Council of the
European Union

Brussels, 8 February 2017
(OR. en)

13203/1/16
REV 1 DCL 1

GENVAL 103
CYBER 112

DECLASSIFICATION

of document:	13203/1/16 REV 1 RESTREINT UE/EU RESTRICTED
dated:	31 January 2017
new status:	Public
Subject:	Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on the Czech Republic

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

Council of the
European Union

Brussels, 31 January 2017
(OR. en)

13203/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 103
CYBER 112

REPORT

Subject:	Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on the Czech Republic

ANNEX

Table of Contents

1. EXECUTIVE SUMMARY

The mission to the Czech Republic was very well organised in an efficient and cordial way by the national authorities. The evaluation team was able to meet representatives of the various authorities involved in the field of preventing and fighting cybercrime, including the Ministry of the Interior, the Ministry of Justice, the Unit for Combating Organised Crime of the Criminal Police and Investigation Service, Analytics and Cybercrime Department of the Regional Directorate of the Police of the Southern Moravian Region, Institute of Criminalistics Prague, Supreme Public Prosecutor's Office, National Security Authority/National Cyber Security Centre and representatives of academia and non-governmental organisations.

During the visit, the representatives of the Ministry of the Interior in charge of the evaluation visit did everything to provide the evaluation team with clarifications on the legal and operational aspects of detecting, preventing and combating cybercrime, international judicial cooperation in criminal matters and cooperation with EU agencies, cyber security strategy, training, etc.

The meetings helped the evaluation team gain a better understanding of the responses provided in the questionnaire and of the national system in the Czech Republic. The evaluation team on its mission to the Czech Republic also recognised the essential effort made by the many speakers who gave presentations highlighting organisational matters, human resources issues, workflow in investigations, the main trends in the field of cybercrime, prevention and awareness raising, training, international police and judicial cooperation — especially in relation to Europol, Interpol and Eurojust — legislation (including recent changes), the criminal justice system, cooperation among national institutions, academia, industry and non-governmental organisations, national strategies to combat organised and serious crime, and strategies on national security and national cyber security.

A judge was present for the first day of the visit, when the team met representatives from the police. The team appreciates the effort of CZ authorities to include judges in the evaluation visit, although their presence would have produced more added value had it been announced before the visit or had it been arranged separately *ad hoc*.

The various authorities, bodies and organisations have different competences and responsibilities but the 'fight against cybercrime' is seen to be a common goal.

In February 2015, the Czech Republic adopted the second National Cyber Security Strategy for 2015 - 2020; this was followed by the Action Plan, adopted in May 2015. The Strategy includes some fundamental principles, such as protection of fundamental human rights, a comprehensive approach to cyber security based on principles of subsidiarity and cooperation, trust-building and cooperation between the public and private sectors and civil society, and cyber-security capacity-building. The Strategy also identifies the challenges and main goals in the field of national cyber security.

The national legislation complies with the Council of Europe Convention on Cybercrime and with Directive 2013/40/EU on attacks against information systems. Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography has also been transposed into national law.

A more coordinated approach on statistics at national level would be beneficial in terms of giving an accurate picture of the types of cybercrime, as reflected in the different stages of investigation, prosecution and trial, especially for offences relating to the sexual exploitation of children.

Regarding the national structure of LEAs, there are 14 police units with nation-wide competences. From 1 April 2016 a reorganisation of the police will be in place as regards cybercrime competence, allowing the Unit for Combating Organised Crime to investigate the most serious cybercrime offences as a specialised body at central level. The Organised Crime Unit will include the Cybercrime Department and the Department of Cybercrime Investigation and Analysis.

Competence for cybercrime offences will then be shared between the Unit for Combating Organised Crime and Investigation Service and the territorial units.

As to prosecution, a network of prosecutors specialising in cybercrime was recently established formally at national level; it includes 17 prosecutors. During the meeting with representatives of the General Prosecutor's Office, a case of trafficking of human beings and child sexual exploitation, which involved the creation of a Joint Investigation Team (SE, ES and CZ), was presented to the evaluation team.

The National Cyber Security Centre was established recently. Its primary task is identification of critical information infrastructure. In addition, it performs security audits, exercises, international cooperation and policy work. It also offers legal and policy support for the governmental CERT's (GovCERT.CZ) activity and technical cooperation with LEAs in the field of cybercrime (it can provide technical help in criminal investigations). The National Cyber Security Centre has an important role in education and awareness-raising concerning cyber-attacks and cybercrime. Its basic services may be summarised as follows: reactive, proactive and analytical. Its main roles are handling incidents, testing development and security, and analysis of networks.

The Czech Cyber Security Incident Response Team (CSIRT.CZ) fulfils the role of a national CERT and coordinates responses to security threats in computer networks and organises cooperation with internet service providers. It offers help to other private companies in establishing their own CSIRTs. The Czech CSIRT runs the PROKI project, designed to predict and protect against cyber-incidents.

Regarding the field of cyber security it should be mentioned that at national level there are already 24 CSIRT teams and one more candidate team.

Actions aimed at prevention and public awareness of cybercrime are carried out by a number of authorities within the Czech Republic. These include the National Cyber Security Centre, the law-enforcement authorities and the private sector, academia and non-governmental organisations. These sectors play active roles in prevention and awareness campaigns throughout the country. An important and innovative role is played by the Institute of Computer Science at Masaryk University Brno, which has developed a special tool, KYPO (Cyber Exercise and Research Platform). During the visit the evaluation team witnessed a very impressive simulation on this tool. The Centre offers training for judicial and police academies, investigators and public prosecutors. It organises summer schools and PhD and master's degrees in cyber-security. Funding is provided by the governmental security research instrument under the Ministry of Interior. The National Security Authority, as cyber security national authority, is part of the project steering committee.

2. INTRODUCTION

Following the adoption of Joint Action 97/827/JHA of 5 December 1997[1], a mechanism was established for evaluating the application and implementation at national level of international undertakings in the fight against organised crime. In line with Article 2 of the Joint Action, the Working Party on General Matters including Evaluations (GENVAL) decided on 3 October 2013 that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of European policies on prevention and combating cybercrime.

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. The evaluation therefore covers three specific areas: cyber-attacks, child sexual abuse/pornography online and online card fraud; it should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[2] (transposition date 18 December 2013) and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015) are particularly relevant in this context.

1 Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997 pp. 7 - 9.
2 OJ L 335, 17.12.2011, p. 1.
3 OJ L 218, 14.8.2013, p. 8.

Moreover, the Council conclusions on the EU Cybersecurity Strategy of June 2013[4] reiterate the objective of ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 as soon as possible and emphasise in their preamble that 'the EU does not call for the creation of new international legal instruments for cyber issues'. This Convention is supplemented by a Protocol on xenophobia and racism committed through computer systems.[6]

Experience from past evaluations shows that Member States will be in different positions regarding implementation of relevant legal instruments, and the current process of evaluation could also provide useful input to Member States which may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary and not focus on the implementation of various instruments relating to fighting cybercrime alone, but rather on operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, this will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from the actors concerned is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to suppression of cyber-attacks and fraud as well as child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to victims of cybercrime.

4 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 CETS No 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.

6 CETS No 189; opened for signature on 28 January2003, entered into force on 1 March 2006.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. The Czech Republic was the (eighteenth) Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request on 28 January 2014 to delegations made by the Chairman of GENVAL.

The evaluation teams consist of three national experts, supported by two staff from the General Secretariat of the Council and observers. For the seventh round of mutual evaluations, GENVAL agreed with the proposal from the Presidency that the European Commission, Eurojust, ENISA and Europol/EC3 should be invited as observers.

The experts charged with undertaking the evaluation of the Czech Republic were Mr Anton Toni Klančnik (Slovenia), Mr Zsolt Szabolcsi (Hungary) and Ms Nienke Ross (Netherlands). One observer was also present: Ms Anna Danieli (Eurojust), together with Ms Carmen Necula from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in the Czech Republic between 8 and 12 February, and on the Czech Republic's detailed replies to the evaluation questionnaire, together with their detailed answers to follow-up questions.

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber-security strategy

On 16 February 2015, the Government of the Czech Republic adopted the new National Cyber Security Strategy of the Czech Republic for the period 2015 to 2020 (hereinafter 'Cyber Security Strategy'), which was submitted by the National Security Authority (NBÚ), the competent national authority for cyber security issues. The Cyber Security Strategy builds upon and develops its predecessor, the Strategy of the Czech Republic in the Field of Cyber-Security for 2012 - 2015. It was followed by the Action Plan adopted by the Government on 25th May 2015.

The Action Plan specifies tasks, competences and the time-frame for meeting the objectives set out in the Cyber Security Strategy, including combating cybercrime. The unavoidable dependence of society on information technology and the associated increase in cybercrime are conceived in the Cyber Security Strategy as being among the main challenges.

One of the principles which the Cyber Security Strategy builds upon, therefore, is the need to develop capacity to ensure cyber security, which also involves structures and processes in the area of combating cybercrime. Another of its priorities is to strengthen cooperation between law-enforcement authorities and other relevant bodies.

As part of the annual Report on the State of Cyber Security in the Czech Republic, a report on the state of the implementation of the Action Plan is envisaged, as an annex. The report will inform the government and the general public as to the effectiveness of measures adopted and the implementation of tasks defined by the Strategy.

The Cyber Security Strategy and the Action Plan are available in English on websites of the National Security Authority (NBÚ):
http://www.govcert.cz/en/info/strategy-a-action-plan/

Promoting the development of the capabilities of the Czech Republic's police to investigate and prosecute cybercrime is the subject of a separate chapter of the Cyber Security Strategy, reflected in the Action Plan by the following tasks:

- to reinforce the personnel of individual cybercrime police departments;
- to modernise technological equipment of specialised police departments;
- to develop cooperation with foreign counterparts;
- to provide professional education and training to police specialists including language training.

The fight against cybercrime is considered in greater detail in the Conception of the Development of Capabilities of the Police of the Czech Republic to Investigate Cybercrime, which was drafted by the Police Presidium of the Czech Republic and adopted by the National Security Council in October 2015.

This material was created in the context of Government Resolution No 598 of 10 August 2011, and its purpose is to formulate measures to develop suitable long-term conditions for the work of the police force in the detection and prosecution of cybercrime on the territory of the Czech Republic based on the analysis of the current situation. It includes organisational and systemic measures including increasing the personnel of police departments linked to the investigation of cybercrime.

The national authorities mentioned as good practice the establishment and development of cybercrime departments staffed by police specialists. What is important is continuous updating of legislation and prevention programmes. Without close cooperation between the government and the private and university sectors, the situation would be difficult.

