Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Justice and Police FDJP

Federal Office of Police fedpol

March 2015

Annual Report 2014

Cybercrime Coordination Unit Switzerland CYCO

Federal Office of Police fedpol

Cybercrime Coordination Unit (CYCO)
Nussbaumstrasse 29
3003 Bern

www.kobik.ch
www.cybercrime.ch

Date of publication : 26 March 2015

Source of illustrations : Thinkstock / CYCO

Foreword

Christoph Neuhaus, Cantonal Councillor
Chairman of the CYCO Steering Committee

Panta rei – literally “everything flows” or “everything is constantly changing.” As usual, CYCO must keep looking ahead and continually adapting. *Confront the challenges, gather experience, analyse critically and continue improving*; this remains the supreme maxim.

In the spring, the German authorities informed CYCO about a major case of identity theft. Using e-mail addresses and the appropriate passwords, criminals tried to log onto e-mail accounts to misuse them for sending spam. CYCO reacted quickly and pragmatically, informing 38,000 users and the providers personally about the incident the following day. Reactions were positive, and CYCO proved how quickly it could react to unexpected situations.

CYCO works closely with INTERPOL, Europol, the FBI, the HSI and many other foreign agencies. Together with its partners – Swiss public prosecutors, cantonal police forces, representatives from the financial sector, Internet Service Providers, the Reporting and Analysis Centre for Information Assurance MELANI, SWITCH Internet Domains and NGOs – it also represents Switzerland in various international working groups. Other participants include Swiss Crime Prevention, the Federal Intelligence Service, the Federal Department of Foreign Affairs and other federal and cantonal agencies. To count on support, particularly in times of need, Switzerland must maintain personal contacts and friendships at international level, as former federal councillor, Adolf Ogi, always underlined.

This international co-operation includes fighting botnets as well as co-ordinating operations to arrest hackers. Equally important is CYCO’s membership in international committees concerned with fighting online paedophile crime or in alliances such as the Global Alliance. In this context, it is absolutely essential to build trust through good work; this will ensure that CYCO remains a valuable partner in the fight against cybercrime.

CYCO need not fear that it will have insufficient work or challenges in the future. Virtual bank robberies resulting in the loss of billions of Swiss francs, the seizure of record levels of child pornography, and the loss by Swiss SMBs of millions of Swiss francs through social engineering clearly illustrate that, with its 16 staff members, CYCO – whose funding comes two-thirds from the cantons and one-third from the Confederation – is working to full capacity. Moreover, CYCO is to submit its strategy for implementing Measure 6 of the National Strategy on Protecting Switzerland from Cyber Threat to the Federal Council by the end of 2016. Work on compiling a case overview and co-ordinating intercantonal case clusters is well underway.

CYCO is in demand; hardly a day goes by without a new and even bigger case of cybercrime hitting the headlines. Possibly one of CYCO’s biggest challenges is to provide decision makers with a general understanding of the far-reaching consequences of cybercrime. Cyber security requires a constructive framework and, ultimately, financial investment.

Table of contents

1 A brief overview

- In 2014, the Cybercrime Coordination Unit CYCO received 10,214 suspicious activity reports on cybercrime (CySARs) via the online reporting form. This represents an increase of 10.9% over the previous reporting year.
- The proportion of CySARs relating to *property offences* rose again in 2014, to 66.9% of total reporting volume. 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 50 crime reports to the competent national or international authorities as a result of the criminal relevance of the CySAR.
- By monitoring open and private peer-to-peer networks, CYCO identified 86 internet connections that were being used to share child pornography.
- As a result of its undercover investigations under the statutory provisions of Canton Schwyz and the Criminal Procedure Code, CYCO submitted 29 crime reports to the competent cantons and 281 crime reports to foreign law enforcement agencies for further action.
- More than 1,000 crime reports on criminally relevant websites were submitted to foreign authorities via INTERPOL, Europol or organisations working in related areas (e.g. Inhope).
- Work on implementing Measure 6 of the National Strategy on Protecting Switzerland from Cyber Threat continued throughout 2014.

2 Cybercrime Coordination Unit Switzerland CYCO

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 the content for criminal relevance. If there is an indication that a criminal offence has been committed, CYCO secures the necessary data and sends a crime report to the appropriate law enforcement agency in Switzerland or abroad.

Enquiries from the public are generally dealt with by CYCO. If this is not possible, CYCO will refer the person concerned to the competent agency or law enforcement authority.

2.1 Reporting volume

From 1 January to 31 December 2014, CYCO received a total of 10,214 CySARs via the online reporting form (www.cybercrime.ch). This is an increase of 10.9% over 2013 (9,208 CySARs).

The number of incoming CySARs does not allow any conclusions to be drawn on the true extent of cybercrime, nor on any trends with regard to an increase or decrease in the volume of illegal content on the web. It only reflects the public's awareness of and willingness to report suspicious content to the authorities.

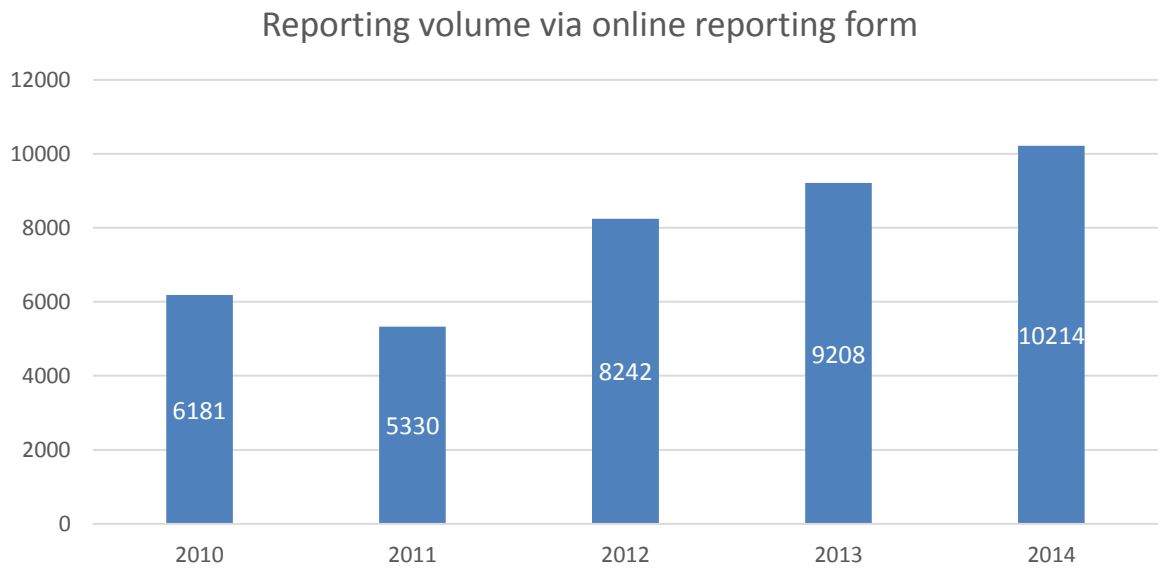

Figure 1: Five-year comparison of reporting volume via www.cybercrime.ch

On average CYCO received 851 CySARs each month. Like in the last two reporting years, there were fluctuations in May (1,024 CySARs), and at the end of September (837 CySAR) and beginning of October (680 CySARs). As in 2013, there was an increase in May and a corresponding decrease in September/October in the number of CySARs relating to phishing and attempted fraud. Due to the significant rise in CySARs on these two phenomena in May, CYCO accordingly published four crime alerts on social media sites and on CYCO's own website. One reason for the increase could be the fluctuation in spam and phishing email traffic intercepted by leading anti-virus software manufacturers and coinciding with the US summer holidays (end of May to end of August). However, it is not possible to say on the basis of the available data to what extent these factors actually influenced reporting volume.

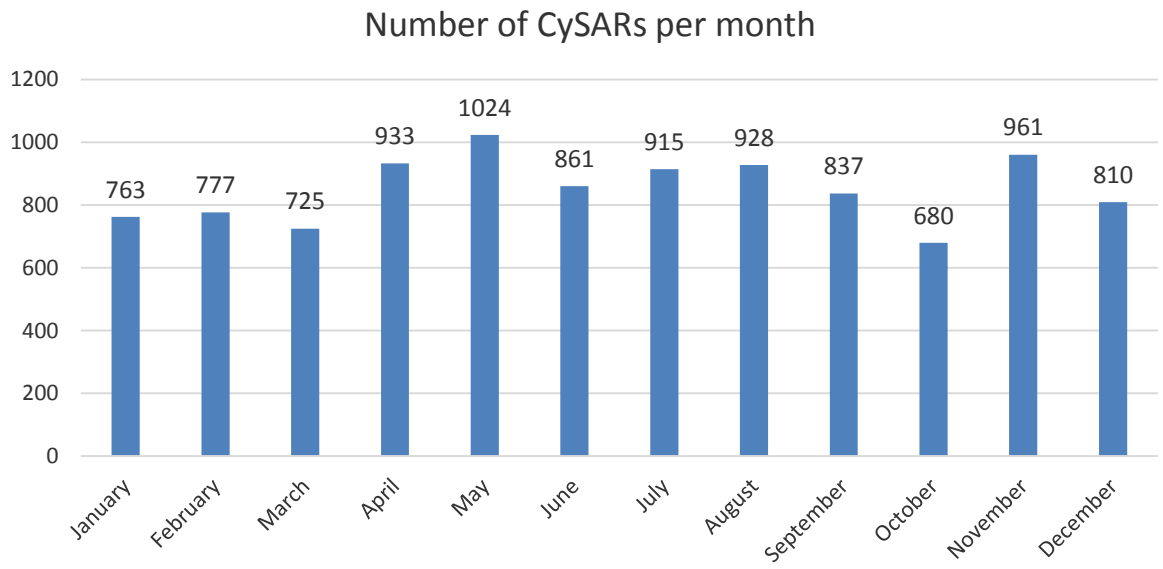

Figure 2: Reporting volume per month via www.cybercrime.ch 2014 (Total: 10,214 CySARs)

2.2 Subject matter of suspicious activity reports

The offences reported in the CySARs can generally be divided into two categories, whereby the boundary between the two is fluid. The first involves cybercrime in the strict sense (hereafter denoted “S”), i.e. criminal offences committed either by using internet technology or by exploiting vulnerabilities in the system such as hacking, Distributed-Denial-of-Service attacks (DDoS) or the production and circulation of malicious software (malware). These phenomena are made possible by the internet and are directed against internet technology. Cybercrime in the broader sense, on the other hand (hereafter denoted “B”), 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.

Approximately 87.7% of the CySARs received by CYCO in 2014 were criminally relevant. Of these, around 88.6% related to offences under the Swiss Criminal Code[1]. The remaining 11.4% related to violations against the Unfair Competition Act[2], the Copyright Act[3], the Trademark Protection Act[4], the Narcotics Act[5] and the Anti-Money Laundering Act[6] (see Chapter 2.2.3, Figure 9).

In 12.0% of the cases, CYCO found no criminally relevant matter following a preliminary investigation of the content. This figure includes general enquiries made to CYCO concerning no particular offence.

---

[1] Swiss Criminal Code (SCC) of 21 December 1937, SR 311.0

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

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

[4] Federal Act on the Protection of Trademarks and Indications of Source (TmPA) of 28 August 1992, SR 232.11

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

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

In cases where the subject matter did not relate to offences prosecuted *ex officio*, the complainant was referred to the competent cantonal police office.

The proportion of CySARs relating to *property offences* rose again in 2014, continuing the trend from the previous year. In 2014, 66.9% of total reporting volume (6,837 CySARs) involved this category of crime (Art. 137-172ter SCC). In second place, with 7.4% of total reporting volume (758 CySARs), were *offences against sexual integrity* (Art. 187-212 SCC). In comparison to the previous reporting period, reporting volume in this category fell drastically both in absolute and relative terms, from 1,842 CySARs in 2013 to 758 CySARs in 2014; a decrease of 58.8%. It should be noted at this point that under the amended Swiss Criminal Code, which took effect on 1 July 2014, possession and distribution of pornography involving excrement are no longer criminal offences (see Chapter 2.2.2).

