cyber threat to private and public sectors, and to operators of critical infrastructures. The strategy identifies cyber threats primarily as being a part of existing processes and responsibilities and concludes that they should be addressed in existing risk management processes. The first step for those responsible for risk management processes is therefore to gather basic information on cyber threats and hence to strengthen their awareness of such threats.

For this purpose the Federal Council appointed the federal departments to start implementing the 16 NCS measures in collaboration with the cantonal authorities and the private sector. The said measures range from risk analysis on critical infrastructures to active participation in Internet governance at an international level.

Under Measure 6, an overview of (criminal) cases as comprehensive as possible is to be compiled and inter-cantonal case clusters are to be co-ordinated. The information gained from this overview and from the case clusters is to be incorporated into an all-inclusive situation report. The FDJP, in collaboration with the cantons, is then to submit a strategy paper to the Federal Council by the end of 2016. The paper is to clarify interfaces with other players involved in reducing the cyber threat, to co-ordinate situation analyses, and to define the resources and legislative amendments necessary at cantonal and federal level for implementing the strategy paper. The CYCO Steering Committee and the fedpol Directorate have appointed CYCO to co-ordinate and implement the NCS measures on behalf of fedpol. The head of the Federal Criminal Police is responsible for managing the project.

The next step is, together with the cantons, to compile a viable strategy, to establish an overview of national cases and to co-ordinate inter-cantonal case clusters. This particularly involves analysing organisational, technical, legal, resource-related (e.g. HR, infrastructure, IT, etc.) and subject-specific aspects. A detailed analysis of the mandate has been completed and the project organisation comprising representatives from fedpol, the CCJPD, the CCPCS, the CSLEA (Conference of Swiss Law Enforcement Agencies), the Swiss Police ICT, the Office of the Attorney General of Switzerland and the Federal Office of Justice has been defined. During 2014, the strategy paper is due to be submitted twice to the cantons and agencies involved for consultation.

6.2. CYCO goes Social Media

As national co-ordination unit for cybercrime control, CYCO must keep abreast of the latest Internet developments. Technical developments influence communications services and subsequently forms of media use. For example, CYCO has started receiving more CySARS on potentially criminal content or conduct relating to Facebook.

In view of this development, CYCO requested the Steering Committee to approve various measures aimed at improving its dialogue with the public. The Steering Committee decided that on the occasion of its tenth anniversary CYCO should participate in social media. On 22nd December 2013 it therefore opened a Twitter and a Facebook account[9]. Its profile is available in three languages.

[9] www.facebook.com/cybercrime.ch and Twitter @KOBIK_Schweiz

7. Working groups, partnerships and contacts

7.1. National File and Hash Value Collection (NFHVC)

The NFHVC has been in operation since October 2012 and is available to cantonal and municipal units. The NFHVC is an efficient tool on condition that a sufficient number of images are categorised and given corresponding hash values. This work is very time-consuming and, with CYCO's limited resources, can only be achieved with the assistance of the cantons.

7.2. National working groups

In 2013, CYCO was represented in the following working groups:

Together with the FCP's Paedophile Crime and Pornography Section, CYCO organised the annual meeting of the *Arbeitsgruppe Kindsmissbrauch* (Child Abuse Working Group). In collaboration with non government organisations, cantonal representatives and those of Swiss Crime Prevention, the Working Group focuses on current issues relating to and fighting child abuse.

As in previous years, CYCO was involved in the steering group (responsible for programme development) and in the support group (responsible for programme implementation) of the national programme *Jugendmedienschutz und Medienkompetenzen* (Media Literacy for Young People and Media Protection Programme). The programme aims to teach children and young people how to handle modern media in a safe, responsible and age-appropriate manner.

CYCO has represented fedpol in the Swiss Crime Prevention commission since 2011. The commission develops projects and tools for use in crime prevention in the cantons and evaluates their implementation.

CYCO continued to be involved in developing the Security and Confidence Action Plan *Sicherheit und Vertrauen*. Under the lead of the Federal Office of Communications (OFCOM), this action plan highlights measures to promote the public's safety and trust when using modern information and communication technologies.

7.3. Co-operation with other federal agencies

CYCO continued to co-operate closely with other federal agencies in fighting cybercrime. Within fedpol it works closely with the International Police Co-operation Division and with several sections of the Federal Criminal Police Division, namely the *Digital Crimes Investigations Section,* the *Undercover Investigations Section* and the *Paedophile Crime and Pornography Section.* CYCO has a particularly intensive working relationship with the latter on account of their common sphere of activity.