Another important need is to provide the personal, technical and educational support to experts and professional staff at the Institute of Criminalistics Prague and departments of forensic technique and expertise which, based on the requirements of law-enforcement authorities, provide expert assessments and examinations in the context of cybercrime.

More information on the National Cyber Security Strategy was obtained during the evaluation visit from representatives of the National Cyber-Security Centre. They underlined that the strategy contains a definition of cyber security which ensure legal certainty and is very useful in practice in order to identify all cyber-security-related issues.

The action plan accompanying the strategy contains a large number of action items (141) and designates 17 responsible entities because in the national authorities view the strategy should not remain merely 'on paper'. Every year the institutions responsible must present an implementation report to the government, which supervises the implementation of the strategy.

The NSA plays a coordinating role in the field of cyber security. It operates the National Cyber Security Centre in Brno, which carries out activities on behalf of the governmental CERT and acts as coordinator for immediate response to cyber-incidents.

Police liaison officers are also part of this structure. The NSA can also act as 'expert' on cyber-security issues for the police. It was one of the main drivers of the National Security Strategy and its Action Plan, adopted in May 2015. Its responsibilities include the defining of agendas for policy and strategy by means of a dedicated Strategy and Policy Unit, providing legal and strategic support to GovCERT.cz. It also engages in dialogue with the other EU Member States.

CSIRT.CZ is active in the region of Prague in the field of prevention and incident handling, especially where repeated or particularly serious. Its role derives from the Act on Cyber Security and a public contract with NSA.

The CERT/CSIRT teams (so far 24 teams have been established, and two more were being set up at the time the visit took place), whether national, governmental, set up by universities, providers, banks, are a significant help in combating cybercrime. The Team observed that teams established in the private sector under the terms of the Cyber Security Act report to CSIRT.

Reference was also made to the PROKI Project, launched by the Ministry of the Interior. The project was initiated because of the need to be able to prioritise within the massive amount of information processed on cyber-security issues. From the collection of security incidents, a report should be sent to inform the operators (say once a week), and at the same time this information should be stored in a system for analysis. As of February 2016, it was reported that the system is up and running.

The Team also heard about how CZ responded, in 2013, to a week of 'waves' of DDoS cyber-attacks against popular news and other media (on Monday), a search engine (on Tuesday), web servers of several banks (Wednesday) and web servers of two mobile operators. The RETN network was the source of the attacks, which luckily were weak and only caused problems in end-user networks. The solution found was to block traffic from abroad: a 'club' of operators as a local peering centre was established in NIX.CZ. Within NIX the project 'FENIX' was initiated, bringing together the biggest local telecommunications companies, hosting companies and service providers. Its members operate trusted networks under strict conditions and can, if necessary, filter out foreign traffic. Those belonging to FENIX contractually prohibit customers from engaging in illegal activities. In the event of a massive attack the targeted operator can shut down connections with attackers and communicate only within the set of FENIX members.

3.2. National priorities with regard to cybercrime

National priorities on cybercrime are directly derived from the Cyber Security Strategy - the section 'Main Objectives' (pp. 17-22). These priorities are linked to strategic objectives and operational action plans drawn up for cybercrime as among the priorities of the EU. Those identified were as follows:

- active international cooperation;
- cooperation with the private sector;
- research and development / consumer trust;
- education, awareness-raising and information society development;
- support for capabilities of the Czech police to investigate and prosecute cybercrime (a separate policy document was produced containing a number of individual points to improve the activities of the police of the Czech Republic in the area of cybercrime).

3.3. Statistics on cybercrime

3.3.1 Main trends leading to cybercrime

The largest proportion of innovations in the field of security threats is represented by mobile platforms. Ransomware is increasing on mobile devices, through virtual currencies like Bitcoin. Attacks using advanced techniques have new and more effective ways to identify and bypass sandboxes and other local security measures. Attacks on social platforms are more aggressive and are aimed at consumers' finance and personal information, as well as entrepreneurs' intellectual property and trade secrets.

Mobile malware is becoming the driving force in terms of both technical innovation and numbers of attacks. New PC malware growth is almost non-existent, while new forms in the Android environment have grown by 33%.

Virtual currencies encourage the spread of malicious ransomware worldwide. Virtual currencies will provide cybercriminals with the unregulated and anonymous payment infrastructure necessary for obtaining money from their victims. Currencies like Bitcoin allow the spread of a new generation of ransomware, such as Cryptolocker.

In the world of cybercrime, advanced attack techniques, such as sandbox-aware attacks, are available. Other technologies include so-called 'return-oriented' attacks, where legitimate applications start to behave in a harmful way, for example, 'self-deleting' malware can cover its trail after reaching its real goal, and advanced attacks also concentrate on specialised industrial control systems focused on public and private infrastructure.

Attacks on social networks are ubiquitous and focused on obtaining passwords or user information, location or business activities. This information can be used to target advertisements or to commit virtual or real crimes.

New attacks on PCs and servers are focused on weak points above and below the operating system. New attacks on PCs utilise vulnerabilities in Web applications in HTML5. Attacks on mobile platforms that will break the 'sandbox' browsers and give attackers direct access to devices and services are expected. Criminals are increasingly focusing on vulnerabilities of operating systems, as well as BIOS.

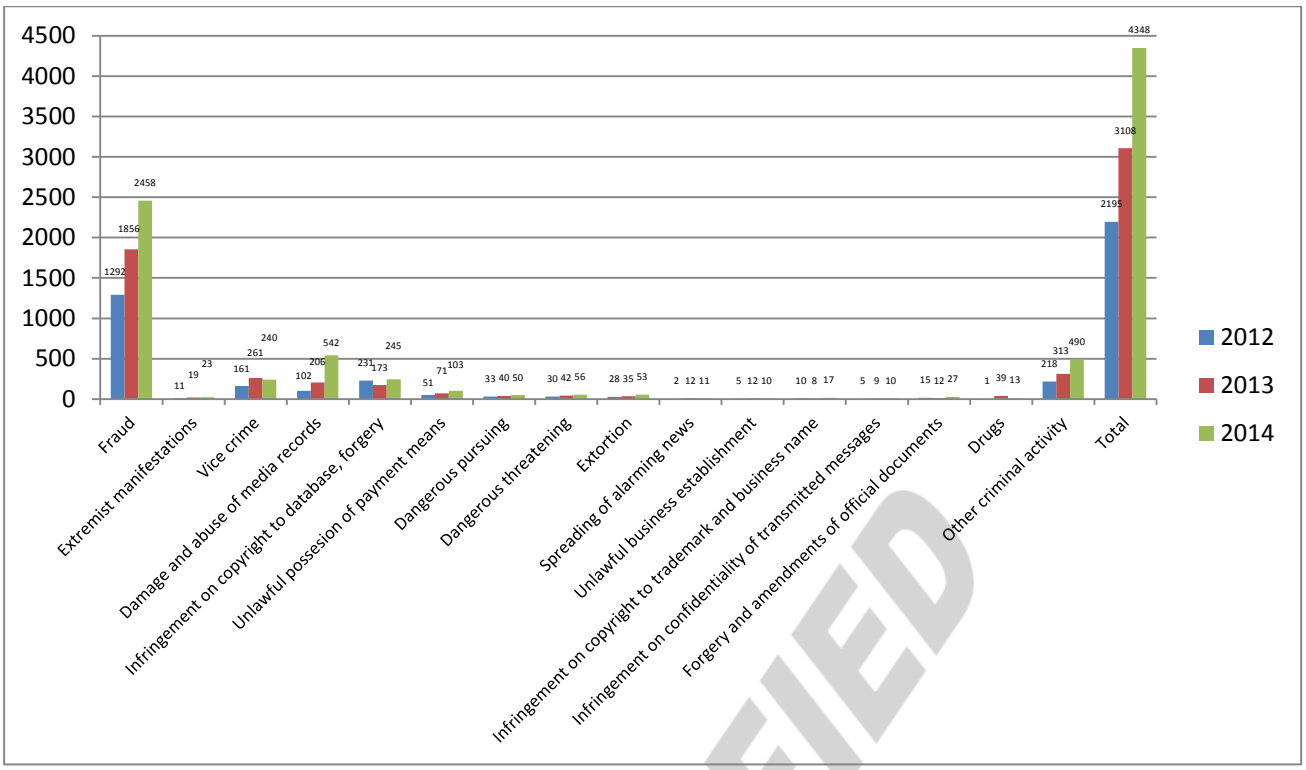
Deploying enterprise applications based on the 'cloud' creates a space for new attacks. Cyber-criminals are exploring ways to use the ubiquitous hypervisors in all data centres, multi-access to users, communication infrastructure of implicit cloud services and infrastructure management, which is used in the provision and monitoring of cloud services on a large scale.

The main trends in the field of cybercrime in the Czech Republic are as follows:

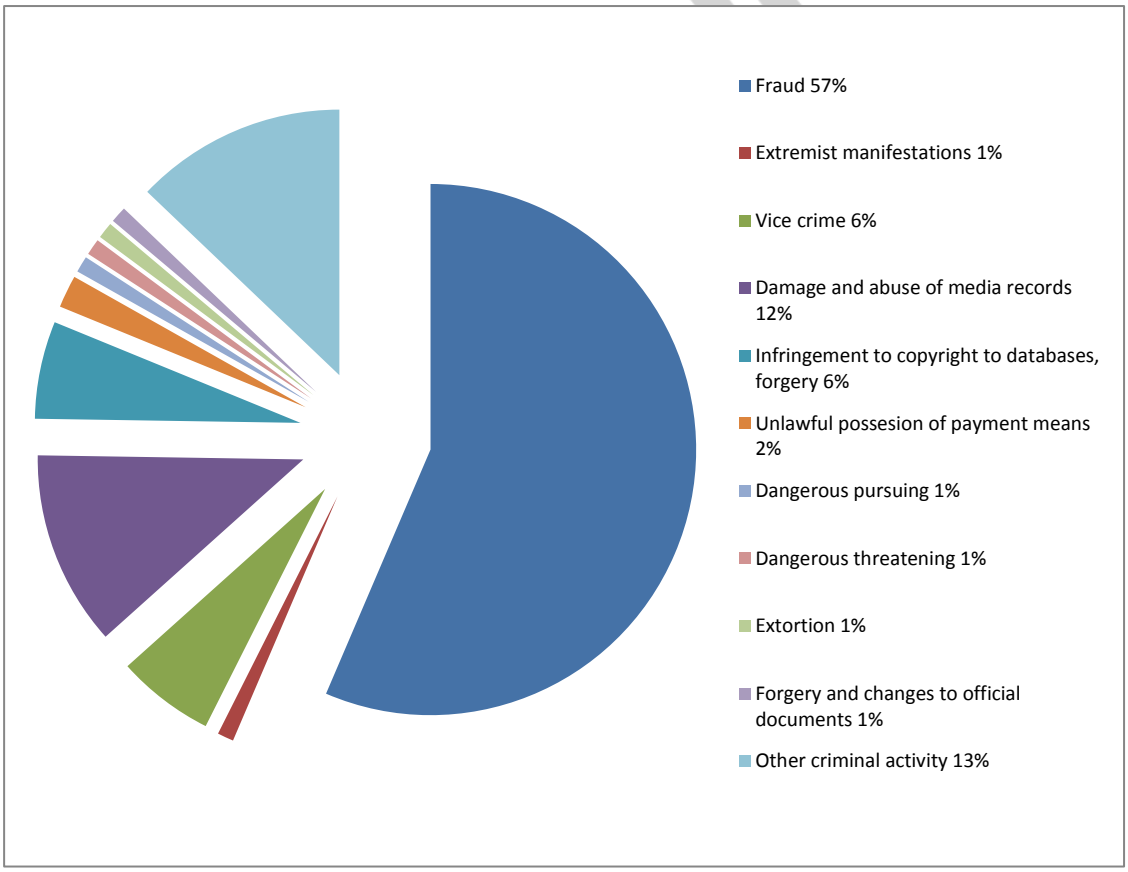
Criminal Offences	Trends
Fraud	- failure to deliver ordered goods – individual, or via whole fraudulent e-shops - failure to pay for delivered goods (predominantly to customers abroad) - organised fraudulent offers to sell, especially, cars from abroad - 'Nigerian letters' (Scam 419) - fraud through spurious e-mails, for example, of the legitimate EMKEI.CZ service
Criminal activities in the field of pornography	- dissemination of pornography, child pornography - production and other handling of child pornography - child abuse for the production of pornography - participation in a pornographic performance - establishing of illicit contacts with a child
Thefts from accounts	- by using malware - by phishing - by abuse of a means of payment
Unauthorised gain, falsification and alteration of a payment instrument	- payment cards, electronic money
Legalisation of proceeds of crime (also as a result of negligence)	- so-called 'work' transfers of stolen money, disguising its origin
Hacking	- attacks on computer and information systems, e-mail accounts etc., and social network accounts – intrusion into privacy, obtaining, their damage and/or destroying information + possible related criminal activity - phishing - DDoS and similar attacks
Dangerous threats, spreading of alarming messages, dangerous stalking	- using electronic communications
Criminal activities in the area of extremism	- defamation of nation, race, ethnic or other group of people, incitement to hatred, establishment and promotion of movements aimed at suppressing human rights and freedoms
Criminal activities in the area of copyright protection	- copying, dissemination, unauthorised use, sharing copyrighted content
Forgery and alteration of public documents, official stamps	- computer technology that allows and significantly facilitates forgery and alteration is used - products are distributed via the internet
Slander	

Cybercrime in the Czech Republic is currently defined as a crime committed in the environment of information and communication technologies including computer networks; the object of an attack is the very area of information and communication technology. There are also cases of criminal activities with a significant use of information and communication technologies as an important means for their commission. It is thus a broader definition of cybercrime than the definition introduced in this questionnaire. For that reason, the Czech Republic feels the need to mention a new phenomenon in the field of cybercrime, i.e. trafficking in drugs and other illicit commodities, both on the open internet and on the dark net. This criminal activity is not directly addressed in this questionnaire but it is gaining in importance. Not only in the field of the conventional drugs trade, but particularly in the retail of new psychoactive substances, drug precursors, chemicals, medicines and anabolic steroids on the internet, we can clearly observe an increase in both the emergence of specialised e-shops and a variety of advertising offers in recent years. Although at present its share in the total volume of crime and also specifically in drug-related crime is small, it shows clear growth. Given the difficulty of detection and investigation of this type of crime (personnel, technical equipment, complicated legislation, etc.), it is necessary to pay far more attention to this area of crime from the perspective of the police in the future. Crime statistics for drug offers and trafficking on the internet are not yet separately followed in the system. For the police of the Czech Republic, this area deserves a higher level of support than in the past, since problems are also reflected in procedural issues, particularly in obtaining data from providers of hosting websites operating abroad. As an example, we can mention requirements towards the US, particularly relating to the services of Google Inc., where repeated requests to supplement information on the basis of international legal assistance can take over six months to be processed. A similar situation is also evident in the area of illegal trade in other commodities - weapons, explosives, explosive precursors, etc.

As regards statistical indicators, we can present statistics on crimes committed in the environment of information technologies and the internet from the ESSK system (see below). However, offences only partly committed in this environment are not included.



Cybercrime offences in 2014 (as percentages):



The total (approximate) capacity of messages exchanged through the Department of International Police Cooperation (OMPS) in the period from 2012 to Q3/2015; for specific categories see question 1.6.:

2012	2013	2014	**3Q 2015**
326	**786**	**814**	**752**

3.3.2 Number of registered cases of cybercrime

Statistical data are provided by the police of the Czech Republic via:

- Statistical Crime Recording System (hereinafter 'ESSK') – this system includes a form with the characteristics of a criminal offence, including indictments and resulting substantive decisions (by police, public prosecutor and court) and a form for statistical reporting of events which are not criminal offences.
- Evidence of Criminal Procedures (hereinafter 'ETR') – a complex information system covering all areas of crime, misdemeanour and other police proceedings including objects, entities, goods and forms; it makes it possible to provide various statistical outputs as well as adding specifics of individual cases – 'monitored event – information crime'.

The majority of criminal complaints originate from individual citizens, not from larger entities such as companies.

Statistical data are also collected in the system of Public Prosecutor's Offices and courts. Court statistics are collected separately from the statistics of law-enforcement authorities (however, the substantive decisions are reflected as described above).

Official national statistics, as mentioned above, are maintained by the law-enforcement sector only (there is no outsourcing, even partial, nor any other similar mechanism). There are also independent studies by private consulting companies that we are aware of; however, these are not taken into account in the official statistics of the law-enforcement authorities and often differ significantly.

Crimes in cyberspace, in terms of monitoring requirements under Directive 2013/40/EC and the requirements of the Joint Action 97/827/JHA of 5 December 1997, may be divided as follows:

a) crimes against the confidentiality, integrity and use of computer data and a system - sanctioned directly in Sections 230 to 232 of the Criminal Code (see attached statistics);

b) crimes of production, distribution and other handling of child pornography in cyberspace;

c) other criminal offences committed via the internet (internet fraud), violations of intellectual property rights (piracy).

Overview of statistics on the exchange of information via the Department of International Police Cooperation in the period of 2013 – September 2015:

received – from abroad via Interpol and Europol channels, or from national bodies – Bureau of Criminal Police and Investigation Service (hereinafter 'ÚSKPV') or other Criminal Police and Investigation Service (hereinafter 'SKPV') bodies								
sent – mainly forwarded to ÚSKPV, or lower units in a follow-up communication								
	2012		*2013*		*2014*		***2015***	
	received	***sent***	***received***	***sent***	***received***	***sent***	***received***	***sent***
child pornography and abuse	***201***	*151*	***88***	*312*	***131***	*325*	***63***	*221*
computer crime	***108***	*99*	***57***	*146*	***51***	*171*	***29***	*170*
CAM notifications	***-***	*-*	***-***	*-*	***561***	*561*	***316***	*316*
fraud and embezzlement	***40***	*36*	***27***	*156*	***23***	*113*	***28***	*120*

CAM notifications only report Czech IP addresses and e-mail boxes, which have sent, received or stored illicit multimedia files containing child abuse and child pornography. They include the date, precise time, and Czech IP address, the number of illicit files, user registration data (if available) and offer to request evidence. This function, however, is not yet automated.

As for other statistics (crimes under points (b) and (c)), their presentation is problematic. Out of the total data, it is not possible to separate / identify offences committed via the internet and other communication technologies (such as crimes in cyberspace), because such distinctions are absent from the statistical sheet. The ESSK police system is currently under development and concrete proposals are being considered to make possible more accurate reporting and monitoring of criminal activities in cyberspace. From 2016 onwards, it will, therefore, be possible to add a relevant distinctive character in the statistical sheet to specify whether a particular offence involved use of the internet (a monitored circumstance of the criminal offence).

During the evaluation visit the national authorities informed the evaluation team that cyber-incidents had been rising very steeply in recent years. They mentioned reasons such as the great ease of cross-border activity and that sometimes people do not even know that they have become victims of cybercrime. In recent years, thanks to national authorities' efforts, people have become more aware, and reporting is also rising. Victims can easily report illegal activities; since August 2012 hotlines managed by experts have been in place, where many reports of suspicions of cybercrime are received.

There is also a pro-active approach on the part of the national authorities to detecting cybercrime incidents, in order to reduce the number of cases.

However, there is a rise in fraud, the most usual type being the creation of e-shops which offer goods for low prices and ask people to pay in advance. Another phenomenon is internet banking attacks; the national authorities also mentioned that some phishing pages are very sophisticated and can mislead people.

The other main trends mentioned were: attacks through social networks to collect data, identity theft and cyberbullying, blackmail, extortion and malware.

Concerning statistics, it should be mentioned that in the Czech Republic two parallel systems are operated by the police, namely ESSK and ETR. Prosecution offices and courts also collect statistics. However, data regarding child sexual exploitation material and sexual abuse of children are not kept separately, but included in a larger category of offences, called 'vice crimes' along with other offences including trafficking of human beings, prostitution, etc.

Statistical data are collected by the Czech police via the ESSK and ETR. As mentioned in the questionnaire, the presentation of statistics on the crimes of production, distribution and other handling of child pornography in cyberspace and other criminal offences committed via the internet and violations of intellectual property rights is problematic. It is not possible to separate or identify offences committed via the internet and other communication technologies because such a distinction is absent from the statistical sheet.

3.4. Domestic budget allocated to prevent and fight against cybercrime and support from EU funding

There are no specific budget resources allocated to preventing and combating cybercrime. However, the resources allocated are included in the budgets linked to the fulfilment of the government's priorities and the required resources for the police of the Czech Republic. It is planned that EU funding to combat cybercrime be used.

A request for funding from the Internal Security Fund – police section (ISF – P) – for the development of the new cyber unit has recently been submitted (approximately CZK 167 million). Therefore, over the coming years, approximately 195 systemised service positions should be created (within both national and regional units).