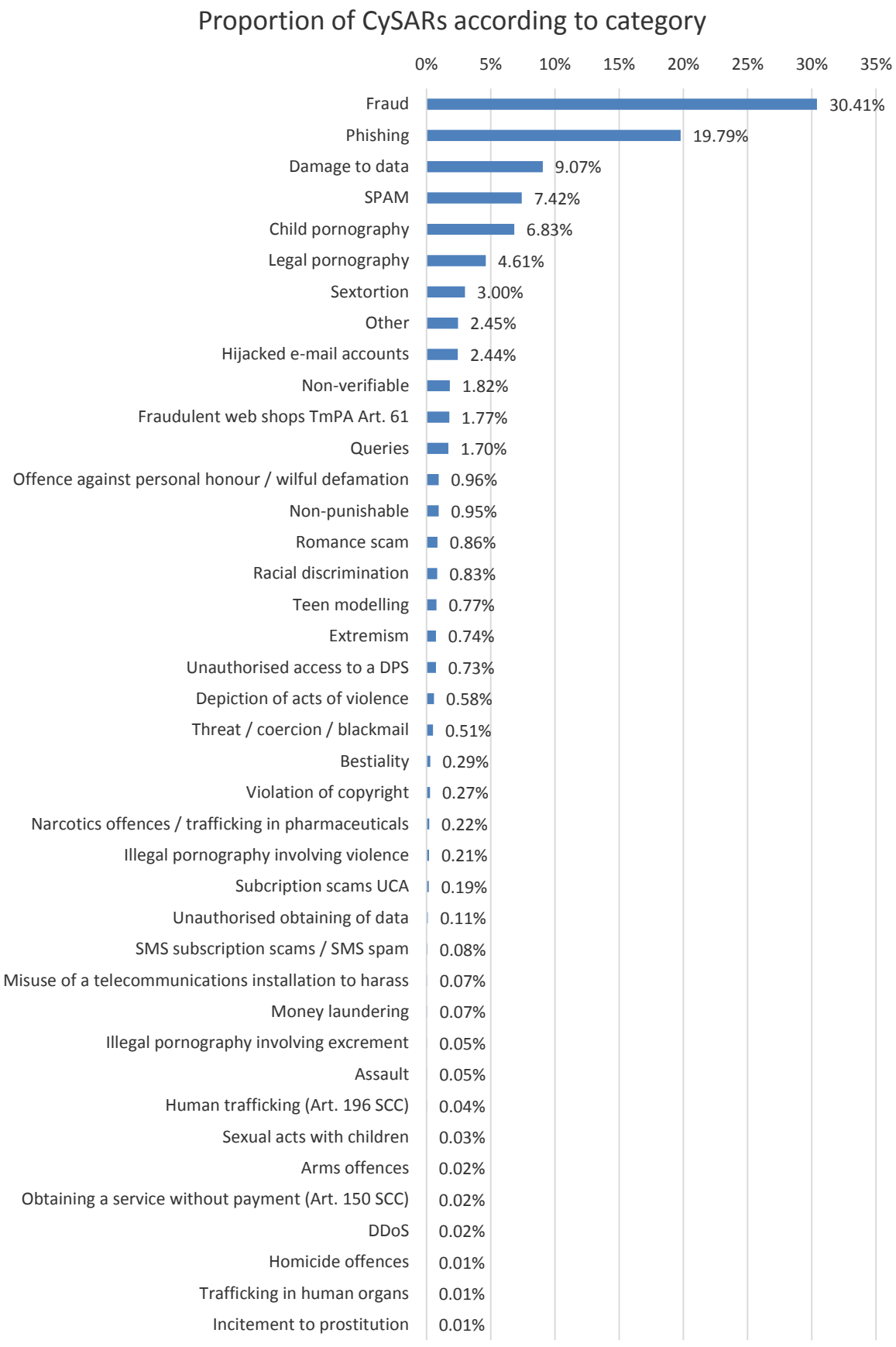

Figure 3: Proportion of CySARs according to category 2014 (Total: 10,214 CySARs)

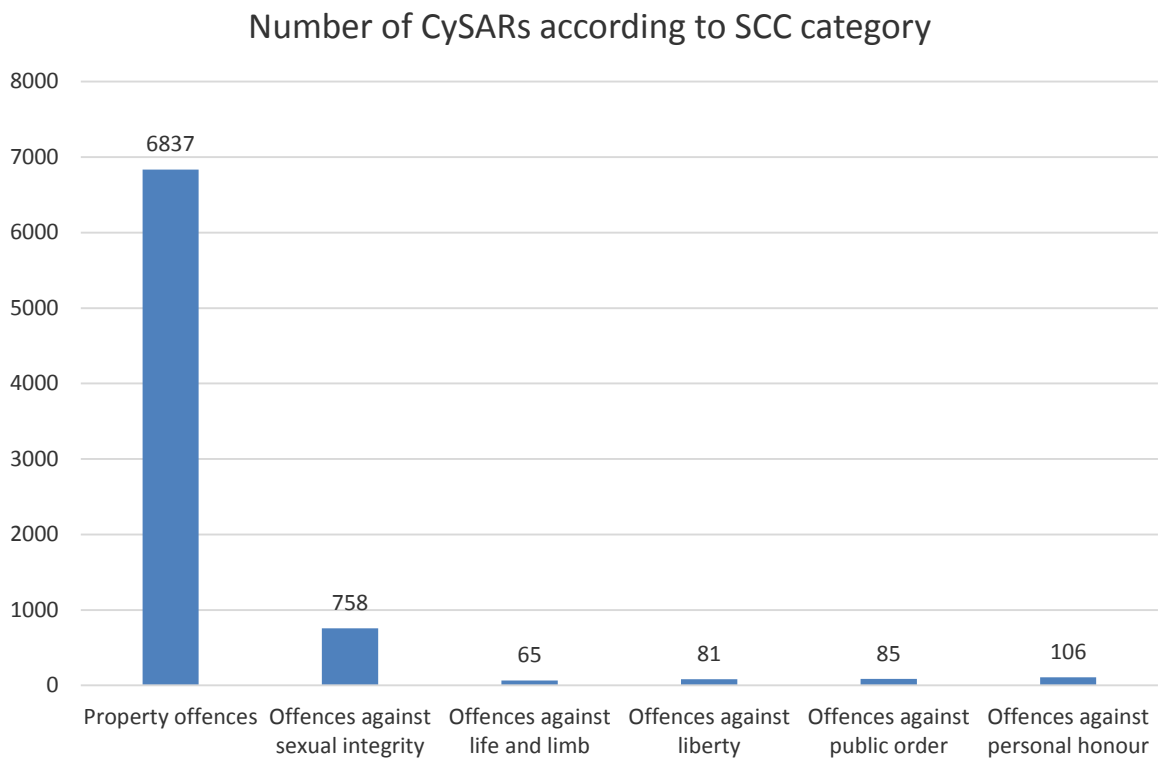

Figure 4: Number of CySARs according to category of the Swiss Criminal Code 2014 (Total: 7,932 CySARs)

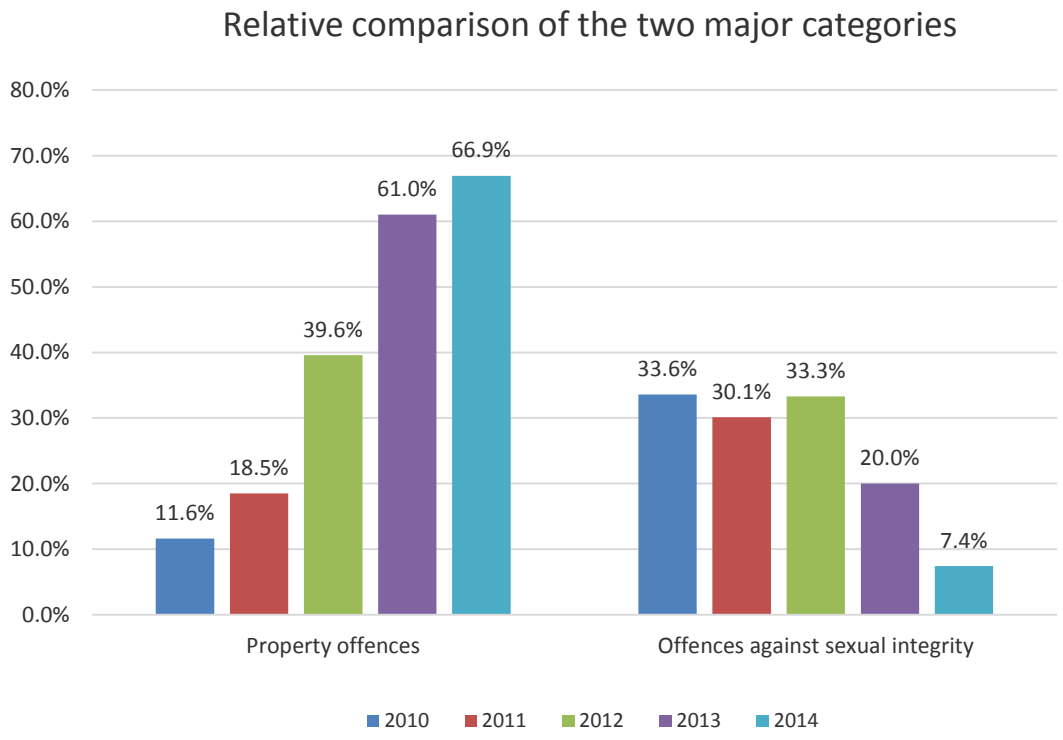

Figure 5: Relative comparison of the two major categories of CySARs 2010-2014

2.2.1 CySARs concerning property offences

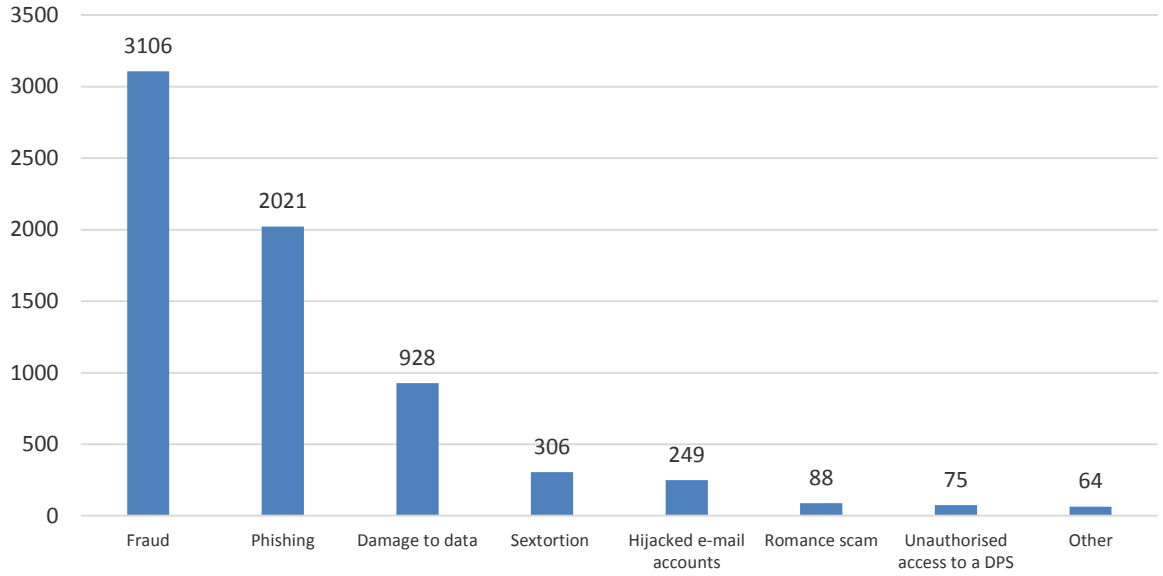

Figure 6: Number of CySARs concerning property offences 2014 (Total: 6,837 CySARs)

Most of the reports submitted to CYCO in 2014 (6,837 CySARs) concerned property offences. The increase correlates to the findings of independent sources such as quarterly reports by anti-virus software manufacturers or internet security researchers, which confirm that the volume of spam and phishing emails, and the number of malware viruses are continually on the increase worldwide. The various types of internet crime mentioned below are not exhaustive, but are representative of the phenomena reported to CYCO.

2.2.1.1 Attempted fraud (B)

With 30.4% of total reporting volume, *attempted fraud* made up the largest sub-category of property offences (3,106 CySARs) in 2014. There was no significant shift in modi operandi over the previous reporting period.

Once again, many of the reported fraud attempts concerned false advertisements on auction and classified advertising websites. Potential buyers were lured with cheap offers for premium products such as smartphones or special types of cars. The fraudsters aimed to dupe their victims into making advance payment without dispatching the supposed goods.

Another type of attempted fraud frequently reported to CYCO in 2014 was the fictitious real estate advertisement. Fraudsters attempted to exploit housing shortages in major Swiss conurbations such as Zurich and Basel by publishing advertisements for cheap but non-existent rental accommodation. On upfront payment of up to three months' rent, victims were promised that they could move into the property immediately or would receive a key to view the accommodation. The scam only came to light when the victims tried to view the property and realized the address did not exist.

Not only buyers, but also sellers fell victim to fraud. For example, fraudsters answered advertisements for home electronics and tried to convince the seller to dispatch the goods abroad, even offering more money than the advertised selling price. Fraudsters frequently claimed that the advertised product was not available abroad and that they were acting on behalf of a third party who was not residing in Switzerland and could therefore not make the purchase himself. Victims were persuaded to dispatch the goods but they never received payment. A variation

on this type of fraud was for the fraudster to persuade the seller to accept payment via an online payment service provider; the seller then received a forged confirmation of payment for the goods – often for a sum higher than the asking price – only then to receive an e-mail supposedly from the payment service provider requesting additional payment for fees, customs charges or delivery charges. To avert suspicion, the fraudster sent the seller e-mails assuring the seller that he, the supposed buyer, would assume all the additional costs. In reality, all the e-mails supposedly from the buyer and the payment service provider were from the fraudster. Naturally, the seller lost not only all the money he had paid supposedly for fees and extra charges, etc. but also the goods he intended to sell.