A number of cross-departmental contacts between federal agencies were expanded and further strengthened throughout 2013, notably with the Reporting and Analysis Centre for Information Assurance (MELANI), the International Mutual Assistance Division of the Federal Office of Justice (FOJ), the Federal Office of Information Tech-

nology Systems and Telecommunication (FOITT), the Federal Social Insurance Office (FSIO), the Federal Office of Communications (OFCOM), the Federal Commission against Racism (FCR), the Federal Customs Administration (FCA), the Swiss Alcohol Board (SAB), the Swiss Financial Market Supervisory Authority (FINMA), the Swiss Federal Institute of Intellectual Property (IIP) and the Federal Gaming Board (FGB).

7.4. Exchanging expertise with the cantons

CYCO maintained numerous contacts with representatives of various police forces and public prosecutors offices.

Of particular note is the co-operation and exchange of experience with the Competence Centre for Cybercrime of Canton Zurich, which came into operation in 2013. In various cases, the authorities of canton Zurich were able to prevent evidence from being destroyed on note of CYCO and to facilitate the institution of proceedings. This could only be achieved due to clearly defined scopes of responsibilities within police and prosecutor's office and due to appointing contact people at all involved parties.

Besides the usual exchanges of experience and expertise with the cantons, several other working meetings between the cantons and CYCO were held as part of undercover investigations (see Chapter 4) or the NFFHVC project (see Chapter 6.1).

In addition, the second *Cybercrime Forum for Public Prosecutors Offices and CYCO* took place on 19th November 2013. Experts from law enforcement bodies and scientific instances provided a practical insight into combating cybercrime at international level and gave an in-depth look into criminal proceedings on botnets, money laundering and online currencies. Participants were also informed by Europol representatives on the co-ordination work of the European Cybercrime Center (EC3) in The Hague, which has been in operation since January 2013. The enormous interest shown – around 100 public prosecutors took part – clearly illustrated the need for such a course. The participation of Councillor of States, Luc Recordon, National Councillor, Daniel Jositsch, and Professor for Criminal Law at the University of Zurich, Christian Schwarzenegger, in the panel discussion gave the public prosecutors the opportunity to discuss first hand practical problems with representatives from political and academic establishments.

7.5. Co-operation with NGOs

For several years CYCO has worked closely with the NGO[10] *Action Innocence Geneva (AIG)* in combating child pornography. Thanks to AIG's active support, a project monitoring P2P networks has been run successfully over the last few years. The co-operation with AIG is highly important because most of CYCO's Internet monitoring activities are only possible due to the software made available by this NGO. AIG also supports CYCO by developing various other projects intended for use in fighting paedophile crime.

10 Non-Governmental Organisation

The *Swiss Child Protection Foundation* and *ECPAT Switzerland* are two further organisations committed to the protection of children and to the prevention of violence against them on the Internet. Their regular meetings aim at harnessing synergies and harmonising child protection efforts.

Closer co-operation was also reached with *Pro Juventute* by inviting this organisation to the seminar of the Working Group on Child Abuse.

7.6. Co-operation with Swiss Internet Service Providers

Since 2007, CYCO has assisted major Internet service providers in taking down foreign websites containing child pornography (as defined under Art. 197 para. 3 SCC). CYCO sends ISPs a regularly updated list of websites containing such material (the current list contains around 300 web pages). Access to web pages on this list is blocked by the ISPs based on corporate ethics and the companies' general terms and conditions. The user is then redirected to a "Stop" page.

As part of this project, CYCO works closely with INTERPOL, whose blacklist of websites containing child pornography is supplemented by CYCO's regularly updated list. INTERPOL's list is compiled in collaboration with various international police agencies.

7.7. International co-operation

CYCO has been a member of Europol's "CYBORG" Focal Point (FP) since 2011. The FP's aim is to combat cross-border cybercrime, with a focus on phishing, botnets and hacking. In the same year CYCO also joined the "TWINS" FP aimed at combating paedophile crime. Both Focal Points are incorporated into the European Cybercrime Center (EC3), which became operative on 1st January 2013.

EC3, based at Europol in The Hague, aims at supporting the EU member states operationally and at providing expertise to joint investigations at EU level. CYCO maintains close contacts with EC3 and has already made an active contribution to several operations. For example, three members of CYCO spent several weeks at EC3 in The Hague during summer 2013 and participated in a successful operation against paedophile offenders in anonymous networks. During the operation, the activities of 25,000 online paedophile criminals were halted, and two million pictures and videos were seized.

Since the 2013 reporting year, CYCO has represented Switzerland in the European Union Cybercrime Task Force (EUCTF) established in 2010 and made up of representatives from Europol, Eurojust and the European Commission. This group of experts, together with the heads of European cybercrime units, aims at facilitating and optimising the fight against cybercrime within the EU. The EUCTF promotes a harmonised EU strategy for fighting online crime and the problems that arise from using cyber technology to commit crimes. The EU has also prioritised the fight against cybercrime within the European Multidisciplinary Platform against Criminal Threats (EMPACT), selecting cybercrime as one of the eight focal points of the platform. CYCO actively follows EU efforts in fighting cybercrime and represents Switzerland's interests in discussions.