3.5. Conclusions

- In February 2015 the Czech Republic adopted the second National Cyber Security Strategy, which builds on the main trends of the previous one. At national level there is continuity in preventing and combating cyber security incidents, as well as cybercrime, and this fact highlights current interest in this field.
- The Strategy is accompanied by the Action Plan, adopted immediately after the Strategy, in May 2015, which establishes many specific targets as well as the institutions responsible.
- CZ seems to have reached a high level in terms of cyber security prevention and response. Particularly interesting is that CZ was the object of DDoS cyber-attacks in March 2013 which prompted a reaction that led to the creation of a more structured approach in cyber-defence/cyber security.
- The CZ National Security Authority has just launched the project 'Digital Footprint' as a preventive tool for children. The main scenario concerns an incident or crime committed against a child, e.g. extortion for illicit pictures of a child, spreading personal data etc., and children have to investigate or discover what actually happened. As a more concrete storyline: young girls posted some sensitive pictures on social networks, and the detectives (children) had to search for relevant data and understand the situation so as to avoid becoming victims in reality. The concept is known as 'learning by doing'.
- The CZ National Security Authority performs prevention and awareness activities for its internal personnel and for public administration personnel, e.g. establishing and implementing security standards, making learning models for public administration (online courses, setting basic administration rules, public communication, basic cyberspace topics, socio-political topics for IT staff at embassies, etc.).

- Statistics are collected by LEAs, prosecution offices and courts. However, a more coordinated approach could be very useful for a clear picture of the dimensions and characteristics of cybercrime, especially for child sexual exploitation cases, which could be reflected in separately in data collected for statistical purposes.
- The statistics on information exchange relating to relevant cybercrime areas are quite difficult for the evaluation team to understand, especially as regards counting notifications named as 'child pornography and abuse notifications' and 'CAM notifications' as two different entities, while the content of both entities deals with the same matter. As the team understood it, the police statistical system is under development and the specific changes to be introduced should give adequate results even for different cybercrimes. This decision is welcomed and supported by the evaluation team.
- The national authorities do not allocate a specific budget line for preventing and fighting cybercrime. These activities are carried out using the ordinary budget of the LEAs. During the evaluation visit, the national authorities expressed the intention of making better use of EU funding for combating cybercrime. It is understood that the police are doing their best in prevention and combating cybercrime; on the other hand, the police are not the only stakeholders to be encouraged to receive a specific budget for preventing and combating cybercrime in various areas (cyber-attacks, cyber-fraud with payment cards, child sexual exploitation online) — the government should also take further steps in raising awareness in the CZ community, professionals, institutions and NGOs, and should maintain a significant budget for the purpose, including projects run in close cooperation with various population groups and institutions.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1 Internal structure

A system of Public Prosecutor's Offices (prosecutors) and the courts (in competence of the Ministry of Justice), which also target cybercrime when taking over the results of the police investigation; effective and timely sanctions also have an impact on the prevention of cybercrime and on increasing legal awareness in this field; jurisprudence is gradually being developed by decisions that can support a proper and accurate interpretation of existing laws or help to generate the necessary impetus for amendments of the law in the future. Their injunction, permitting and supervisory function is also very significant, in cases of serious violations of rights and freedoms of citizens or breaches of confidentiality, and also in gathering evidence linked to cybercrime.

Criminal offences in the area of cybercrime are dealt with by the courts of general trial jurisdiction and the Public Prosecutor's Offices; however, they do not have any special powers as regards cybercrime. Related provisions:

Exercise of criminal justice by courts:
Jurisdiction in criminal matters is exercised by district courts, regional courts, high courts and the Supreme Court.

Exercise of criminal justice by Public Prosecutor's Offices:

The Prosecutor's Offices are organised to mirror the organisation of the courts.

Under Section 7 of Act No 283/1993 Coll. on the Public Prosecutor's Office:

Seats and competence districts

(1) The seats of the Public Prosecutor's Offices and their competence districts correspond to those of courts.

(2) The Public Prosecutor's Office is responsible for representing the state in the court at which the Prosecutor's Office operates unless a special regulation stipulates otherwise.

The Prosecutor's Office appears to have been actively involved in pooling expertise among prosecutors in CZ. It has set up a national network of cybercrime prosecutors (consisting of nearly 20 specialists), which has recently been 'formalised' by decision of all the chief public prosecutors. The team was informed that a national correspondent for cybercrime will also be added to the Eurojust National Coordination System. In addition, the team were provided with a copy of an opinion issued by the Supreme Prosecutor's Office (File No 1/2015) entitled '*Opinion unifying the interpretation of laws and other legal enactments regulating the issue of seizure of mobile phones and other data carriers, including the contents of e-mails*'. The team was also given a presentation on best practices in CZ when dealing with international cooperation in criminal matters. Reference was made to issues encountered by CZ as requested/executing country, when the requesting authority needed to send requests to several authorities in the same state. As a solution, national authorities referred to coordination meetings at Eurojust, the use of EJN, and the fact that ultimately CZ changed its system. In general, the outcome is that only one judicial authority (prosecutor's office in pre-trial proceedings, court in trial proceedings) is responsible for the execution of a MLA request, even if evidence has to be gathered in different districts in CZ. A template for a '*Model request for legal assistance consisting in requesting information on telecommunications traffic, including the contents of communication*' with the USA was also handed out and presented. The form was drafted by the International Affairs Department of the Prosecutor's Office and competent US authorities.

4.1.2 Capacity for and obstacles to successful prosecution

The Czech government has adopted the National Cyber Security Strategy for the period 2015 - 2020. One of its priorities is to strengthen cooperation between the law-enforcement authorities and other entities involved in ensuring cyber-security in the Czech Republic.

Existing structures and processes of cooperation in the area of combating cybercrime are being strengthened. The increase in cybercrime, threats and risks associated with the use of social networks on the internet is noted. The strategy expressly provides for and analyses in detail the ability to support the development of the Czech police to investigate and prosecute cybercrime.

On the basis of the main goals of this strategy, a detailed Action Plan that defines concrete steps and deadlines for their implementation and monitoring was drawn up. As part of the annual Report on the State of Cyber Security in the Czech Republic, a report on the state of the implementation of the Action Plan is envisaged, in the form of an annex. The report will inform the government and the general public about the effectiveness of measures adopted and the implementation of tasks defined by the Strategy.

Currently, a reorganisation of the Department of Information Crime, formerly under the Police Presidium is taking place, with the aim of enhancing the capability to combat and prevent cybercrime. The Department of Information Crime was moved under the Unit for Combating Organised Crime of the Criminal Police and Investigation Service on 1 October 2015. Another new department, Department of Cybercrime Investigation and Analysis (V8), within this unit was be established on 1 January 2016, whose aim will be to detect and investigate the most serious crimes in the area of cybercrime. The focus of the Department of Information Crime will then be the development of methodology and support activities to regions; its role as the focal point for international cooperation in this area will continue.

These two departments will be coordinated by the new Deputy Director of the Unit for Combating Organised Crime of the SKPV. As mentioned above, it is planned to establish about another 195 systemised service posts in the future, of which 42 posts will be assigned to the Department of Information Crime and 36 to the V8 group (investigations, operational activities and analysis of cases which will be taken over by the Unit for Combating Organised Crime).

There will also be more posts for the Institute of Criminalistics Prague and the Special Operations Unit - the Institute will be enlarged by 10 people over the next few years (two already recruited in 2015). In connection with the increased allocation of personnel, more effective and intensive training of police specialists is also planned.

The main obstacles to successful prosecution of cybercrime are:

- as yet too few and inadequately trained police experts, on national and international levels;
- the issue of an excessively short period for retention of data on telecommunications traffic, and the fact that many organisations are not obliged to retain data;
- slowness of international cooperation, along with different legislation in individual countries.

The strengthening of the systemised service posts in the police of the Czech Republic, as defined by the management of the police of the Czech Republic and where the total subsidy is based on the Conception of Capability Development of the Police of the Czech Republic to Investigate Cybercrime, is given below. However, there has been a numerical redistribution between the various organisational elements of the police of the Czech Republic.

CYBERCRIME – PLAN FOR ENHANCEMENT OF THE SYSTEMISED SERVICE POSITIONS OF THE POLICE

	2016	**2017**	**2018**	**Total**
OIK ÚOOZ (Department of Information Crime of the Unit for Combating Organised Crime)	6	6	6	**18**
V8 ÚOOZ (V8 of the Unit for Combating Organised Crime)	13	4	3	**20**
KÚP (Institute of Criminalistics Prague)	5	4	1	**10**
ÚZČ	12	6	5	**23**
ÚOKFK (Unit for Combating Corruption and Financial Crime)	1	0	0	**1**
Regional Directorates of the Police of the Czech Republic				
Capital City of Prague	6	3	4	**13**
Central Bohemian Region	6	3	3	**12**
Southern Bohemian Region	3	2	2	**7**
Pilsen Region	3	2	2	**7**
Ústí nad Labem Region	3	2	3	**8**
Hradec Králové Region	3	2	2	**7**
The Southern Moravian Region	6	4	4	**14**
The Moravian-Silesian Region	3	2	2	**7**
Karlovy Vary Region	3	2	2	**7**
Liberec Region	3	2	2	**7**
Pardubice Region	3	2	2	**7**
Vysočina Region	4	2	3	**9**
Zlín Region	6	2	2	**10**
Olomouc Region	3	2	3	**8**
Total	**92**	**52**	**51**	**195**
total departments with national competence	*36*	*20*	*15*	*71*
total Regional Police Directorates	*55*	*32*	*36*	*123*

The table below reflects the material costs of individual components of the police of the Czech Republic in the current year and the years immediately following. Amounts are expressed in millions of CZK:

	2015	*2016*	*2017*	*2018*	*usability*
SKPV PČR	28.298	28.298	28.298	28.298	75% is possible to use further
KÚP and OKTE SKPV	15	5	15	5	25% is possible to use further
Total	43.298	33.298	43.298	33.298	

As regards the prosecution of specific criminal offences, the police sometimes encounter difficulties related to the lack of substantive knowledge of the issues of computer crime or even aspects often related to the transnational nature of this type of crime on the part of some public prosecutors and judges, which may be considered natural to some extent (see also question 10.B.7).

4.2. Law-enforcement authorities

Regional Directorates of the police of the Czech Republic operate in individual regions, which are the territorial administrative units of the Czech Republic. There is also an Information Crime Unit (which is a part of the Analytical Department of any regional SKPV) in each Regional Police Directorate; specialists in investigations of cybercrime operate within these units.