Small and medium-sized businesses were increasingly targeted by fraudsters who went to considerable lengths to obtain information on companies' payment methods, for example by collecting information on employees who had regular contact to fiduciaries or banks. Using stolen e-mail access data obtained by phishing to gather information on payment methods and outstanding invoices, the fraudsters then sent forged e-mails – supposedly from the company – to employees at the fiduciary or bank ordering payments to the fraudster's account. The scam can be extremely profitable; proceeds can range from a few hundred to several tens of thousands of Swiss francs. Based on reports by the cantonal police, the extent of damage in Switzerland in 2014 was estimated at several million Swiss francs (see Chapter 4).

2.2.1.2 Sextortion (B)

CYCO received the first reports on sextortion – a portmanteau from "sex" and "extortion" – in 2013. Most of complainants were men who claimed to have been targeted on social media or dating websites, supposedly by women. Following an initial written exchange, the perpetrator suggested continuing the exchange on an online video platform. Via webcam, the complainant was shown images of a woman undressing and indulging in sexual activities. Ultimately, the complainant was seduced into doing the same, not realising that the acts were being recorded. The images were subsequently used to extort money from the complainant under threat that they would be posted online if the sum demanded was not paid. The demands continued even when the complainant paid the sum requested, the amount successively rising.

2.2.1.3 Phishing (B/S)

With 19.8% of total reporting volume, there was a slight fall in the number of CySARs involving phishing (2014: 2,021, 2013: 2,208). This represents 8.9% fewer CySARs than in the previous reporting period.

Phishing describes a technique used by fraudsters to lure as many people as possible onto fake websites of well-known providers of online services by randomly sending a large number of e-mails to a wide audience. Once on the website, the victim is deceived into divulging personal data such as passwords or usernames. Online services that are especially lucrative for fraudsters include e-banking services, online payment services, auction and e-shopping sites, cloud service providers, music download sites and app stores for smartphones.

CySARs often involved cases of fraudsters misusing the server of a third person to host a phishing site. In some cases, fraudsters exploited security vulnerabilities, for example in out-dated versions of content management systems. Similarly, phishing e-mails were often sent by misusing web servers or by using botnets.

2.2.1.4 Police ransomware (S)

Police ransomware (from *ransom* and *malware*) is a malicious program that uses messages supposedly from a legal authority – often a police authority – to inform the user that their

computer has been blocked and to demand a sum of money (usually a few hundred Swiss francs) to unblock the system. The message requires the user to pay the ransom via an anonymous online payment service provider. The computer becomes infected when the user unwittingly opens an e-mail attachment or visits a website specially created for the purpose. Fraudsters do not target their victims, but send out the malware randomly in order to infect as many computers as possible, thus maximizing profits. In contrast to encryption Trojans (see below), it is relatively easy for a specialist to clean up an infected system and recover the data.

2.2.1.5 Crypto ransomware (S)

In the latter half of 2013, CYCO started receiving a growing number of reports on Trojans that were encrypting files and demanding a ransom to unblock the data. Like police ransomware, this type of malware is distributed in e-mail attachments and specially doctored websites. Once a computer becomes infected, the malware encrypts all the data on the computer's hard drive (e.g. Microsoft Office files, music or video files) rendering it inaccessible to the user. The user is required to pay a sum of money with virtual currency to have the files decrypted. However, not even paying the "ransom" guarantees decryption. Sometimes the files can be decrypted by an IT specialist with a considerable amount of time and at great cost; at worst, not even a specialist succeeds in retrieving the blocked data.

2.2.1.6 E-banking Trojans and keyloggers (S)

CYCO received numerous CySARs in 2014 on e-mails containing e-banking malware as an attachment. The e-mails were worded in such a way as to prompt recipients into opening the attachment and thus installing the malware onto their computer. For example, e-mails informed recipients that the attachment contained an unpaid invoice from a major mail-order company or a list of mobile telephone calls abroad. Once the malware had been installed, the sender was able to infiltrate e-banking sessions and change browser settings. While the sender of the malware was carrying out transactions, the unwitting user believed that updates or maintenance work was being carried out. Variations of the malware can also map keyboard entries and network traffic in order to steal usernames and passwords.

2.2.2 CySARs concerning offences against sexual integrity

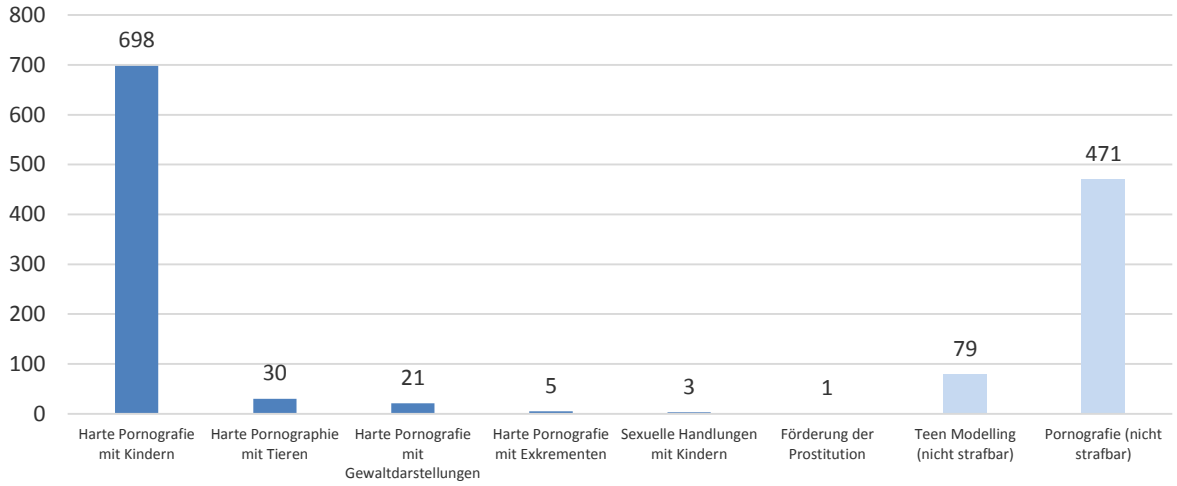

Figure 7: Number of CySARS concerning offences against sexual integrity 2014 (Total 758)

The number of reports concerning offences against sexual integrity fell significantly, from 1,842 in 2013 to 758 in 2014. This is a decrease of 58.8%. The number of reported websites containing child pornography also fell noticeably, from 1,414 websites in 2013 to 698 websites in 2014, a relative decrease of 50.6%. As already mentioned, possession and distribution of pornography involving excrement are no longer criminal offences under the amended Swiss Criminal Code, which took effect on 1 July 2014. Therefore, CySARs submitted after 1 July and relating to this offence were no longer criminally relevant.

CYCO received 79 CySARs relating to websites containing inappropriate images of teenagers ("teenage modelling"). Such images are not pornographic under the penal code and are therefore not criminally relevant. The pictures often show teenagers – usually girls – in provocative poses or in age-inappropriate clothing. Although these pictures do not constitute child pornography, many internet users perceive them as such and therefore report such content to CYCO.

In a further 471 cases CYCO was notified of suspected pornographic content that, following further investigation, turned out not to be criminally relevant. For example, the reports concerned websites that contained pornographic images with excrement (see above) or that depicted sexual practices, which the viewer found disturbing but which, in fact, were not criminally relevant. The cases were therefore not registered in the statistics on offences against sexual integrity.

The decline in the number of CySARs concerning offences against sexual integrity is due to two main factors. First, CYCO continues to work closely with internet service providers (ISPs) and INTERPOL in blocking websites containing illegal pornography. The Coordination Unit continually updates its list of websites blocked by ISPs and makes this list available to INTERPOL to supplement its own “worst websites” list (see Chapter 6.6). Cooperation between search engines such as Google or Microsoft with INTERPOL means that many such websites are no longer available in the engine’s search results. It is possible that as a result fewer people are confronted with such images and that the number of CySARs has fallen for this reason. CYCO’s close cooperation with ISPs and INTERPOL makes an important contribution to limiting the availability of illegal pornography online. This in turn helps to stop the ongoing abuse of the victims by preventing the repeated viewing of their abuse online. A second reason for the decline in CySARs on offences against sexual integrity might be linked to the trend identified since 2012 of sharing illegal pornographic images over anonymous areas of the internet (such as onion networks or anonymous I2P networks) or of offenders changing to private P2P networks (see Chapter 3.2).

2.2.3 Other criminal offences

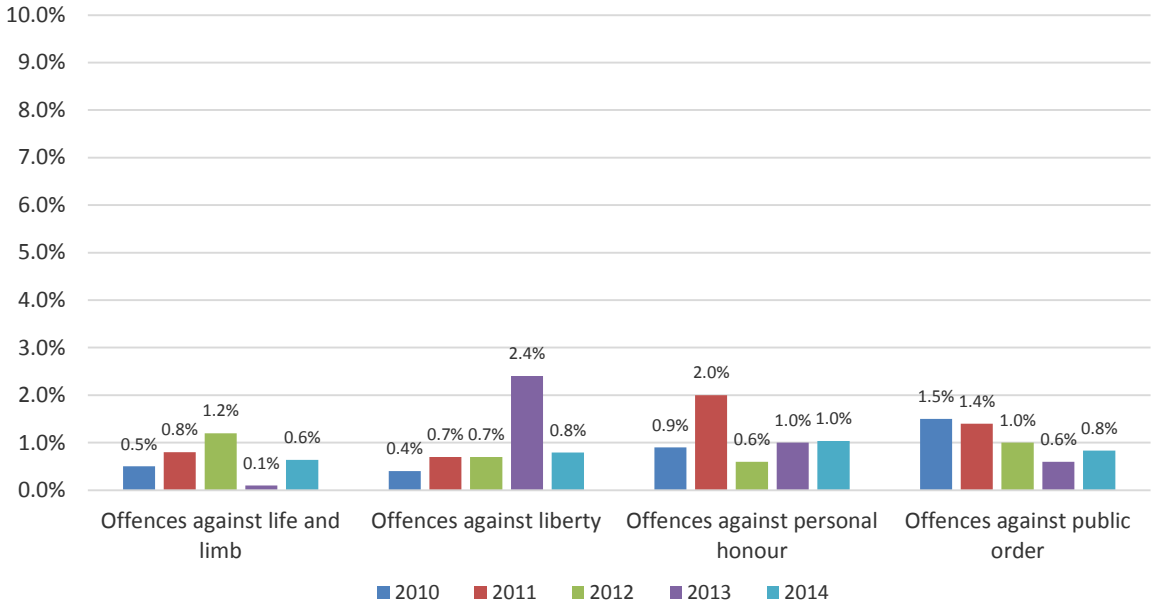

Figure 8: Relative comparison of other reported criminal offences under the Swiss Criminal Code 2010-2014

3.3% of the total reporting volume concerned offences against life and limb, liberty, public order and personal honour. CYCO received 85 CySARs concerning offences against public order; these primarily involved racist or extremist statements posted on social media websites. Although there was a slight increase in the number of CYSARs on these offences in absolute terms, the proportion of reports remained unchanged over the previous reporting period.

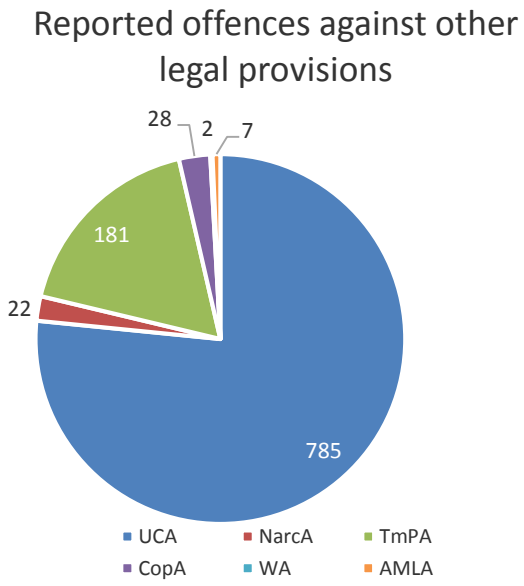

Figure 9: Absolute comparison of reported offences under other legal provisions 2014 (totalling 10% of overall reporting volume)

Approximately 10% of the CySARs concerned offences under other legal provisions, in particular the Unfair Competition Act. These CySARs related to mass advertising e-mails, i.e. spam.

CYCO received 181 CySARs concerning fraudulent web shops and product piracy on websites designed for selling counterfeits. These cases primarily involved web shops selling luxury items and brand products such as sports equipment, sunglasses, designer handbags etc. at discount prices. Customers who order products from these websites usually do not receive any goods at all or low-quality pirate copies. In 76 cases, the web shop was registered under a Swiss – *.ch* – domain name.