CYCO is also involved in the CIRCAMP project. The project was initiated by the European Chief of Police Task Force (EPCTF) and fights the distribution of child pornography on the Internet. As in previous years, CYCO was in contact with the European Financial Coalition (EFC) again in 2013. The EFC, co-funded by the EU, is made up of major players from law enforcement and the private sector who share the common goal of combating the commercial sexual exploitation of children on the Internet.

A similar goal is pursued by the Global Alliance against Child Sexual Abuse Online, which Switzerland joined on 6th December 2012 in Brussels. On signing the alliance, Federal Councillor Simonetta Sommaruga emphasised that Switzerland placed great importance on international co-operation in fighting paedophile crime and that co-operation should be further strengthened. One of the milestones of co-operation with the Global Alliance concerns Switzerland's membership of the Virtual Global Taskforce (VGT), an international partnership between law enforcement agencies, NGOs and the private sector for the protection of children from online child abuse. The VGT aims to make the Internet safer, to identify abuse, to locate and help children in need, and to ensure that offenders are brought to justice. The VGT currently has 12 full members and various partners (see www.virtualglobaltaskforce.com). Switzerland's application for membership was unanimously approved by the Board of Directors in 2013, and CYCO will be participating as a new member in the next VGT meeting in Brussels in May 2014.

8. Media presence, training and conferences

8.1. Media presence

Reports on CYCO's activities appeared in numerous media reports throughout 2013. Its alerts on specific cases of Internet crime were also brought to the attention of the media. One particular event worth mentioning was CYCO's participation in the programme "Chronik eines Missbrauchs" (Chronicle of Abuse), which was broadcasted as part of Swiss television's documentary series entitled "Schweizer Verbrechen im Visier" (Swiss Crime in Focus).

8.2. Social media

There has been a positive response by Facebook and Twitter users to CYCO's new social media profiles www.facebook.com/cybercrime.ch and @KOBIK_Schweiz.

8.3. Training and conferences

CYCO participated in various conferences, international congresses and training courses during the course of 2013, benefiting from the opportunity to cultivate contacts with partners and experts.

Also, CYCO participated in over 50 events either as instructors or as discussion partners in open forums, such as the Swiss Police Institute's workshops on international co-operation in the field of cybercrime, or the talks on the cybercrime underground economy held at the training courses by IT investigators from the northwest of Switzerland.

9. Political initiatives at federal level

9.1. Parliamentary initiatives

Interpellation 13.3229: Cyberwar and Cybercrime. How big is the thread and with which measures is it addressed? - Recordon Luc, 22.3.2013

Interpellation 13.3986: Enquiries in Social Media. Why does Switzerland receive that little information? - Vogler Karl, 27.9.2013

Motion 13.3490: Competence center for ICT security. - Guhl Bernhard, 19.6.2013

Question 13.5380: Insufficient Tools for Combating Cybercrime – Maximilian Reimann, 18.9.2013

Question 13.5356: Ordering Narcotics on the Silk Road Website - Andrea Martina Geissbühler, 16.9.2013

Question 13.5321: Is the NSA also Conducting Industrial Espionage in Switzerland? – Susanne Leutenegger Oberholzer, 11. 9.2013

Question 13.5281: US Secret Service Activities in Switzerland – Daniel Vischer, 12.6.2013

Question 13.5059: Culpability of Hosting Providers, and Blog and Forum Operators - Balthasar Glättli, 6.3.2013

Question 13.5224: The Presence of US Secret Services and their Cyber Espionage in Switzerland – Maximilian Reimann, 10.6.2013

Interpellation 13.4077: Data Espionage and Internet Security - Raymond Clottu, 5.12.2013

Parliamentary Initiative 13.442: Trawling Minors - Commission for Legal Affairs, 15.8.2013

Postulate 13.3707: Integral Cyber Space Strategy for the Future- Bernhard Guhl, 17.9.2013

Interpellation 13.3773 : Telecommunications Legislation for the Future – A Global Strategy for Cyber Space - Groupe libéral-radical, 24.9.2013

Interpellation 13.3033 : How to Protect the Personal Data of Swiss Citizens Held by American Companies - Jean Christophe Schwaab; Groupe socialiste, 6.3.2013

Interpellation 13.3726: Identity Theft : A Vulnerability in Penal Law? Jean Christophe Schwaab; Groupe socialiste, 18.9.2013

Postulate 13.3678 : Evaluating the Risks of the Bitcoin - Jean Christophe Schwaab; Groupe socialiste, 11.9.2013

10. Trends and potential threats in 2014

Based on the reports received by CYCO, very few if any conclusions can be drawn as to future trends in cybercrime or regarding illegal Internet contents. The figures merely reflect reporting practice by the public. At best, trends can be identified with regard to society's perception of Internet crime. The following statements are based on CYCO's open-source monitoring and its interpretation of these sources, together with its own operative findings.