Regional Police Directorates are further divided into smaller territorial units (Territorial Departments), where information crime groups are based (usually one police officer, a specialist in cybercrime investigation).

Methodologically, investigation, preventing and combating cybercrime are covered by the Department of Information Crime of the Unit for Combating Organised Crime of the SKPV. As mentioned above, a new department V8, in charge of the investigation, operational activities, and analysis of specific cases, will be established on 1 January 2016.

Expert departments of the police of the Czech Republic, such as the Institute of Criminalistics Prague and Departments of Forensic Techniques and Expertise of the Regional Police Directorates (OKTE), which address both expert examinations and expert evaluation of traces (evidence) and, for the purpose of the forensic/technical activities of the police of the Czech Republic, activities related to such traces, also belong to these authorities.

Then there is the system of Public Prosecutor's Offices and courts of general trial jurisdiction, organised in basically the same way in the following levels:

- The District Court and the District Public Prosecutor's Offices represent the lowest constituents, their powers established by a group of municipalities (or neighbourhoods in larger cities); they act as the first instance in less serious cases.
- The competences of Regional Courts and Regional Public Prosecutor's Offices are bounded by regions, the basic units of territorial administration; they function as the second-instance authorities in less serious cases and as the first-instance authorities in more serious cases (where the law sets a minimum length of custodial sentence of at least five years) or in complicated cases (insider trading, breach of international sanctions, organ trafficking, etc.).
- The High Court and the High Public Prosecutor's Offices (one in Prague for the western part of the country, one in Olomouc for the eastern part of the country) act on appeal in more serious cases heard at the first-instance stage by the regional courts.

The Supreme Court, in certain cases specified by law, assesses second-instance decisions and unifies the case-law. The Supreme Public Prosecutor's Office may issue general guidelines to unify the activities of public prosecutors and also has substantial powers in international legal assistance during investigation stages.

A specialised body is made up of police officers from Information Crime Units of the Analytical Departments of the SKPV under the Regional Police Directorates and police officers from Information Crime Groups of the Territorial Departments under Regional Police Directorates. Many of them are forensic investigators in the field of information technology.

The police of the Czech Republic have set tasks for the investigation of cybercrime by the National Cyber Security Strategy for the period 2015 - 2020, which was adopted by the Government of the Czech Republic on 25th May 2015 via Resolution No 382.

Currently, a specialised unit is being established within the structure of an existing body (the Unit for Combating Organised Crime SKPV (ÚOOZ SKPV)). ÚOOZ SKPV operates across the Czech Republic and deals with the most serious organised crime. ÚOOZ SKPV also has connections with foreign partners; these contacts are handled by the National Focal Point for Terrorism, incorporated in the current structure of the ÚOOZ SKPV.

A separate section within the Unit for Combating Organised Crime SKPV was therefore established on 1 October 2015: a department for IT and cybercrime. This section consists of the Information Crime Department transferred from the ÚSKPV and an emerging executive department of the ÚOOZ SKPV, to which some investigators and IT experts will be transferred. In the future, the emerging section will be a central executive but also a methodological centre.

The CZ police are engaged in a broader reorganisation, which is related to establishing relevant capabilities and capacities in the cybercrime framework. According to information received, internet penetration in CZ stands at about 80%. It is understood that reorganisation of the police service, which has about 41 000 posts with police officer status and about 20 000 additional support personnel, certainly represents a big project for the country, its law-enforcement agency and its society.

During the evaluation visit, representatives of the Ministry of Interior explained to the evaluation team that the organisation of the police previously included an IT Crime Department of the Police Presidium, responsible for methodological guidelines and international cooperation. However, most cases were investigated at territorial level, with different approaches. A change was necessary for a better coordinated approach in criminal investigations of cybercrime offences and to put into practice a connection between the practical aspects of criminal investigations and the methodological procedures at central level.

According to the national authorities this process of organisational reform included consultations with other Member States such as Austria, Poland, Slovakia and Germany, and a prior analysis in order to provide sufficient skills and competences for combating cybercrime.

The recent new organisation aims to allow to the Organised Crime Unit, as a specialised body, to investigate the most serious cybercrime offences. This new arrangement will enter into force from 1 April 2016. Competence for cybercrime offences will be then shared between the Organised Crime Unit at the central level and the territorial units.

The Organised Crime Unit will include the Cybercrime Department and the department of cybercrime investigation and analysis.

The Cybercrime Department will offer methodological guidance to the local level and will manage international cooperation and training.

In addition, from 1 April 2016, the Cybercrime Investigation and Analysis Unit will be in place as well, with responsibility for conducting criminal proceedings at the Organised Crime Unit for attacks on critical infrastructure and cybercrime attacks that have an impact on the whole of society. That unit will provide technical assistance to the territorial cybercrime units.

Special attention is being paid to the recruitment of new staff, as already planned. The representatives focused on police officers with technical skills which they plan to provide through training.

During the evaluation visit the representatives of the Cybercrime Unit of the SKPV Regional Directorate of the Police of the Southern Moravian region presented the current situation, as well as the future reorganisation of the unit.

Currently, the unit performs criminal investigations into offences such as advertisement fraud, identity thefts, fraudulent e-shops and Facebook phishing. It also engages in technical cooperation, e.g. in securing of and access to data, operational analysis, technical consultations and support to other territorial units.

Police representatives highlighted good cooperation with specialised cybercrime prosecutors in solving cases.

The specialised police unit makes technical analyses, which produce evidence accepted by the courts. They also support other police units by securing data, and this is also a form of evidence according to the law.

Within the Police Presidium there is an International Police Cooperation Division, which has four units: information exchange and international search, general exchange of information, non-operational cooperation and foreign missions. This division does not perform operational work, but handles communication with foreign counterparts, such as Interpol and Europol (FP Cyborg within EC3), and takes part in different platforms and tools, like EPE (European Platform Experts).

The Czech Republic is not yet involved in the EMPACT project dealing with cybercrime issues, but the decision on joining it could be reconsidered.

Within specialised authorities, there are positions allocated for forensic activity in the field of information technologies at the Institute of Criminalistics Prague and OKTE.

The 24/7 operational contact point for urgent requests is a structure of operational officers of the Regional Directorates of the police of the Czech Republic, providing a continuous service and making possible the immediate reception and investigation of any notification. There is also a permanent service at the Department of International Police Cooperation of the Police Presidium of the Czech Republic.

The Information Crime Department of the Unit for Combating Organised Crime of the SKPV (published in the Council of Europe Convention on Cybercrime) serves as the international focal point.

When a request is received, there are no specific procedural measures established - telephone, fax and e-mail connections are disclosed, and requests are processed according to their content.

4.3. Other authorities/institutions/public-private partnership

As regards national authorities involved in preventing and combating cybercrime standing outside of judicial and law-enforcement authorities, these are:

- a system of schools, NGOs and the Ministry of the Interior of the Czech Republic - the area of prevention;
- projects of some major telecommunication companies and server service providers - the area of prevention;
- The national CERT, GovCERT and other CSIRT / CERT teams (there are 22 teams currently listed in Trusted Introducer and more are being established);

GovCERT, operating within the National Cyber Security Centre, a part of the National Security Authority, is responsible, within its competence as conferred by Act 181/2014 Coll. on cyber security, for resolving incidents within critical infrastructure systems and important information systems. From this position, it can help detect cybercrime directed against members of their constituency and therefore works with law-enforcement authorities as well as with other relevant bodies. It also provides ad hoc consultations regarding analysis of cybercrime; this component of its activities will be strengthened in the future with the planned development of an expert department for forensic analysis. To a limited extent, the national CERT may also be considered as an authority on which the Act on Cyber Security imposes certain obligations on the basis of a contract governed by public law.

The primary task of both institutions, however, is to ensure cyber security, rather than to fight cybercrime.

- administrator of the national TLD CZ.NIC domain (see national CERT);
- The Czech Telecommunication Office.

The Czech Telecommunication Office is also an administrative authority and can impose coercive measures and fines if the Act on Electronic Communications and instructions of the Office under this law is not complied with; GovCERT has similar powers, but these arise from the law on cyber security; other authorities have no powers except the administrator of the CZ.NIC domain - a domain may be blocked, but only on the basis of a court decision, or provisionally.

The Czech Republic does use Public-Private Partnership (PPP) in preventing and combating cybercrime. There is a whole range of projects that aim to disseminate information and prevention with regards to users, but also organisations, with the aim of raising knowledge and awareness of the issues of cyber security and cybercrime.

An important role is played by the Ministry of Education – from primary schools to universities. The police of the Czech Republic, judicial authorities and government agencies participate in lectures, conferences and workshops. The National Cyber Security Strategy for the period from 2015 to 2020 is also very important in this regard, as it directly assumes and establishes cooperation with the private sector.

The main objectives are to:

- cooperate with the private sector;
- continue engaging in cooperation with the private sector and raise awareness of the work and activities of the National Security Authority in cyber security;
- develop, in cooperation with the private entities, unified safety norms, standardise cooperation and establish a mandatory level of security for operators of critical information infrastructure;
- ensure, in cooperation with the private sector, that cyberspace provides a secure environment for sharing information, research and development, and provide a safe information infrastructure that stimulates private enterprise with the aim of promoting the competitiveness of all private businesses in the Czech Republic and protecting their investments;
- educate and raise awareness in the private sector of cyber-security issues and provide necessary guidance to private entities on appropriate behaviour, not only in emergency situations, i.e. cyber-incidents, but also in everyday activities.
- raise confidence between the private sector and the state, including through the creation of a national platform/system for sharing information on threats, incidents, and actual situations of insecurity.

At the moment, the National Security Authority is not implementing any specific form of PPP. However, cooperation takes place on an ad hoc basis within the framework of specific projects. The National Security Authority cooperates closely with the CZ.NIC association, which serves as the National CERT, and also, for example, with Microsoft in connection with operating the Botnet Feed tool, and with the Czech Banking Association. The Action Plan for the Cyber Security Strategy assumes further deepening of cooperation, including on research projects.

During the visit the evaluation team had the opportunity to visit Masaryk University's Institute of Computer Science in Brno, and the Czech Cybercrime Centre for Excellence (C4E).

CZ Masaryk University in Brno is engaged in raising awareness, including through training courses on law and technology (organised by the Law Faculty, Institute of Law and Technology).

The Team also visited CSIRT-MU, i.e. the Computer Security Incident Response Team of Masaryk University. CSIRT-MU is part of the Institute of Computer Science, which is responsible for the development of information and communication technologies at the university.