Having such web content removed from the internet is not easy outside the sphere of criminal proceedings. CYCO has to request the domain holder's valid Swiss address from the domain registration service SWITCH. If the domain holder does not respond to SWITCH's request for a valid address within 30 days (which is usually the case), the domain name is revoked under the provisions of SWITCH's general terms and conditions.

2.2.4 Summary

Continuing the trend of the last few years, the number of CySARs concerning property offences increased in 2014 once again, both in absolute and relative terms. Likewise in keeping with developments of past reporting years was the decline in the number of CySARs concerning offences against sexual integrity. The number of CySARs relating to other offences under the Swiss Criminal Code remained stable.

The cybercrime phenomena of 2014 were generally not new; most of them were consistent with the modi operandi identified in the last few years, be it in slightly modified form. However, CYCO did notice that the scams had become increasingly professional: the grammar and spelling in phishing attempts, and in false classified advertisement and fraudulent e-mails were of a higher standard, and the layout and design were of a better quality. This makes it increasingly difficult for users to distinguish between genuine and lookalike web content.

2.3 Facts and figures

When CYCO receives a CySAR several steps are involved in its processing; for example, analysing the incoming CySAR, deleting the content of the website reported, or forwarding the CySAR to the competent law enforcement agency for further action. Here is a summary of the most important facts and figures concerning the CySARs submitted to CYCO in 2014:

- All 10,214 CySARs were analysed with regard to their criminal relevance.
- In 3,218 of the 10,214 cases reported, the person submitting the CySAR received a personal reply from CYCO.
- CYCO sent 50 crime reports directly to the competent canton or authority on account of the criminal relevance of the CySAR.
- More than one thousand crime reports concerning criminally relevant websites were forwarded to our foreign partners via INTERPOL, Europol or organisations working in the same field such as Inhope.
- Numerous CySARs were forwarded to fedpol's Federal Criminal Police Division (General, Organised and Financial Crime Section, or the Paedophile Crime and Pornography Section), or to the Money Laundering Reporting Office Switzerland MROS.
- CYCO published 27 crime alerts on the most frequently reported crime phenomena. The alerts were published on its own website (www.cybercrime.ch), and on Facebook and Twitter. CYCO also notified its partners – Reporting and Analysis Centre for Information Assurance MELANI, Swiss Crime Prevention and the media – of the alerts, thus reaching large sections of the public.

2.4 Case studies

During 2014, CYCO was informed about a user of a well-known pornographic video platform who had published videos of guests at a public swimming pool on his user profile. The pictures, mostly of women, had obviously been taken without their knowledge. The camera frequently focused on the young women's breasts and rear parts, and the images were accompanied by captions that were defamatory and sexist. One of the victims notified the press, following which several other victims came forward and made a complaint to the competent cantonal police. With CYCO's assistance, the cantonal police with the help of the website operator managed to identify the owner of the profile (who was also the person who had produced the images) and arrest him.

Reports of cybercrime from the public are an important tool in prevention. Based on these reports CYCO can publish crime alerts on its website and on social media platforms, thus alerting the public to potential acts of crime. One example of this occurred in April, when users of a particular social media platform informed CYCO that they had received an advertisement for a competition to win a car over the said platform. The advertisement claimed that the competition was organised by the French and Swiss agency of the car manufacturing company and that participants need only submit their telephone number. However, the advertisement was really a subscription scam; by submitting their telephone number, participants were unwittingly subscribing to a fee-based mobile service. Within one hour of receiving the complaint via its online reporting form, CYCO published a crime alert on social media sites; several national and international press agencies as well as Swiss Crime Prevention picked up on the alert and broadcasted it further.

3 Monitoring

The CYCO Steering Committee redefines the monitoring priorities for CYCO each year. As in previous years, the priority for 2014 was combating paedophile crime on the internet. However, in view of the rapidly rising number of reports on economic crime since 2012, the Steering Committee decided that CYCO should also continue monitoring this area of crime. In practice, this means that CYCO ensures the exchange of information in operations involving national and international agencies (see Chapter 4).

As a result of CYCO's monitoring of the internet, 396 crime reports were submitted to law enforcement authorities in Switzerland and abroad. This is a decrease of 6.4% over the previous year.

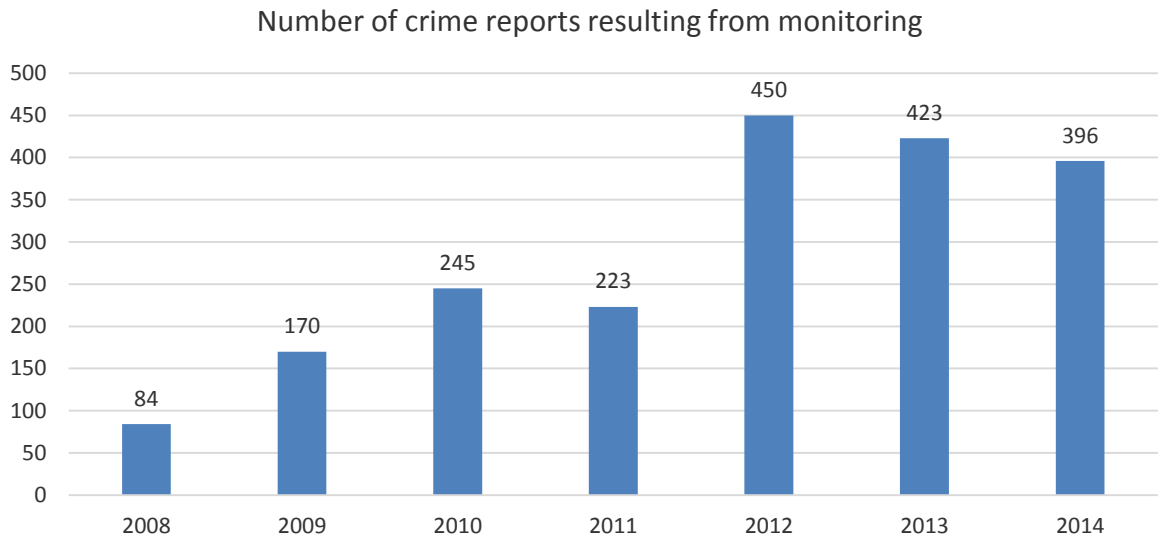

Figure 10: Number of crime reports from active monitoring of the internet 2008–2014

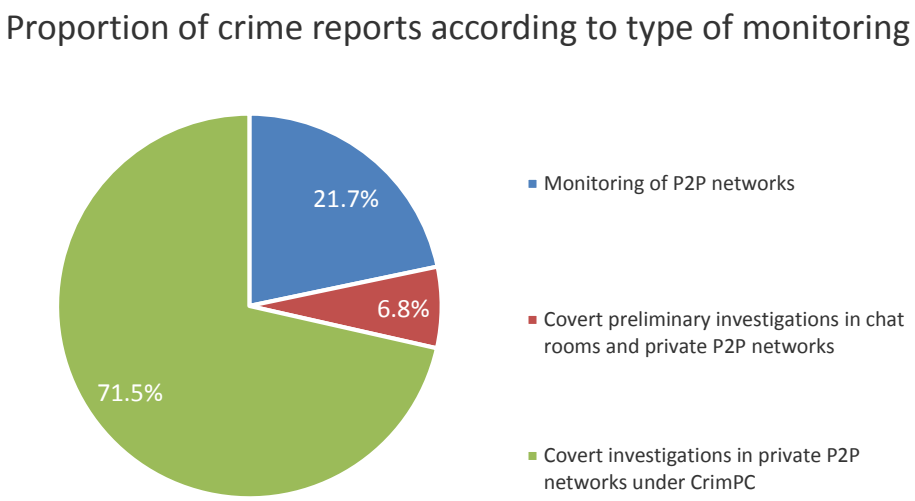

Figure 91: Proportion of crime reports according to type of monitoring 2014 (Total 396)

3.1 Monitoring peer-to-peer networks

Of the 396 crime reports submitted to domestic and foreign law enforcement authorities, 86 resulted from monitoring open peer-to-peer networks (P2P). This is a notable decline over the previous year (2013: 238). One of the reasons for the decrease in crime reports from this type of monitoring is that the number of open P2P network users has also been declining in recent years; instead of using open networks, users have gradually shifted their activities to hidden areas of the internet such as private P2P networks or to deep web and the Darknet[7].

The crime reports concerned internet users who were repeatedly exchanging child pornography (Art. 197 para. 4 or 5 SCC). Although CYCO specifically monitors users in Switzerland, it also registered a US national and sent its findings via INTERPOL to the competent agency abroad.

3.2 Undercover preliminary 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 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 undercover preliminary investigations explicitly by order and under the supervision of the police of Canton Schwyz. This ensures the continuity of preventive monitoring of online paedophile activity and the centralised coordination of efforts by individual cantons in this field.

As a result of CYCO's undercover preliminary investigations, 26 crime reports were sent to the competent cantonal authorities and one crime report to foreign law enforcement agencies. Two crime reports were a result of undercover investigations in chat rooms exclusively reserved for children. In a further case, CYCO sent a crime report to the competent authority after a user switched on a webcam and involved the undercover agent (who was posing as an underage girl) in his sexual activities. All three cases were submitted under Article 187 of the Swiss Criminal Code (attempted sexual activities with a minor). The low number of investigations by CYCO in children's chat rooms can be explained by the fact that most cantons now have their own statutory provisions allowing the cantonal authorities to conduct their own investigations in such chat rooms. By providing the cantonal police with a central platform for planning national operations and exchanging information, CYCO ensures that chat rooms are not simultaneously monitored by multiple cantons. Thus, an instrument has been created that provides ongoing nationwide monitoring of the internet by the cantons. The level of these undercover operations, which are focused on cases concerning Switzerland, depends however on the resources of the cantons.

Since more and more cantons are conducting their own monitoring of chat rooms, CYCO was able to concentrate its resources on undercover investigations in private P2P communities and on the Darknet. These operations must be centralized because, initially, it is uncertain where the victim and the offender are located and criminal jurisdiction is therefore unclear. From an ethical standpoint it is essential that such investigations are carried in the sense of emergency

[7] This term was originally used to refer to a virtual private network in which users only connected to people they trusted. Nowadays, the term "Darknet" more broadly refers to the part of the Internet that is invisible (deep web). It is mainly comprised of webpages that are not indexed by search engines.

[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).

intervention. Once victim and offender have been identified and located, the case can be forwarded to the competent authorities. CYCO therefore performs these undercover operations on behalf of the cantons.

The remaining 24 crime reports resulted from undercover investigations of closed-source P2P file-sharing applications. In contrast to classic P2P networks, data is not shared on an open network but encrypted and shared directly between computers. Undercover agents are therefore required to initiate contact with the users. Most of the crime reports resulting from these investigations are based on the possession and distribution of illegal pornography (Art. 197 para. 4 or 5 SCC after, and Art. 197 no. 3 or 3bis SCC before the entry-into-force of the amended provisions on 1 July 2014).

3.3 Undercover investigations under the Criminal Procedure Code

As in the previous year, CYCO was instructed by cantonal public prosecutors' offices to conduct undercover investigations in cantonal proceedings under the Criminal Procedure Code (CrimPC). The investigations in private P2P file-sharing communities were carried out under Article 285a et seq. CrimPC and were a result of criminal proceedings that had been initiated following monitoring of the internet under the statutory provisions of Canton Schwyz, during the course of which further cases came to light. The investigations resulted in 283 crime reports being sent to the competent police authorities.

The software used in private P2P communities enables two computers to establish a direct connection for exchanging data regardless of the location of the user. This technical feature renders it difficult to focus investigations on Swiss users only. During the investigations, CYCO managed to identify three Swiss users; the remaining 280 crime reports together with the incriminating evidence were forwarded to the competent law enforcement authorities abroad as part of international cooperation. By systematically processing evidence from Swiss cases regardless of where victims and offenders are, CYCO is fulfilling on behalf of the cantons Switzerland's obligations under the Global Alliance to act in solidarity to prosecute online child abuse. This relieves the cantons of the burden of employing resources to process cases involving offenders who are ultimately prosecuted abroad.

3.4 Feedback from the cantons

To gain an overview of the action taken by the cantons, CYCO requests updates on the progress of the case (e.g. on what police measures have been taken and the outcome of court proceedings).

The following data comprises feedback from the cantons in 2014 but concerns cases based on investigations from 2013. The reason for this is that CYCO only receives feedback from the cantons once the criminal proceedings have been concluded and the judgment has become final.

3.4.1 Feedback from the cantonal police

The feedback received so far from the cantons revealed that, for the first time CYCO started its undercover investigations, a house search had been carried out for every crime report submitted by CYCO. However, since not all feedback forms have been received for the 2013/2014 period, this figure is not final. The high rate of house searches according to the current figures does show, however, that the cantonal police take CYCO's crime reports seriously and treat them with a high level of priority.