Increase in successful online fraud attempts

From the reports received by CYCO, it is apparent that over the years fraud attempts – or scams, as they are known – have become increasingly sophisticated in terms of visual appearance and orthography. This applies to nearly all kinds of attempted fraud, from phishing e-mails to fraudulent advertisements and replies on advertising platforms, to ransomware lock screens. And this trend is likely to continue. It will therefore become increasingly difficult for Internet users to identify such scams. Since many scams originate from countries in North and West Africa, and the scammers have a global network of "money mules"[11] and know how to exploit legal hurdles or loopholes in law enforcement to their own advantage, it is extremely difficult to prosecute this type of crime. For this reason, efforts must be focussed on prevention and getting the website operators to adopt better technical countermeasures against uploaded fraudulent content.

Growth of the cybercrime underground economy

A veritable underground economy has developed around all types of Internet crime over the last few years. Services such as the manufacture of malware, the distribution of spam, DDoS attacks and fake social media profiles – to name only a few – can be readily and anonymously be bought over the Internet using anonymous and virtual currency such as bitcoin or using exchange platforms. Popular too are the money transfer services of large international payment services providers which can be easily used in countries outside of Europe without the user having to disclose his true identity. Using these services renders tracking financial flows nearly impossible.

The economic situation in Europe is likely to facilitate an increase in the underground economy. Fighting this phenomenon with conventional methods is not effective. That is why the focus must be on undercover investigations in close co-operation with international partners and with the aim of compiling a global picture of this economy and identifying the main players. In specific terms, this means that it will be nearly impossible for individual cantons to prosecute perpetrators. Rather, it will require a co-ordinated effort based on a Swiss-wide overview of cases as foreseen under Measure 6 of the National Strategy on Protecting Switzerland from Cyber Threat. Proceedings could be conducted by joint working groups under the lead of one canton or the federal authorities.

[11] Financial agents involved in money laundering

Greater focus on small and medium-sized businesses (SMBs)

The amount of know-how available in the underground cyber economy and the propagation of application software probably mean that SMBs will increasingly become victims of data theft. SMBs are a lucrative target for cyber criminals because their data pool of e-mail addresses, passwords, contact information and postal addresses is extremely valuable to the underground cyber economy and their infrastructures are not as secure as big businesses such as major banks. It is also probable that the number of cases involving attempted blackmail using previously stolen data, DDoS attacks on the websites of smaller companies and, in particular, blackmail using so-called CryptoLockers will increase.

Stolen digital certificates

In the current reporting year, CYCO received several reports on the theft of digital certificates[12] from Certificate Authorities (CAs). The stolen certificates were then used by cyber criminals to sign malware with the aim of evading security mechanisms such as anti-virus programmes. This can unhinge a major cornerstone of Internet security, the Certificate Authorities' chain of trust. For end users this means that criminals could, under certain circumstances, secretly infiltrate connections to web servers (believed by users to be secure) and read, divert and modify data exchange for criminal purposes. The browser, however, would continue to indicate to the user that he is communicating with a server that has a legitimate signature. This could have serious consequences, for example for online banking, online shopping data transmission and other high-security applications.

More mobile malware expected

The shift in Internet access to mobile appliances could accelerate the number of malware variations on mobile phones, smart phones and tablets. The greater propagation of e-banking authentication mechanisms which require an additional appliance such as mobile phones or smart phones, means that the number of attacks on such systems using mobile malware may increase. The variety of devices, their different structures, the necessary know-how and the increase in experts subsequently required will pose in future a greater forensic and financial challenge to cantonal police corps with small IT-investigation departments.

[12] A digital certificate is a digital signature (containing a variety of identification information) issued by a Certificate Authority (CA) to verify that a user sending a message is who they claim to be and to provide the receiver with the means to encrypt a reply.

11. 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 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.
Peer-to-Peer	In a peer-to-peer network, members can access the same data and exchange data with third parties.
Hard Pornography	Sexual acts involving children (synonym: child pornography), animals or human excrement, or sexual acts involving violence (Art. 197 sec. 3 SCC).
Hash values	Clearly classifiable parameters of an image (digital fingerprint).
Phishing	Methods to acquire an Internet user's data (e.g. password, username, etc.) via fake websites.
Proxy	Communication interface between the client and a server in an IT network, via which, for example, a website can be accessed.
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	Transmission of audio or video files. Files are downloaded via a computer network onto a system, not in full but continuously. As a result, the full download 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).