The Czech Cybercrime Centre of Excellence (C4E) was also presented. It brings together top Czech experts from academia, the Czech police, private digital forensic laboratories, NSA, justice, prosecution and other areas and individual experts. It is active in education, training, research and development on cybercrime, covering a wide range of issues, including law and technical development.

The evaluation team attended a practical demonstration of the KYPO project, which aims to provide a unique environment for research and development of new methods for protecting critical infrastructure against cyber-attacks in CZ. It operates within a cloud infrastructure, aiming to detect threats and 'visualise' them. It also facilitates exercises of forensic analysis and network simulations that help making CZ better able to cope with cyber-attacks. They ran a nationwide cyber-exercise in 2015, called Cyber Czech 2015, where four teams were involved in a simulated cyber-attack. One of the teams engaged as the 'legal team' (the White Team) was also covering legal aspects of defence against cyber-attacks.

Additionally, the same centre has produced some extremely helpful material, such as the Guidebook on Digital Evidence in Criminal Proceedings (in CZ), and a book on interception and data retention (in EN) published with the Max Planck Institute.

The evaluation team also appreciated the presentation by and dialogue with the Director of National Centre for Safer Internet. The Centre carries out a vast range of activities aiming at raising awareness. Particularly interesting is that it also works to raise awareness among seniors, for instance by launching the Senior Safe Online campaign in 2015, using a sort of peer-to-peer system to spread awareness of possible frauds, including social engineering and other similar practices. They have also organised competitions in schools in which children have to draw a cartoon to illustrate a certain topic pertaining to cybercrime, and prizes (sponsored by private companies) were given. They have newsletters for schools, municipalities and other readerships, and they have also appeared on TV. They also receive reports on suspicious activities (averaging about 43 per month), and if an initial assessment reveals a criminal dimension, they report directly to the police (around 10 to 15 cases per month).

The three most frequent problems encountered are attacks from fake profiles on Facebook, abuse of real FB profiles and technical issues (e.g. need to retrieve access codes). As to cyber-bullying, they focus on prevention and try to explain how to use social networks properly. They also referred to Facebook as particularly cooperative on these activities. Awareness-raising activities are also carried out in partnership with the police. Particularly interesting was the training initiative on the dark net to enable teachers to engage in fruitful discussion with children rather than refusing any confrontation with them.

4.4. Cooperation and coordination at national level

4.4.1 Legal or policy obligations

The National Security Authority (NBÚ), which plays the role of coordinator on cyber security as well as being the national authority in this area, as identified in Government Resolution No 781 of 19th October 2011, is another key body in the structure. Under the Cyber Security Act, it also exercises supervision over the Critical Information Infrastructure and Important Information Systems. Since September 2012, the National Security Authority has operated the National Cyber-Security Centre (NCKB) in Brno, which carries out activities of the governmental CERT (GovCERT) and is also a coordination point for immediate response to cyber-incidents within the relevant important information systems of the government administration and the critical information infrastructure. It has been fully operational since 2015. Within NCKB in Brno, there are also liaison officers of the police of the Czech Republic, who deal with recorded incidents from the perspective of cybercrime.

Other NCKB activities include awareness-raising and support for educational and training activities in the field of cyber security, as well as research and development in this field. In addition, the Centre's tasks also include international cooperation with relevant persons and bodies in cyber security field.

The Ministry of the Interior of the Czech Republic (MOI), to which the police of the Czech Republic are subordinate, is responsible for the methodological management of the police and plays an important role in crime prevention. The EU Information Society agenda, Digital Agenda for Europe (as one of the main initiatives of Europe 2020), also falls within the MOI's remit, in particular the section on the fight against cybercrime. In addition, it also involves prevention, e.g. the Safer Internet programme.

The Ministry of the Interior has adopted the Strategy to Combat Organised Crime, which also deals with cybercrime perpetrated by criminal groups, and defines cooperation with Europol's EC3.

A system of Public Prosecutor's Offices (prosecutors) and the courts (in the competence of the Ministry of Justice) also target cybercrime when taking over the results of police investigations; effective and timely sanctions also have an impact on the prevention of cybercrime and on increasing legal awareness in this field; jurisprudence is gradually developed by decisions that can support proper and accurate interpretation of existing laws or help to find the necessary impetus for future amendments of the law. Their injunction-issuing, permissive and supervisory functions are also very significant – in cases of serious violations of rights and freedoms of citizens or breaches of confidentiality, and also in gathering evidence linked to cybercrime.

The Ministry of Industry and Trade of the Czech Republic is in charge of regulation of electronic communications including data retention and, therefore, may significantly contribute to the fight against cybercrime by proposing relevant legislation on duties of providers.

The private sector is generally not obliged to report cyber-attacks. However, there are companies whose size and importance brings them within the scope of the cyber security law (because they are part of the critical infrastructure or manage major information systems), and in these cases they do have such an obligation. They fulfil it by reporting security incidents to GovCERT, which has a form detailing the extent and structure of such reports, including the required communication channel.

Act No 181/2014 Coll. on Cyber Security assigns specified subjects various degrees of responsibility in dealing with security incidents, including the obligation to inform GovCERT, if they are a part of the critical infrastructure and major information systems (MIS).

Some subjects are obliged to report incidents to the national CERT. These subjects have to report incidents (which include attacks); they report the actual incident as well as the manner in which it was handled. Incidents are reported via a form (electronic and paper versions; some circumstances allow reporting via telephone); in the future an automated online tool should become available. The minimum extent of reports is set out in Annex No 5 of Decree No 316/2014 Coll. on cyber security, and includes inter alia the level of protection of information provided, the identification of the subject, the details of the incident – time, category, and type of incident, the current state of response to the incident, the number of systems attacked and users affected, a description of the incident, and system details of the incident. In the future, the scope of the reports should expand, in order to better reflect the needs of concerned parties.

Sec. 21 of the Act on Cyber Security defines the state of cyber-emergency as a sui generis emergency situation in cases where the attack cannot be managed by standard means and the safety of the Czech Republic could be compromised. The mechanism for coordination reaction to serious cyber-attacks functions mainly on the basis of ad hoc cooperation between the national CIRT, GovCERT, the police of the Czech Republic, intelligence agencies, and the army.

In situations of cyber-emergency, the relevant stakeholders and entities have specific obligations and responsibilities according to national legislation. This includes National Security Authority/GovCERT, the national CERT, KII and VIS administrators, as well as key actors from the private sector. The exact procedures for the field of cyber security are currently being drafted. The generic plan will serve as a methodological tool for developing specific plans by individual subjects.

The biggest local peering centre, NIX.cz, is an important player in this field, as it oversees a large part of internet connectivity in the Czech Republic. It was within this organisation that the FENIX project was initiated, uniting the biggest local telecommunications companies, hosting companies and service providers, as well as some subjects from Slovakia. In the event of a massive attack from abroad, the project is capable of maintaining at least the basic functions of the internet. Its members operate trusted networks and can, if necessary, filter out foreign traffic.

Cooperation between industry, banks, the private sector and LEAs to prevent and fight online card fraud exists and is sufficient. The general objective is to prevent and combat internet fraud with payment cards.

A certain unwillingness on the part of financial institutions is evident - the banking business has always been based on trust; according to banks, publication and media coverage of security incidents, assaults and similar incidents is not good for the credibility of the institution concerned.

As regards the detection of abuse of new payment instruments, the police usually have the necessary information.

Security of cashless payments is gradually increasing; the usability of magnetic-strip cards is decreasing. In Europe, the Czech Republic is in the vanguard as regards contactless payments. There are also abuses of contactless payments not requiring a PIN code (limit of payments to CZK 500); in the case of card misuse, the overall damage is negligible.

Since the banks' initial reluctance to tighten verification of online transactions, the situation has improved. At the moment, at least two-factor authentication is used by all banks and internal software has gradually also been deployed. It allows suspicious transactions to be monitored and blocked in a timely manner.

Telecommunications operators and providers are primary partners, who often supply information that is used to combat cybercrime. However, only subjects that operate on the basis of the Act on Electronic Communications are obliged to retain and provide information; because some civic associations and other organisations, whilst de facto providers, are not obliged to retain information, it would be desirable to widen the circle of these subjects. As mentioned above, the data retention period is too short. In particular, large companies providing server (and also e-mail, chat, dating, etc.) services cooperate unwillingly with law-enforcement authorities and look for ways not to provide information or to limit its scope. At the same time, they proclaim their interest in working for a 'safer internet' and combating cybercrime. Their attitudes and actions are ambivalent. On the other hand, no problems are usually encountered when removing illegal content. The CERT/CSIRT teams – whether national, governmental, set up by universities, providers, banks – are a significant help in combating cybercrime.

They operate continuously and have trained staff whose members, in case of a cyber-attack, are able to take action, take control of the security incident, and cooperate during the investigation, helping to secure evidence. It would be impossible to detect, or to solve, certain cybercrimes without their help. Nevertheless, GovCERT does not have the powers of law-enforcement authorities vis-à-vis private subjects. With the exception of emergency situations defined by law (essentially cyber-emergency situations), it cannot impose obligations on private subjects beyond those defined by the Act on Cyber Security and its implementing regulations. Therefore, when resolving incidents it largely relies on trust within the community, which it is constantly working to strengthen.

Cooperation from the bank sector could be more effective and more intense in combating and preventing cybercrime. As already indicated, it seems to fear negative publicity. It is, however, necessary to respond to cases from recent years, where perpetrators circumvent the two-factor authentication of payments, e.g. by taking control of mobile devices.

As regards the banking sector, there are at least two acts that oblige banks to retain personal data. These are Act No 21/1992 Coll. on banks, as amended (Act on Banks) and Act No 253/2008 Coll. on some measures against the legalisation of proceeds from crime and on the amendment of related acts, as amended (Act on Money Laundering).

Under Sec. 21(2) of the Act on Banks, a bank, as well as a branch of a foreign bank, is obliged to register transactions relating to a client's bank account and transactions relating to an account of a bank or a branch of a foreign bank within the accounting department. Banks and branches of foreign banks are obliged to retain transaction records for at least 10 years.

The Act on Money Laundering lays down rules on how bank clients must identify themselves (Sec. 5). For natural persons, the identification data include the name (or all names) and surname, birth registration number or date of birth, sex, and permanent or other residence addresses, followed by verification of the data provided against their identity card. Furthermore, it involves verification of the correspondence of their appearance with the photograph on the identity card, as well as verification of the identity card number, its expiry date and the issuing authority or state.

As regards natural persons engaged in business activities, the data also include their company information, differentiating addenda or other indications and identification number. However, such identification is only required at particular types of businesses.