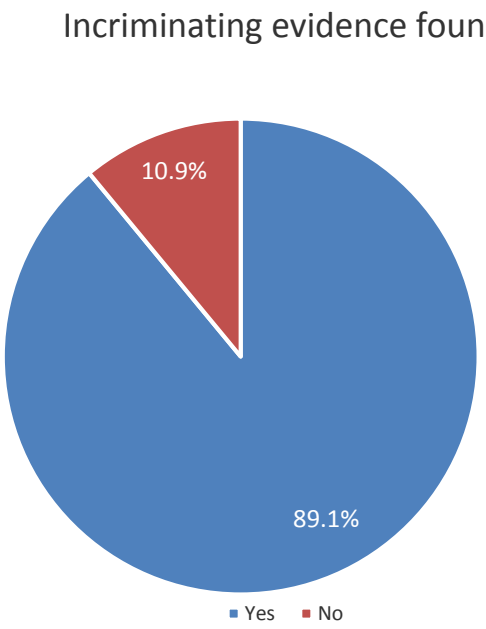

Figure 102: Incriminating evidence found during house searches 2014

Police found incriminating evidence in 89.1% of all house searches carried out as a result of CYCO's crime reports. Where a house search did not turn up any incriminating evidence it is difficult to pinpoint the reasons: unencrypted and therefore unprotected wireless networks often make it difficult to clearly identify offenders. Compact storage media make it increasingly easier for offenders to hide incriminating evidence. Also, offenders are making greater use of encrypted media, which makes it difficult for law enforcement to prove that a person is in possession of and exchanging unlawful material.

In 93% of the cases where incriminating evidence was seized, the material related to child pornography. This high figure is not surprising since CYCO searches open and private 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 59.1% of the house searches, the police identified further offences relating to illegal pornography as defined by Article 197 SCC.

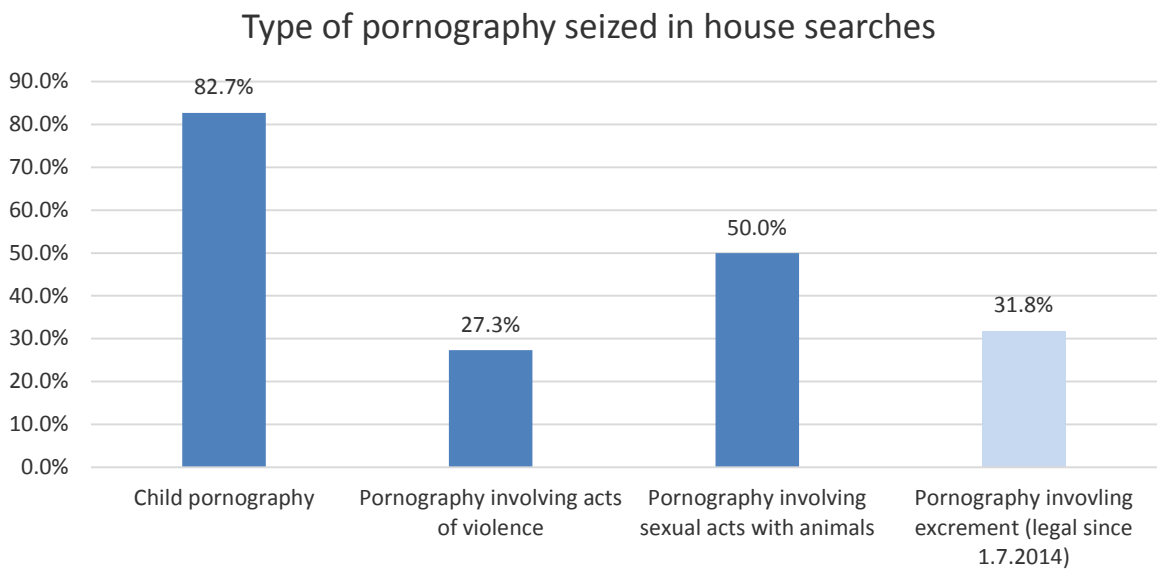

Figure 113: Type of pornography seized during house searches 2014

Feedback from the cantonal police also revealed that video files were seized in 57.1% and picture files in 59.2% of all house searches. In 6.1% of the house searches police also seized other incriminating material. In total, the house searches led to the seizure of nearly 700,000 illegal picture and video files.

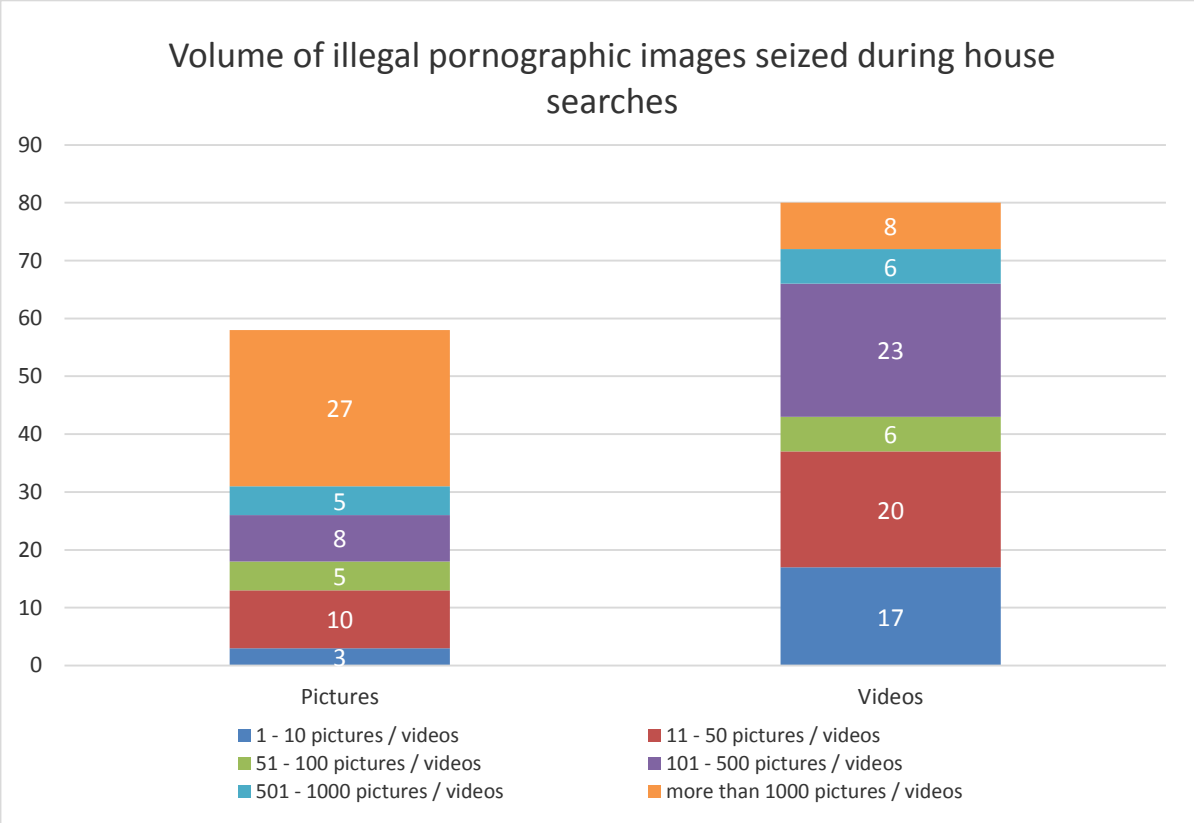

Figure 124: Volume of illegal pornographic images seized during house searches 2014. The diagram shows in how many cases (number listed) what volume (colour) of incriminating material was found.

3.4.2 Feedback from the cantonal judiciary

In 89.5% of the cases in which the cantonal judiciary provided CYCO with feedback, criminal proceedings had led to a conviction.

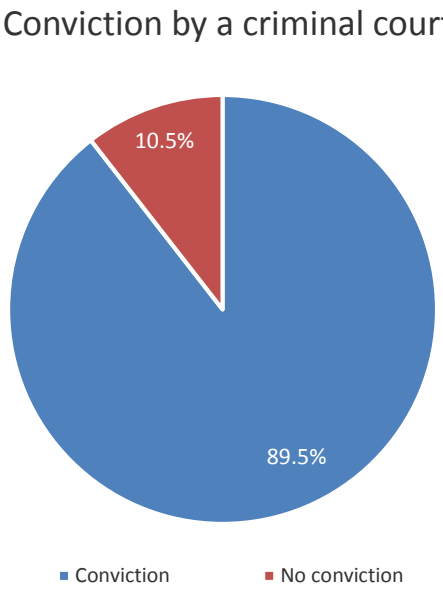

Figure 135: Proportion of convictions either through a criminal court or based on a summary penalty order 2014

Most convictions were for the possession of illegal pornography, in particular for the acts defined under Article 197 SCC (paragraphs 3 and 3bis before amendment of the act and paragraphs 4 and 5 since 1 July 2014).

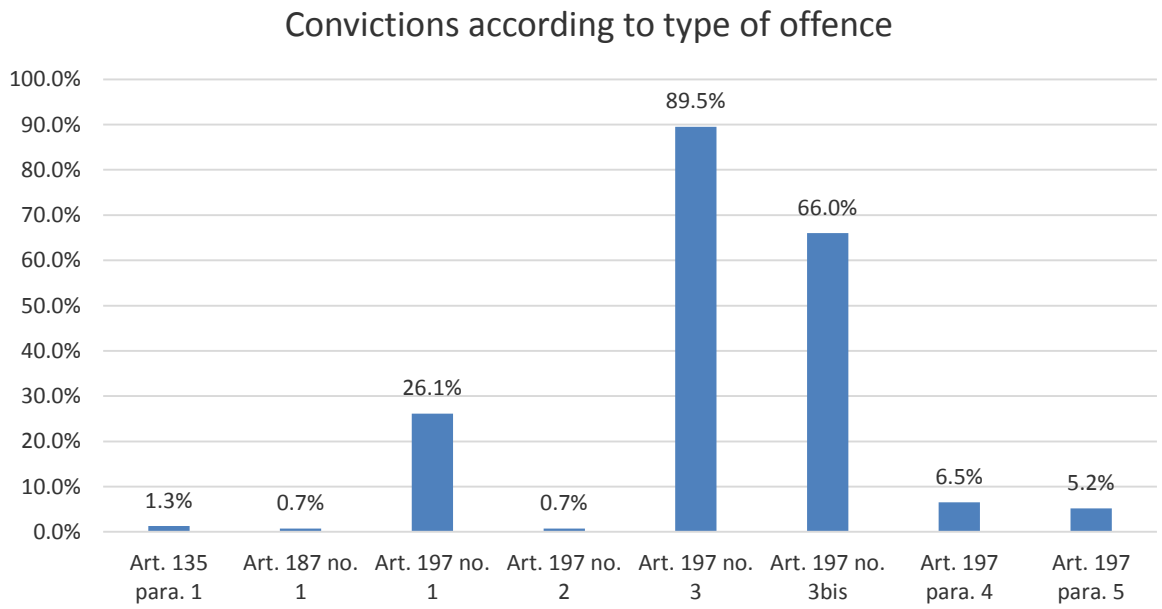

Figure 146: Relative comparison of convictions according to type of offence 2014.

In 92.2% of the convictions reported to CYCO, 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 74.5% of these cases the offender also received a fine. In 9.3% of the convictions the monetary penalty was combined with probation. In 5.2% of the convictions, the offender was ordered to undergo therapy, was sentenced to perform community service, was given a custodial sentence or received a monetary penalty not combined with probation.

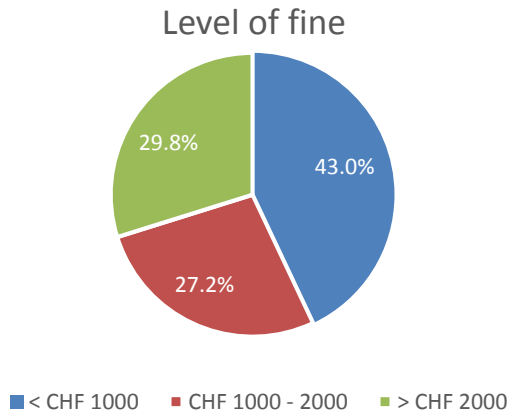

Figure 157: Amount and number of daily penalty units imposed 2014

In approximately 43% per cent of the convictions the fine amounted to less than CHF 1,000. In 27% of the convictions the offender was fined between CHF 1,000 and CHF 2,000. Only 30% of the fines were higher than CHF 2,000.

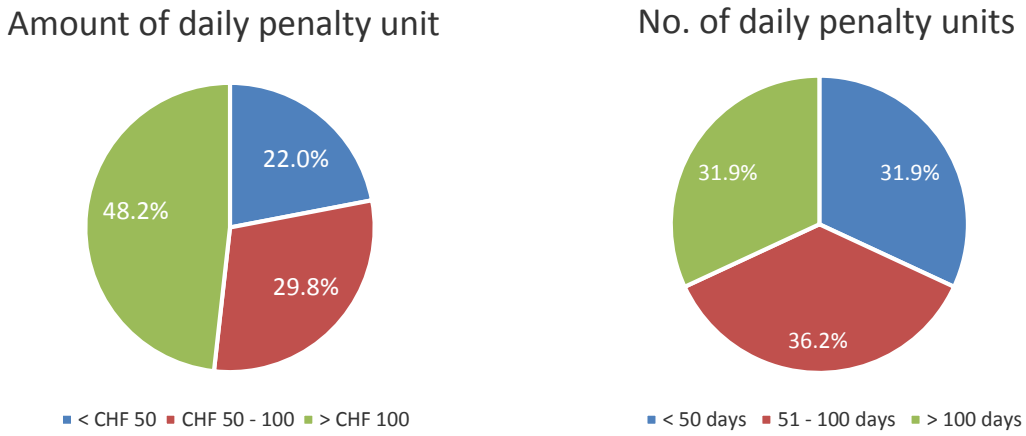

Figure 168: Amount and number of daily penalty units imposed 2014

Thirty-two per cent of the monetary penalties were fixed at 50 or less daily penalty units. In 36% of the convictions the monetary penalty was fixed at between 51 and 100 daily penalty units. In 32% of the convictions the monetary penalty was fixed at more than 100 daily penalty units.

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

3.5 Case studies

During monitoring of private file-sharing communities, CYCO's covert operations identified a user in Austria who granted CYCO's undercover agent access to his comprehensive collection of child pornography. The subsequent investigations revealed an internet connection in Austria from which the user was logging in to the file-sharing network. CYCO transferred the case to its Austrian partners, following which further investigations by the *Landeskriminalamt Steiermark* identified 51 further suspects from Sweden, Netherlands, Belgium, Denmark, Brazil and Iran.

In another case, a house search following a crime report submitted by CYCO to the competent cantonal police authority led to the seizure of child pornography. Since the accused was the husband of the child's day carer, the authorities of the commune involved informed the public about the case in a press release. Fortunately, the police investigations did not reveal any further cases of abuse despite the fact that the day carer had been looking after three other children since 2012.

4 Exchange of police data

4.1 Incoming and outgoing police requests

Since its incorporation into the Federal Criminal Police in 2009, CYCO has coordinated the international exchange of police information on internet crime, thus providing coordinative support to the cantons in their investigations. Since the entry into force of the Budapest Convention on Cybercrime on 1 January 2012, Switzerland has gained growing international recognition as an active partner in this field. To fulfil its mandate, CYCO has established a wide network of contacts in Switzerland and abroad. These contacts include stakeholders from both the private and public sector. Moreover, CYCO acts as interface between the cantons, INTERPOL and Europol in cybercrime matters. One of its most important partners is Europol's European Cybercrime Center (EC3).

In 2014 CYCO received 1,314 requests for information, which is an increase of 77.8% over the previous reporting period. Similarly, there was an increase of 35.8% in the number of requests for information CYCO made to foreign law enforcement agencies, from 946 in 2013 to 1,285 in 2014. These figures include the exchange of information with both national and international agencies.

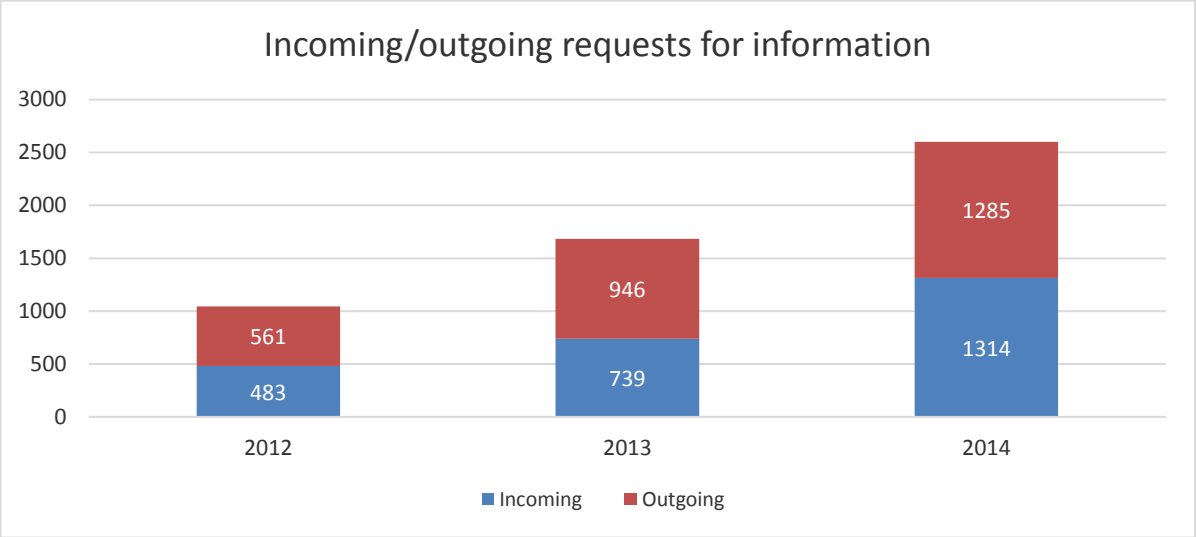

Figure 179: Number of incoming/outgoing requests for information 2012-2014

A special feature of the Budapest Cybercrime Convention is the expedited preservation of stored computer data under mutual assistance (Article 29 et seq.). Under these provisions CYCO forwarded 15 requests on behalf of the cantons to foreign law enforcement agencies and, conversely, received 11 requests from its foreign partners.

4.2 Co-ordinating national and international investigations

CYCO co-ordinates the incoming and outgoing requests for information as part of the international exchange of police data. In 2014, these requests totalled 146.The type of support provided by CYCO depends on the specific case and situation. In international investigations, for

example, it assumes a coordinative role, acting as the national contact point for law enforcement agencies from abroad, and as an advisor to the police and judiciary at home. Where jurisdiction for a case lies with the canton, on the other hand, CYCO provides the competent agencies with its analytical, technical and legal expertise or with undercover investigators.

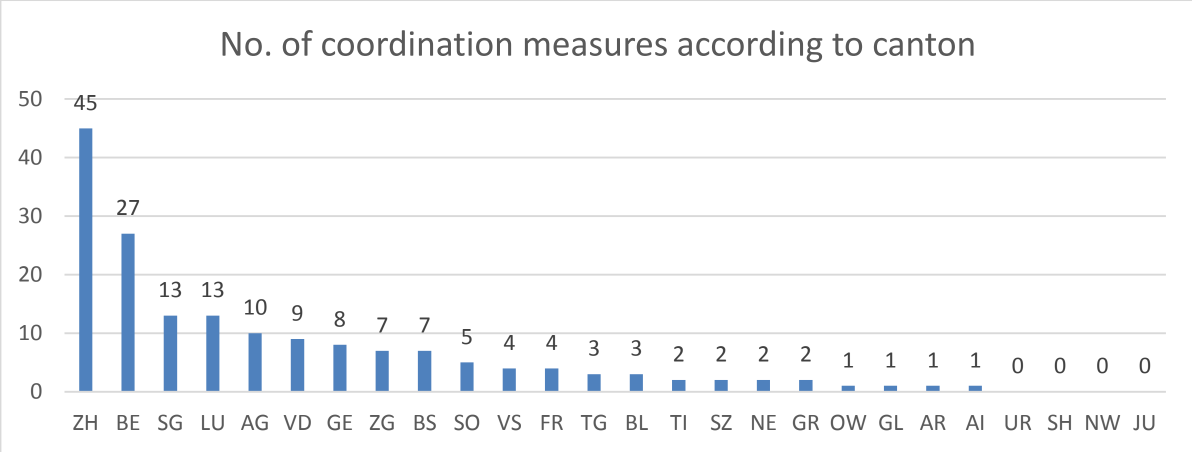

Figure 20: Number of coordination measures according to canton 2014. Since a coordination measure can have a bearing on several cantons, the total in the graph does not correspond to the total listed above (i.e. 180).

The measures CYCO takes aim to ensure that the resources of the cantonal police are used in an optimum way, and to prevent duplication of efforts in national investigations. In 2014, for example, CYCO organised coordination meetings in two cases with representatives involved in investigating the same case.

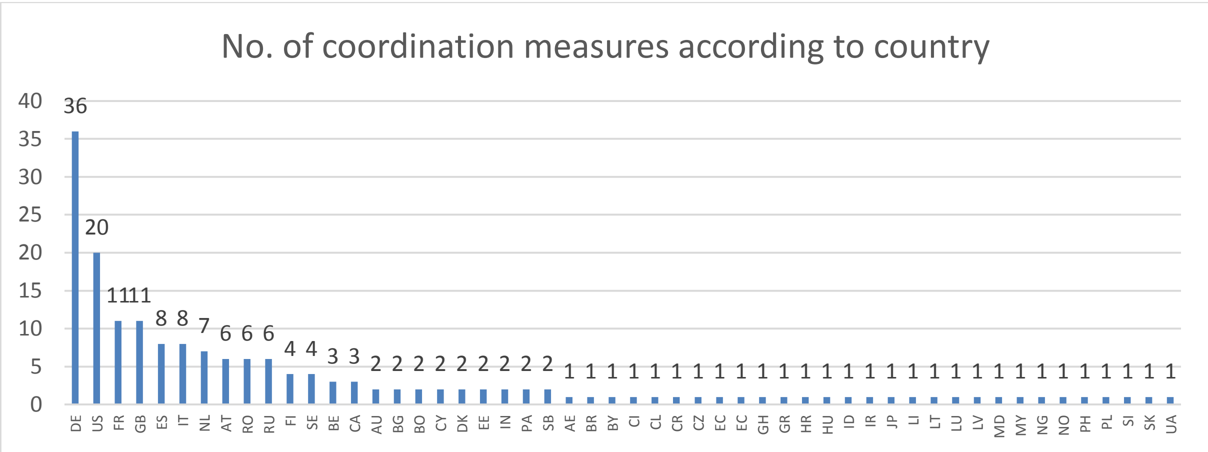

Figure 181: Number of coordination measures according to country 2014. Since a measure may have a bearing on several countries, the number of measures listed in the graph does not correspond to the above-mentioned figure (i.e.180).

Prosecuting offenders who are loosely organised and act from abroad requires extensive resources and know-how. Prosecuting individual criminal acts as part of a case cluster – for example, one case of damage or loss from a widely spread malware campaign – is often doomed to failure on account of the lack of hard evidence. Experience gained on the occasion of a malware attack against Swiss banking clients showed that it is extremely important – although laborious and costly – to have an overview of cases at national level in order to identify links between the malware attack, the distribution of the malware via e-mail or bogus websites,

and the payment and transfer of the stolen money (see Measure 6 of the National Strategy on Protecting Switzerland from Cyber Threat). Only once the authorities have been able to analyse the findings from all the reports submitted on a certain phenomenon do the investigations produce further leads. Since such case clusters often involve not only Switzerland but also other French, Italian and German-speaking regions within Europe, international cooperation and data exchange with other agencies such as Europol's European Cybercrime Center EC3 are essential and also save resources.

4.3 Case studies

In May, an international operation in 16 countries, co-ordinated by the US Federal Bureau of Intelligence FBI, led to the arrest of approximately 100 people in connection with the malware "Blackshades." In the run-up to the operation, CYCO launched a preliminary investigation based on the information it had received from the FBI and aimed at identifying potential offenders in Switzerland. Based on these investigations and following a coordination meeting called by CYCO with the competent public prosecutor's offices and police authorities, criminal proceedings were opened in 11 cantons under Article 144bis paragraph 2 SCC against suspects accused of importing unlawful malicious software. In a second coordination meeting, the cantonal prosecuting authorities presented the first results of their investigations. They also coordinated the procedure for the day of action. On the day itself, the cantonal police simultaneously carried out 16 house searches and questioned suspects. Those arrested were an average of 24 years of age, the youngest being only 16. The first verdicts have already been passed.

In another case, CYCO received a request for assistance from a foreign partner agency under Articles 29 and 30 of the Budapest Convention on Cybercrime. During its investigations, the foreign partner agency had established that a Swiss web service had been used in a case of extortion to send e-mails. The foreign partner agency requested CYCO to secure information that could lead to the identification of the person who had sent the e-mails. The service had been operated by an unknown person via a website hosted by a Swiss ISP. However, the residence of the person and the actual data were located in two different cantons, which therefore required the police and judicial authorities of both cantons to coordinate measures. In cooperation with the competent police corps, the cantonal public prosecutors and the department for international mutual legal assistance at the Federal Office of Justice, CYCO managed to quickly identify the operator of the service and secure the release of the data. On receiving an upfront digital copy of the mutual assistance request from the requesting authority, CYCO was able to transmit the necessary data via the police the following day (Art. 30 Budapest Convention on Cybercrime).