The obligation to retain that information is set out in Sec. 16 of the Act on Money Laundering, which imposes an obligation to retain specified data, as follows:
The obliged entity shall, for the period of 10 years after the transaction or after having terminated its business relationship with the customer, keep a record of all data and documents on transfers requiring identification.

The obliged entity stipulated […] shall keep a record of all data and documents for the period of at least 10 years after the transaction or after having terminated its business relationship with the customer should such transaction or relationship reach or exceed EUR 10 000; in other cases it shall keep its records for a period of 5 years.
The statutory period […] shall commence on the first day of the calendar year following the calendar year in which the obliged entity performed the last transaction.

In 2014, the Court of Justice of the European Union ruled that Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.

The data to be retained pursuant to Directive 2006/24/EC are the so-called traffic and location data and related data necessary to identify subscribers or users. Traffic and location data also include information on internet access, internet telephony, and internet e-mail. They include e-mail addresses of senders and recipients and also IP addresses of source and destination devices. The purpose of the directive, according to the preamble, was to harmonise the Member States' regulations as concerns the obligation of electronic communications providers and public communication networks to retain traffic and location data with the aim of ensuring the availability of these data for the purposes of the investigation, detection, and prosecution of serious crime.

Even after the abolition of this Directive, retention of data is provided for by the Act No 127/2005 Coll. on electronic communications, as amended, and by Decree No 357/2012 on the retention, transfer, and disposal of traffic and location data of the Ministry of Industry and Trade, which was issued in accordance with provisions of Sec. 150(3) of Act No 127/2005. Conditions for accessing these data in criminal proceedings are set out in Sec. 88 (a) of the Code of Criminal Procedure (see above). All these norms were reviewed, as regards protection of privacy and personal data, by the Constitutional Court, and subsequently partly cancelled and re-adopted in modified form to comply with its requirements.

Sec. 97 (3) of the Act on Electronic Communications obliges operators of public communication networks and publicly accessible electronic communication services to retain traffic and location data that have been generated or processed in the provision of their services for six months.
The Act on Electronic Communications thus regulates the manner in which traffic and location data are retained and specifies the range of entities that may have access to them provided they comply with further conditions. These conditions are defined by Act No 141/1963 Coll., the Code of Criminal Procedure, Act No 273/2008 Coll. on the Police of the Czech Republic, Act No 154/1994, Coll. on the Security Information Service, Act No 289/2005 Coll. on Military Intelligence, and Act No 15/1998 Coll. on supervision in the field of capital markets.

For the purpose of providing information to law-enforcement authorities, Sec. 88 (a) of the Code of Criminal Procedure sets out specific restrictions so that data on telecommunications traffic could be used as evidence in criminal proceedings and specifies the range of crimes for which this data may be requested.

The Act on the Police of the Czech Republic (Sec. 66(3)) gives the police the authority to request traffic and location data 'for the purposes of initiating a search for a specific wanted or missing person, establishing the identity of a person of an unknown identity or of a corpse, preventing or detecting specific threats in the field of terrorism or the vetting of protected persons'. The police can request remote and continuous access to traffic and location data from providers of public communication networks or publicly accessible electronic communication services. In this regard, the law does not require any licensing regime, and the only limitation on police access to data requested in terms of the abovementioned purposes is the obligation to retain identification information on the police department or the officer who requested the data and the reasons for which they did so. Operators and providers of such registers are obliged to maintain their contents in confidentiality, although the information is to be retained for five years.

4.4.2 Resources allocated to improve cooperation

The software and hardware of the law-enforcement authorities are at the minimum level necessary to ensure operational capability, as well as capacity and knowledge; it would therefore be appropriate to reinforce their resources, including the Institute of Criminalistics Prague and OKTE.

In particular, it is necessary to strengthen human resources — the numbers of police officers who deal with cybercrime — and to enhance the education of specialists already involved. This applies to police officers involved in the fight against cybercrime as well as those from economic crime departments and units with republic-wide competence, especially UOOZ.

It is also necessary to further strengthen international police cooperation (according to some findings, payment card fraud is typically carried out by foreign gangs). It would be appropriate to introduce a targeted monitoring of hidden or 'grey' areas of the internet, where business with data enabling payment card fraud occurs.

Raising awareness among parties concerned with cyber security can improve the security of e-shops, retailers' servers and payment gateways, all potential targets holding theft-prone payment information.

Finally, by intensifying routine patrols by the public order and traffic police services (which also includes raising awareness among the public), criminal activities such as 'skimming' (copying of payment card data) may be reduced - technical equipment will not be installed by criminals on cash machines, etc.; such equipment may already be detected during transfer, criminals sometimes remain near cash machines and wait for information detected from payment cards. Police officers investigating this criminal activity must be equipped with conventional but powerful (portable) computers supplemented by high-quality internet connections. It is also appropriate to use mobile technology (mobile phones, tablets), again accompanied by the option of high-quality internet connections.

As regards software, this includes standard Microsoft Windows operating systems, a forensic version of the Linux operating system (e.g. DEFT, CAIN), forensic examination and evaluation software (e.g. EnCase, FTK, Belkasoft Evidence Centre, X-Way Forensic, R-Studio Network, etc.). Software, such as UFED, XRY, Oxygen, and MobilEdit! is used for the analysis of mobile devices; however, there is insufficient provision of these programs. Police analysts need such tools; at the moment, they are equipped with Analyst's Notebook software. There is a need to increase the number of licences.

The police of the Czech Republic have financial resources earmarked for strengthening/improving cooperation with the private sector; this mainly concerns acquisition of technical equipment for monitoring and tracking telecommunications or data traffic. In case of need, the police of the Czech Republic have the technical equipment, human, and financial resources.

The National Security Authority has no special financial resources intended for cooperation with the private sector in its budget. Strengthening and improvement of cooperation with the private sector are being implemented across the board within specific areas.

4.5. Conclusions

- The setting up of a national cyber-prosecutors' network is a best practice to be shared among Member States.
- The appointment within the Eurojust National Coordination System of a 'national correspondent for cybercrime' is a good example that should be taken into consideration by other Member States.
- The model request template drafted with US authorities to facilitate gathering of evidence is also considered a good practice by the evaluation team and could be shared with other Member States.

- While it is remarkable that CZ took the initiative to thoroughly reform its police so as to guarantee a national approach, in particular for the detection of cybercrime cases, the evaluation team awaits further developments in this regard with interest. In particular, the team would be interested to see if this department can detect cases of cybercrime that are serious, but not necessarily perpetrated by organised criminal groups.
- The Institute of Computer Science, Brno and the Czech Cybercrime Centre for Excellence (C4E) should consider disseminating an extract in English of the Guidebook on Digital Evidence in Criminal Proceedings.
- The Institute should continue organising Cyber Czech exercises, and also consider inviting other Member States to take part in these exercises.
- The national authorities should continue to support the very useful work of the National Centre for Safer Internet NGO and other initiatives, particularly in partnership with the police.
- The national authorities should consider establishing professional expert groups from different national bodies and institutions where they can meet and discuss cybercrime threats and other related topics in a safe/secured environment.
- In the area of responding to various cyber-threats (in order to respond properly on cyber card frauds and cyber-attacks), a good option should be to establish a standing committee with representatives from law enforcement, banks and other financial institutions, internet service providers, judicial bodies and other relevant stakeholders, to exchange information on trends, threats and *modus operandi* of perpetrators.
- GovCERT is part of the National Cyber-Security Centre located in Brno. Czech GovCERT operates under the National Security Authority. The CERTs and CSIRT organisations have a strong position in eastern Europe, especially in the V4 countries (currently 22 teams).
- GovCERT has also a Digital Trace project, which is an exercise based on lost pictures; the participants (children) have to find mistakes and hear prevention advice.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on Cybercrime

The Czech Republic deposited the ratification documents for the Council of Europe Convention on Cybercrime on 22 August 2013 (promulgated under No 104/2013 Coll. Int. Treaties). The Czech Republic has also been a party to the Protocol to the Convention on Cybercrime since 2014 (promulgated under No 9/2015 Coll. Int. Treaties). The main reason for a certain formal delay was the need to legally establish the liability of legal persons for conduct defined as criminal, but the national criminalisation and operational cooperation with foreign partners had already been applied long before formal ratification.

5.1.2 Description of national legislation

A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems

According to the Czech legislation, the acts listed in Table 2 are considered to be:
Crimes specific to information systems: **Section 230 (Unauthorised Access to Computer Systems and Information Media)**, **Section 231 (Obtaining and Possession of Access Device and Computer System Passwords and other such Data), Section 232 (Damage to Computer Systems and Information Media Records and Interference with Computer Equipment out of Negligence), Section 180 (Illicit Disposal of Personal Data)**, **Section 182 (Breach of Secrecy of Correspondence)**, **and Section 183 (Breach of Confidentiality of Files and other Private Documents).**

Crimes related to content: **Section 191 (Distribution of Pornography), Section 192 (Production and other Disposal of Child Pornography), Section 193 (Abuse of a Child for Production of Pornography), Section 193a (Participation in a Pornographic Performance), Section 193b (Establishment of Illicit Contacts with a Child), and Section 201 (Endangering a Child's Upbringing).**

Crimes involving computers/information systems as a tool or a target, especially in cases of internet fraud related to credit cards: **Section 209 (Fraud (in connection with Section 120 (Misleading of Persons and Using their Error by the Means of a Technical Appliance)), Section 181 (Infringement of Rights of Another).**

- **Definitions and Penalties**

  See the relevant sections of the Criminal Code

- **Intent / Negligence**

Criminal responsibility for these crimes must be a result of intentional culpability, unless the Criminal Code expressly states that culpability as a result of negligence suffices (Section 13 paragraph 2). This is always specified for particular crimes. (As a typical example, see the words 'even negligently' in Section 180, paragraph 1.) Intent and negligence are defined in Sections 15 and 16 respectively.

- **Mitigating / Aggravating Circumstances**

Aggravating circumstances in general – applying to all crimes:

Section 17
Culpability with Especially Aggravating Circumstances

Section 39
Determination of the Type and Extent of Punishment

Aggravating and mitigating circumstances more specifically:

Section 41

Mitigating Circumstances

Section 42

Aggravating Circumstances

These apply in general and within the limits of sanctions applicable to the offence.

Additionally, there are aggravating circumstances specifically given for each individual crime – they are expressly listed in the definition of the provisions of the crime. These are circumstances that increase the degree of harmfulness of a crime for society and imply using higher sanctions. Typically, the first (or second) paragraph of a section defines the offence and possible additional paragraph(s) provide for higher set(s) of sanctions for particular aggravating circumstances.