5 Projects

5.1 National Strategy on Protecting Switzerland from Cyber Threat

On 27 June 2012 the Federal Council approved the National Strategy on Protecting Switzerland from Cyber Threat (NCS). Combating cybercrime is one of the important factors in protecting Switzerland's critical infrastructures, which finds expression in Measure 6 of the strategy. The Federal Department of Justice and Police FDJP has been mandated to implement this measure. To this end the FDJP, in collaboration with the cantons, is to compile an overview of internet crime in Switzerland with the aim of improving the coordination of intercantonal case clusters. The information gathered from prosecuting such cases is to be integrated into MELANI's situation analysis.

A strategy paper for implementing Measure 6 is to be submitted to the Federal Council by the end of 2016. The paper is to clarify interfaces with other players involved in reducing the cyber threat and review the coordination of situation analyses. Further, it is to define the resources and legislative amendments necessary at cantonal and federal level for implementing the measure.

Work on the strategy paper for Measure 6 NCS is successfully underway. At the beginning of May 2014, CYCO launched a national questionnaire among all the cantonal and federal law enforcement authorities. The findings from this questionnaire, together with the vulnerabilities and needs of all agencies involving in fighting cybercrime, have been incorporated into the strategy paper.

Due to the complexity of the mandate, the project work has proven to be more extensive than originally expected. For this reason, consultation with the cantons has been delayed to the first quarter of 2015. Final revision of the strategy paper is expected in September 2015, after which it will be submitted to the Federal Council.

6 Working groups, partnerships and contacts

6.1 National File and Hash Value Collection

CYCO and the cantons operate the National File and Hash Value Collection NFHVC, a database containing the hash codes of pornographic images that are classified as illegal. The purpose of this database is to reduce the amount of work of, and the psychological stress on child pornography investigators by automatically categorizing images whose hash code is already registered in the database. The database has been in operation since October 2012 and is used by specialist units of the cantonal and municipal police.

Following the amendment to Article 197 SCC with effect from 1 July 2014, the database had to be adapted to the new statutory provisions. This meant that the hash codes of pornographic images containing excrement had to be deleted from the system.

The cantons can only access the hash codes of images that have been clearly defined three times as illegal. Categorising the images is time-consuming. To exchange data between international partner agencies, the categorisation of images must be uniform and the quality reliable. This means that images whose hash codes are exchanged must clearly constitute child pornography under international standards so that, for example, a hash code generated in Germany under German standards can also be used in Switzerland to classify child pornography. The objective of these measures is ultimately to ensure that the hash codes of images that are clearly illegal can be used as evidence in court documents.

Up to the end of 2014, approximately four million images had been entered in the database. Categorising the images takes time and can only be assured thanks to the active support of the cantons. An image only constitutes illegal pornography if it has been classed as such three times by officers from the cantonal police or CYCO. To date around 138,000 images have been clearly identified as illegal; their hash codes can therefore be accessed in the database.

CYCO has also received approximately three million hash codes from foreign law enforcement agencies and made these available to the cantons for forensic evaluation. However, since the corresponding images are not available, CYCO cannot perform a quality check. These codes are therefore designated as “suspected hash codes” as opposed to the confirmed hash codes in the database. In addition, CYCO has made available 78 million “white list” hash codes; that is, parameters such as the icons of operating systems or applications that do not denote illegal content. These white lists automatically reduce the data prepared by the forensic officer. CYCO systematically procures such white lists and makes them available to the cantons at the same time as the black lists.

One of the Global Alliance’s policy targets for Switzerland is to enhance efforts to identify victims of online child abuse (see Chapter 6.7.3). To this end, CYCO is working on a strategy with the cantons to increase its collection of data in order to facilitate a comparison of data with INTERPOL’s ICSE database and hence systematic identification of victims. The strategy paper is expected by 2016.

Besides the importance of hash values for forensic evaluation, a central database of images offers numerous investigative approaches for identifying the geographical location of offenders and their victims, and hence for determining legal jurisdiction (which may be different from that originally thought to be the case). There is international consensus that investigations based on seized images and international cooperation are very promising approaches to identify victims. It is also justifiable from an ethical standpoint to use available resources to identify children who are possibly still being sexually abused at the time the images are discovered or seized, even if the law enforcement agency in question discovers that the case does not fall

within its jurisdiction. Thus, victims can be assured that law enforcement agencies will act to prevent future abuse and arrest offenders regardless of location or jurisdiction. Law enforcement must take on joint responsibility for combating online child abuse and exploit all available avenues for preventing this global phenomenon.

Switzerland's efforts in identifying victims still have potential for improvement. The hash value database is the first cornerstone in the systematic identification of online abuse victims. Unfortunately, the numerous online communication channels such as forums, P2P networks, social media sites and anonymous networks remain targets for those who wish to harm children.

The hash value database is also an important tool in combating the production, trade and distribution of illegal pornography and hence in combating online child abuse and the ongoing victimization of children. Through her participation in the Global Alliance Conference against Child Abuse on 6 December 2014, Federal Councillor, Simonetta Sommaruga, underscored Switzerland's commitment to support the fight against child abuse both at national and international level.

6.2 Working groups at national level

In 2014, CYCO was represented in the following working groups:

Together with the FCP's Paedophile Crime and Pornography Section, CYCO organises and is a member of the *Arbeitsgruppe Kindsmissbrauch* (Child Abuse Working Group). The working group comprises representatives from federal and cantonal law enforcement agencies, Swiss Crime Prevention and NGOs involved in child protection.

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.

6.3 Cooperation with other federal agencies

Since internet crime involves offences that fall under nearly all titles of the Swiss Criminal Code, CYCO cooperates closely with other federal agencies. Within fedpol it works primarily with the Federal Criminal Police Division's *Digital Crimes Investigations Section, Undercover Investigations Section* and *Paedophile Crime and Pornography Section.* The Coordination Unit also works closely with the International Police Cooperation Division.

CYCO also intensified contacts with various other federal agencies such as with the Reporting and Analysis Centre for Information Assurance MELANI, the International Mutual Assistance Division of the Federal Office of Justice FOJ, the Swiss Financial Market Supervisory Authority FINMA, the Swiss Federal Institute of Intellectual Property IPI and the Federal Gaming Board FGB, the Federal Department of Foreign Affairs FDFA and the Security Alliance of Switzerland SAS.

6.4 Exchanging expertise with the cantons

Throughout 2014 CYCO maintained numerous contacts with representatives of various police forces and public prosecutors' offices. Most of these contacts were linked to ongoing cases. These contacts not only enabled the cantons to benefit from CYCO's expertise and its international contact network, they also allowed CYCO to profit from police knowledge of local conditions, from well-established procedures between the police and public prosecutors' offices, and from the forensic expertise of the cantons.

In its role as a coordinating body and through its close cooperation with the cantons (see Chapter 5.3), CYCO succeeded in preventing the destruction of evidence by several suspects and in helping to bring charges against a suspect as a result of facts reported from abroad.

6.5 Cooperation with non-government organisations and associations

For several years CYCO has worked closely with the NGO[9] *Action Innocence Geneva (AI)* in combating child pornography. Thanks to AI's active support, the project monitoring P2P networks has been run and expanded successfully over the last few years.

CYCO also maintains close ties with "Stop Piracy", an association that reports to the police or the hosting provider fraudulent online shops selling forged brand products.

In addition, CYCO is also working towards cooperation with the "Swiss Internet Security Alliance SISA", an association of internet service providers and IT specialists whose aim is to free the internet in Switzerland from malware.

6.6 Cooperation with Swiss internet service providers

Since 2007, CYCO has assisted major internet service providers (ISPs) in blocking access to foreign websites containing child pornography (as defined under Art. 197 para. 4 and 5 SCC). CYCO sends ISPs a regularly updated list of websites containing such material; the current list contains between 700 and 1,000 web pages. Access to web pages on this list is blocked by the ISPs based on their 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. CYCO monitors the internet actively for child pornography, updates its blacklist regularly and supplements INTERPOL's "worst websites" list with its own entries. INTERPOL's list is compiled in collaboration with various international police agencies.

9 Non-Governmental Organisation

6.7 International cooperation

6.7.1 Europol

CYCO has been a member of various European Cybercrime Center EC3 working groups since 2011. EC3, based at Europol in The Hague, provides EU member states and third states with operative support in combating cybercrime and with expertise for joint investigations at EU level. CYCO maintains close ties with EC3, participating regularly in various strategic and operative meetings in 2014. EC3 focuses on combating three areas of cybercrime: cybercrime in the strict sense (Focal Point *Cyborg*); payment card fraud (Focal Point *Terminal*); and online child sexual exploitation (Focal Point *Twins*).

CYCO is a member of the Focal Point *Cyborg*, whose goal is combating transnational cybercrime in the strict sense. Its priorities, amongst other phenomena, are phishing, DDoS attacks, botnets, and hacking. In addition, CYCO and the FCP's Paedophile Crime and Pornography Section are members of the Focal Point *Twins* whose priority is combating online paedophile crime.

6.7.2 Swiss membership of the Virtual Global Taskforce

The rapid development of the internet provides criminals with ever new means of being one step ahead of law enforcement when it comes to child abuse. In response to this development, the Virtual Global Taskforce (VGT) is an international partnership between law enforcement agencies, NGOs and the private sector for the protection of children from online sexual abuse. The alliance aims to make the internet safer, to identify abuse more quickly, to locate and help children in need and to ensure that offenders are brought to justice.

Switzerland has been a member of the Global Alliance against Child Sexual Abuse Online since 2012, thus sharing responsibility for combating paedophile crime. In 2014, it fulfilled one of the milestones of cooperation with the Alliance by becoming a member of the VGT.

Other VGT members include Australia, Great Britain, Italy, Canada, Colombia, Korea, Netherlands, New Zealand, the United Arab Emirates, the United States of America, Europol and INTERPOL.

Members from the private sector include End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes network (ECPAT International), International Association of Internet Hotlines (Inhope), National Center for Missing & Exploited Children (NCMEC), International Centre for Missing and Exploited Children (ICMEC), PayPal, Microsoft Digital Crimes Unit, World Vision, Blackberry, The Code, Kids Internet Safety Alliance (KINSA), NetClean, International Justice Mission and Telstra.

Further information on the VGT is available on www.virtualglobaltaskforce.com.

Figure 22: On 13 May 2014, Thomas Walther, Head of CYCO, signs the act of Switzerland's accession to the Virtual Global Taskforce in Brussels in the presence of Anthony L. Gardner (left), US Ambassador to the European Union, Roberto Balzaretti (right), Swiss Ambassador to the European Union, and Ian Quinn, VGT Chair (second from left).

6.7.3 Global Alliance against Child Sexual Abuse Online

At the invitation of EU Commissioner for Home Affairs, Cecilia Malmström, and US Attorney General, Eric Holder, representatives and experts from over 40 countries met on 30 September 2014 in Washington D.C. for the second ministerial conference of the Global Alliance.

During the conference, speakers from law enforcement, the private sector and NGOs provided an insight into what had so far been achieved in the four policy target areas (victim identification, offender identification and prosecution, awareness-raising among children of online risks, and preventing re-victimisation). In his opening speech, Mr. Holder, expressed his pride in the developments since the Global Alliance came into existence and the achievements so far. Since 2012, 54 countries have joined the Alliance in the active fight against the online sexual abuse of children. Mr. Holder emphasized the need for work to continue because the threat of abuse was increasing all the time. One problem of particular note is that online child pornography circulates freely and leads to a perpetual victimisation of the children concerned. The Alliance cannot solve the problem single-handedly and therefore considers its work as a supplement to all the structures and agreements that already exist at international level.

The Global Alliance establishes political and operative goals but leaves it up to the individual countries to decide for themselves how to implement or achieve them. Switzerland attained – even superseded – its goals for 2014 in all areas. This has led to a high level of regard for our country in fighting child sexual abuse online; Switzerland was mentioned on more than one occasion during the presentations, and has come into the forefront in the last two years in the international fight against online child abuse.

On the initiative of the British Prime Minister, David Cameron (and in keeping with the objectives of the Global Alliance), the #WePROTECT Children Online Global Summit took place in London on 10 and 11 December 2014. As opposed to the Global Alliance, the focus of #WePROTECT is not on law enforcement agencies but on stakeholders from the private sector. Leading technology companies have pledged their support for this mission and, together with representatives from law enforcement and from private organisations, have signed a statement of action[10].

6.7.4 US FBI & Homeland Security

Since most of the major internet service providers are based in the USA and the US authorities also work closely with Europol and its member states on fighting cybercrime, CYCO maintains close ties to the office of the FBI Legal Attaché in Bern. With this office CYCO exchanges not only police data but also information at an informal level on best practices with regard to securing the data of major American service providers. Similarly, CYCO receives requests via fedpol's Operations Centre from the Legal Attaché to secure the data of Swiss internet service providers.

CYCO is also in close contact with the US Department of Homeland Security's Immigration and Customs Enforcement (ICE) Attaché in Rome. The attaché liaises with the ICE's Homeland Security Investigation's Cyber Crime Center, whose head currently chairs the VGT.

[10] Statement of action under https://www.gov.uk/government/publications/weprotect-summit

7 Media coverage, training and conferences

7.1 Media presence

During the reporting year, CYCO's activities received considerable media attention. CYCO staff responded to around one hundred media queries.

CYCO's online crime alerts in particular are worth mentioning. Some were covered in the media and brought to the attention of partner organisations such as MELANI and Swiss Crime Prevention. Alerts are mainly issued when CYCO receives a surge in reports concerning a specific phenomenon. Alerts are also issued at specific times of the year, e.g. right before holidays when certain types of offences tend to occur. During the reporting year, CYCO warned of e-mail scams where fraudsters purporting to be mail-order companies, telecom operators, etc. notified recipients of unpaid bills that were in fact malware. CYCO also warned of more frequent attempts at fraud and fake online shops during the period right before Christmas.

Many of the largest Swiss publishing houses have already established digital departments that deal specifically with cybercrime issues and provide information to broad swathes of the general public. In recent years, many celebrities have fallen victim to cyber criminals. Social media pages maintained by CYCO (Twitter in particular) have been actively followed by online editorial teams in Switzerland and abroad. Alerts published by CYCO have been widely reported through media channels and also often include information on how to report incidents.

7.2 Social media

CYCO has been active on social media platforms Facebook (www.facebook.com/cybercrime.ch) and Twitter (@KOBIK_Schweiz) since 2013. These platforms serve to quickly alert the Swiss general public to the latest phenomena such as frequently reported scams or the most recent malware campaigns. Feedback has been quite positive so far.

Regular Facebook postings over the past year in German, French and Italian have already drawn 3,576 Likes. In addition, the multilingual Twitter profile currently has 487 followers.

7.3 Training and conferences

CYCO staff have taken part in several international conferences, meetings and training courses. These events are used not only for personal development purposes but also to keep in touch and share information with partners and experts in the area of cybercrime, child protection and victim identification.

CYCO staff also conducted various training activities. For example, two employees gave a two-day training course in Switzerland on Open Source Intelligence at the Central European Police Academy (MEPA). CYCO staff also served as experts, instructors and guest speakers at over a hundred other events.

In addition, CYCO held the third “CYCO – Public Prosecutors Forum on Cybercrime” on 13 November 2014. International law enforcement experts provided participants with practical insight into international efforts to crack down on cybercrime. In addition, INTERPOL’s mobile laboratory for the identification of victims of child pornography was presented and participants were asked to carry out practical exercises. In the closing panel debate, revision of the Federal Act of 6 October 2000 on the Surveillance of Postal and Telecommunications Traffic (SPTA, SR 780.1) was discussed. Around one hundred people took part in the forum.

With support from INTERPOL, CYCO devoted the following day, 14 November 2014, to providing cantonal and municipal police officers with training in victim identification. This training day is the direct result of Switzerland’s membership of the “Global Alliance against Child Sexual Abuse Online” (see 6.7.3 Global Alliance) and the corresponding measures and commitments. Among other things, member countries are required to intensify their efforts to identify the victims of child pornography and afford these victims protection, guidance and support. The training day was conducted with the aim of enabling police officers to proactively and systematically identify the victims of child pornography over the internet using an international template. In addition, action will be taken to determine whether synergies can be created between image categorisation in the hash value database and victim identification through INTERPOL’s ICSE database. Moreover, a task-sharing procedure to enable cooperation and victim identification will be established with the help of the cantons by the end of 2016.

In relation to the hash value database, CYCO organised several training courses throughout the year on the categorisation of images and video content. At the request of cantonal public prosecutors, these training courses were given to police investigators and representatives of private companies involved in the forensic analysis of seized material and associated categorisation of images. The aim is to ensure that illegal pornographic images may be categorised within the NDHS using Swiss-wide criteria, thereby ensuring that the database is qualitatively reliable. During the two half-day courses, course participants also learnt about legal matters and were given the opportunity to categorise their own images and discuss any categorisation disagreements with the instructors.

8 Political motions at federal level

Motion 14.3022: Child pornography. Prohibiting images of posing children– Rickli Natalie Simone, 3.3.2014

Question 14.5175: Cyber risks. Tumblr platform – Schmid-Federer Barbara, 12.3.14

Interpellation 14.3204: Consensus of Agur 12 working group. Subsequent action – Gutzwiller Felix, 20.3.14

Interpellation 14.3250: What can be done to curb youth violence? – Grin Jean-Pierre, 21.3.14

Motion 14.3288: Identity theft. A criminal act in itself – Comte Raphaël, 21.3.14

Motion 14.3367: Cracking down on sexting – Amherd Viola, 8.5.14

Postulate 14.3655: Defining what digital identity means and finding ways to protect it – Derder Fathi, 20.6.14

Motion 14.3665: Additions to Article 260bis SCC (Art. 187 SCC, “Sexual acts with children”) – National Council Legal Affairs Committee, 14.8.14

Motion 14.3666: Article 198 SCC. From offences prosecuted on complaint to offences prosecuted ex officio – National Council Legal Affairs Committee, 14.8.14

Interpellation 14.3888: International efforts to suppress hate propaganda over the Internet – Naef Martin, 25.9.14

Motion 14.3905: Identifying the authors of hate messages – Schwaab Jean Christophe, 25.9.14

Postulate 14.3908: Internet. Non-tolerance of intolerance – Tornare Manuel, 25.9.14

Postulate 14.3962: Improving international administrative assistance in cases involving criminal acts against children – Müller-Altermatt Stefan, 26.9.14

Postulate 14.3963: How paedophiles hide behind data protection rules – Müller-Altermatt Stefan, 26.9.14

Interpellation 14.3969: Using media competence to defuse hate campaigns – Masshardt Nadine, 26.9.14

9 Future developments

The number of reports received by CYCO depends primarily on the inclination of the population to report suspicious content found on the internet. Thanks to these reports, CYCO now has a clearer view of the cybercrime landscape in Switzerland. Nevertheless, this is only the tip of the iceberg. Most illegal activities on the internet remain largely beneath the radar screens of the general public in Switzerland. The following paragraphs are based on *open source* information[11] and other reports as well as on the expertise gained by CYCO over the past 11 years of activity.

Phishing campaigns and fine-tuning of fraud tactics

In the early days, internet fraud was largely perpetrated via e-mail. Since then, cyber criminals have evolved and now use some rather ingenious tactics. They have a better mastery of IT tools, some of which help them to hide their tracks (e.g. TOR network, VPN services and bulletproof servers). As we enter 2015, Switzerland will remain a favoured target for phishing campaigns due to its prosperity and high density of internet usage. Cyber criminals use phishing sites that look identical to official sites and are practically undetectable to the untrained eye. In order to circumvent anti-virus programs and firewalls, cyber criminals save their webpages to their own or pirated accounts, or on cloud services (e.g. *Dropbox*, *Google Drive*, etc.). This lends the phishing page an appearance of legitimacy. An alternative method is to inject malicious code into a reputable website and redirect visitor traffic to the phishing site. Along this line, an increase in abusive use of new top-level domain names (e.g. *support*, *.email*, etc.) and more expired or stolen security certificates is expected.[12]

There are two parallel trends that are a goldmine for swindlers on the web: people wishing to be connected at all times (even while on the move) and people wishing to share information with everyone (one's daily routine is punctuated by the publication of statuses, physical location, moods…). Cyber criminals begin by harvesting large volumes of information about their target for the purpose of preparing highly sophisticated frauds (namely via social engineering techniques). Such illicit activities are not only detrimental to individual citizens but also to SMEs and large companies alike. A heightened prevalence of identity theft associated with a rise in fraud cases is therefore likely.

The Darkweb underground economy

The rapid growth of the internet combined with the prevalence and popularity of anonymisation techniques have prompted cyber criminals to make increasing use of Darkweb services. Launched on 6 November by Europol and the FBI in collaboration with sixteen European countries, including Switzerland, Operation Onymous[13] is indicative of the level of penetration of these techniques among the general public. Many shops and illicit traffic have moved to the Darkweb where it is possible, more or less anonymously, to buy malware and credit card information, to rent a botnet or to launch DDoS attacks[14]. These platforms have also become a place where child pornography, drugs and all manner of prohibited goods are bought and sold. These activities are facilitated by the spread of virtual currencies such as bitcoins and other

[11] The following links were last accessed on 18 March 2015.

[12] http://www.csoonline.com/article/2687132/social-engineering/recently-introduced-tlds-create-new-opportunities-for-criminals.html

[13] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network

[14] Trend Micro, Deepweb and Cybercrime, 2013, pp. 9 et ss.

forms of remote payment, which allow funds to be transferred more discretely and anonymously.

Certain groups of criminals no longer limit themselves to merely selling their services. Nowadays, they even offer "after-sales service" and 24/7 assistance to their "clients"[15]. For example, it has become possible to hire botnets to send spam or Trojan horses while benefiting from technical support in the event that a problem arises. These criminals have developed a new *business model,* referred to as *Crime-as-a-Service,* which is capable of innovating and competing. Cybercrime is no longer the preserve of specialists but is accessible to anyone with a large enough budget. There is every reason to believe that this trend will accentuate even more over the next few years.

Malware on mobile phones

In the future, smartphones and other tablets will take an even greater market share away from traditional computers[16]. For some users, smartphones have already become the option of choice, since they enable people to be even more readily accessible. Smartphones are a veritable hyphen between the person using it and the person's virtual identity. With perhaps one notable difference: while an individual in society has an intrinsic identity, their virtual identity is comprised of many scattered elements that are difficult to keep under control (e.g. e-mail messages, photos, SMS, social network postings, etc.). While the average user has understood the importance of installing an anti-virus program and performing regular updates of the various software programmes on their computer, this is not at all the case when it comes to mobile devices where an understanding of the inherent risks and dangers is minimal. Cyber criminals exploit this negligence by developing an increasing number of malware programs to mine the various bits of data saved to mobile phones or over the web. These applications can also be used to subscribe to and send messages to premium services without the owner's knowledge or consent. Previously limited to computer systems, these malware programs are now being written for the operating systems of mobile devices. This is the case of the police-ransomware *Reveton*, for which a version for Android was identified for the first time last year.[17] The world of virtual cash has also been turned upside down with the arrival of the first malware programs capable of transforming the smartphone of an unsuspecting user into a "bitcoin miner".[18]

Although the general public in Switzerland has thus far been spared, this situation may change in the future.

Past vulnerabilities, cloud computing and new payment systems

The previous year witnessed the emergence of several critical vulnerabilities (e.g. *Heartbleed*[19] and *Shellschock*[20]), or holes in older protocols (e.g. *POODLE*[21]) that enabled criminals and

[15] Europol, The Internet Organised Crime Threat Assessment (iOCTA) report, 2014, p. 11

[16] http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones

[17] http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-moves-to-mobile/

[18] https://blog.lookout.com/blog/2014/04/24/badlepricon-bitcoin/

[19] http://heartbleed.com

[20] http://www.troyhunt.com/2014/04/24/badlepricon-bitcoin/

[21] https://access.redhat.com/articles/1232123

hackers to gain access to mail servers, which they then exploited to create and manage botnets[22]. In the future, we need to be able to anticipate such attacks and respond promptly.

Due to the enormous quantity of information that they contain, cloud services are the preferred target of criminals. The scandal in which explicit photos of certain American celebrities were obtained from hacked *iCloud* servers[23] shows the consequences of having a poorly protected account. Cyber criminals are drawn to the large quantity of personal information and are likely to continue attacking different cloud services in the future. Users must be made aware of this and should take the necessary steps to secure access (e.g. two-factor authentication and use of difficult passwords).

Another area of concern is the increasing use of new cashless payment systems. Companies are engaged in fierce competition to create tomorrow's digital wallets. Examples include: *Apple Pay*, *Google Wallet* and *Cashcloud*. As with all new technologies, these payment systems will invariably draw the interest of criminals. To counter this, consumers will need to learn how to use these payment systems as securely as possible.

The Internet of Things

Cisco estimates that the number of devices connected to the internet will reach 50 billion in 2020[24]. In addition to computers, tablets and other smartphones, the internet will connect all sorts of different objects: showers, kitchens, lamps, thermostats, cars, etc.; this state of affairs is referred to as the *Internet of Things*[25]. There is every reason to believe that this trend will lead to new vocations among cyber criminals. For this reason, it is all the more important that the general public be made aware of both the possibilities and risks of these new technologies and that they learn how to properly protect themselves.

[22] SWITCHcert Report on current trends in IT security and privacy (in German), November 2014, pp. 1-2

[23] http://time.com/3247717/jennifer-lawrence-hacked-icloud-leaked/

[24] SWITCHcert Report on current trends in IT security and privacy (in German), October 2014, pp. 4-5

[25] http://postscapes.com/internet-of-things-examples/