- Minimum and maximum penalties:

Minimum and maximum penalties always include specific definitions of crimes; they are not generally given. For an exceptional decrease or increase of a prison sentence, the following apply (for all crimes):

Section 58

Extraordinary Mitigation of a Sentence of Imprisonment

Section 59

Extraordinary Increase of a Sentence of Imprisonment

- Multiple crimes/recidivism:

Section 116

Persisting in a Criminal Offence

Some specific definitions of offences require, for them to be criminal, to be committed repeatedly – in such cases it is always expressly stated. If, in an otherwise specific definition of an offence, the word 'repeated' is mentioned, it is an aggravating circumstance, and is a condition for a higher sentence, and is always expressly stated to be such.

- Incitement, aiding and abetting, and attempt:

Some other forms of criminal cooperation are *Participation, Incitement to Criminal Offence, Approval of Criminal Offence, Favouritism, Non-obstruction of Criminal Offence, Non-reporting of Criminal Offence, Attempt.*

Generally, it can be said that the criminalisation of an attempt is admissible for all intentional crimes (not an option for crimes of negligence).

The preparation of a crime is punishable only if expressly stated in its definition. (As a typical example see Section 209, paragraph 5). Preparation is defined in Section 21.

Sec. 7 of Act No 418/2011 Coll. on the Criminal Liability of Legal Persons and Proceedings against Them stipulates that legal persons are criminally liable for the following offences from the Criminal Code (including offences in the field of cybercrime):

- *Section 182 — Breach of Secrecy of Correspondence;*
- *Section 230 — Unauthorised Access to Computer Systems and Information Media;*
- *Section 231 — Obtaining and Possession of Access Device and Computer System Passwords and other such Data;*

- *Section 232 — Damage to Computer Systems and Information Media Records and Interference with Computer Equipment out of Negligence;*
- *Section 209 — Fraud;*
- *Section 192 — Production and other Disposal with Child Pornography;*
- *Section 193 — Abuse of a Child for Production of Pornography;*
- *Section 193a — Participation in a Pornographic Production;*
- *Section 193b — Establishing Illicit Contacts with Children;*
- *Section 201 — Endangering a Child's Upbringing*

Sec. 15 of Act No 418/2011 Coll. on the Criminal Liability of Legal Persons – types of penalties and protective measures

(1) For offences committed by legal persons, only the following penalties can be issued:

a) abolition of a legal person,

b) confiscation of property,

c) fine,

d) forfeiture,

e) withdrawal of a license,

f) ban from execution of public contracts, participation in concession procedures, or public tenders,

g) prohibition from receipt of grants and subsidies,

h) publication of the judgement.

(2) For offences committed by legal persons, the protective measure of forfeiture may be imposed.

(3) Legal persons can be issued with penalties listed in paragraphs 1 and 2 separately or together. However, a fine cannot be imposed along with forfeiture and forfeiture cannot be imposed along with confiscation of the same property or another property of value.

Furthermore, Czech law also recognises the liability of legal persons for administrative offences (non-criminal liability). It is enshrined, in the field of electronic communications, in Act No 127/2005 Coll. on Electronic Communications, although it only marginally concerns the area of cybercrime (abuse of a client's e-mail address, providing private telephone numbers, breach of technical and information responsibilities, breach of data protection, etc.).

Non-criminal liability of legal persons in the area of cybercrime is also provided for by Act No 181/2014 Coll. on Cybersecurity. However, this act too touches on cybercrime only marginally (breach of safety measures, failure to comply with instructions of the National Security Authority, not reporting incidents).

The Criminal Code does not distinguish between 'serious' or 'large-scale' cyber-attacks and others. However, if a crime causes substantial (or even extensive) damage or a serious disorder, the definition of the offence provides for the possibility of issuing a higher prison sentence or another higher sentence (e.g. Sec. 230 (4)).

Many crimes are thus classified according to the nature and consequences of the conduct, which include severity, scope, and degree of damage caused. Cyber-attacks are primarily punished according to Sec. 230 of the Criminal Code (Unauthorised access to a computer system and data carrier). Paragraph 1 defines a simple overcoming of security measures and gaining unauthorised access to a computer system.

Paragraph 2 defines unauthorised use, damage, deletion, or other damaging activity in relation to computer system data or data carriers, and the penalty is higher.

Paragraph 3 requires that the crime have been committed with the intention of causing damage or limiting the functionality of the system; again, the penalty is higher.

Paragraph 4 requires that the crime have been committed in an organised criminal group or caused significant damage or generated considerable (substantial) gain (at least CZK 500 000), or that a serious disruption was caused.

The fifth, and last, paragraph requires that the crime caused large-scale (extensive) damage or generated large-scale gain (at least CZK 5 000 000).

The degrees of damages are listed in Sec. 138 of the Criminal Code.
Decree No 316/2014 Coll. on Cyber Security classifies cyber-security incidents into three categories according to their consequences and negative manifestations, from less to more serious, for handling purposes. Furthermore, within the crisis management system, there are impact and sectoral criteria for identifying elements of critical information infrastructure, i.e. major information systems. These criteria, however, do not affect the criminal/legal evaluation of specific attacks.

In less serious cases, the initial paragraphs defining criminal offences are applied, e.g. Sec. 230 of the Criminal Code (unauthorised access to a computer system or data carrier, which does not require the offence to have caused any damage) in paragraph 1. When the conduct does not fully cover all elements of definition of any criminal offence (e.g. when no security measures have been overcome during unauthorised access, as none exist), the conduct could still, at least in some cases, be treated as a misdemeanour (administrative offence) against civil coexistence or against property. In such cases, the criminal/legal evaluation often depends on the specific circumstances of the case.

Typical crimes committed using information technologies may also include: *Practice of Unfair Games and Wagers, Money Laundering, Money Laundering out of Negligence, Unauthorised Operation of Lottery and other Similar Gambling, Infringement of Copyright, Rights Related to Copyright and Rights to Databases, Violence against Group of People and Individuals, Dangerous Threatening, Dangerous Pursuing, Defamation of Nation, Race, Ethnic or other Group of People, Instigation of Hatred towards a Group of People or of Suppression their Rights and Freedoms, Spreading of Alarming News, Establishment, Support and Promotion of Movements Aimed at Suppression of Human Rights and Freedoms, Expressing Sympathies for Movements Seeking to Suppress Human Rights and Freedoms, Denial, Impugnation, Approval and Justification of Genocide.*

The legislation on cybercrime is relatively new and for some provisions there is as yet not enough applicable case-law. Recently, EU directives and Council recommendations have been implemented, and the Council of Europe Convention on Cybercrime has been ratified. For this reason, we do not feel the necessity to amend existing legislation or to introduce new legislation.

In the future, it would be appropriate to consider whether the legal protection of children and minors on the internet could be enhanced, especially in connection with the development of social networks and electronic communication as a whole. It would also be useful to consider a more accurate definition of prosecuting DDoS cyber-attacks.

There is a lively discussion about existing legislation on data retention. In our opinion, the retention period in the Czech Republic is too short (six months), and the circle of subjects required to retain data could also be widened because a number of subjects not covered by the law are de facto communication service providers.

Extending the data-retention period would not help national investigations so much as enable the Czech law-enforcement authorities to respond effectively to requests from abroad. In many cases, other countries take too long to find reasons for addressing the Czech Republic and to file a request. The Czech Republic is, of course, aware of the need to carefully consider any further action in this area in terms of respecting fundamental human rights and freedoms, especially the right to privacy and protection of personal data.

The planned proposals for amending regulations in the field of cybercrime are given by the legislative programme of the government and are also discussed within the National Security Council.

Directive 2013/40/EU on attacks against information systems has been implemented, especially in Act No 40/2009 Coll., the Criminal Code, as crimes of unauthorised access to a computer system or data carrier (Sec. 230) and procurement and possession of access instruments and passwords to a computer system and other such data (Sec. 231)], and in Act No 418/2011 Coll. on the criminal liability of legal persons and on proceedings against them.

There were no difficulties registered during the implementation.

B/ Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography

The Directive is implemented particularly in Act 40/2009 Coll. – the Criminal Code, in the area of trafficking in human beings and the fight against child sexual abuse, including the punishment of production and possession of child pornography.

The Criminal Code was also supplemented by the criminal act establishing illicit contacts with a child, so-called grooming (Section 193B). Section 7 of the Act on criminal liability of legal persons and proceedings against them was supplemented by additional offences, for which a legal person may be prosecuted, since the directive expressly provides that the Member States shall take all necessary measures to ensure that legal persons may be held liable for offences referred to in Articles 3 to 7 of the Directive, i.e. sexual abuse, sexual exploitation of children, including the production and possession of child pornography, and rape.

C/ Online card fraud

Corresponds with point 6.1 and 6.2 of the questionnaire

Such cases are reported ordinarily and are checked subsequently; latency is not anticipated. Reporting of such cases does not differ from reporting of any other offences or other unlawful behaviour. If a victim (a natural person or a representative of a legal person) detects a payment card fraud, they must either contact the police (in person, in writing, by telephone, etc. - every police station is obliged to accept such notification) or contact their bank, which usually recommends, or even requires, that a complaint be filed with the police. Reporting is usually followed by procedural steps - interrogation, instruction, obtaining evidence, or even money (if applicable), and the results will determine further action.

Cooperation between industry, banks, private sector and LEAs exists and is sufficient. The general objective is to prevent internet fraud with payment cards and fight against it.

A certain unwillingness of financial institutions is evident - the banking business has always been based on trust; according to banks, publishing and media coverage of security incidents, assaults and similar incidents is not good for the credibility of the institution concerned.

As regards the detection of abuse of new payment instruments, the police usually have the necessary information.

Security of cashless payments is gradually increasing; the usability of magnetic-strip cards is decreasing. In Europe, the Czech Republic is in the vanguard as regards contactless payments. There are also abuses of contactless payments not requiring a PIN code (limit of payments to CZK 500); in the case of card misuse, the overall damage is negligible.

After the banks' initial reluctance to tighten verification of online transactions, the situation has improved. At the moment, at least two-factor authentication is used by all banks and internal software has gradually also been deployed. It allows suspicious transactions to be monitored and blocked in a timely manner.

D/ Other cybercrime phenomena

Software used includes: standard Microsoft Windows operating systems, a forensic version of the Linux operating system (e.g. DEFT, CAIN), forensic examination and evaluation software (e.g. EnCase, FTK, Belkasoft Evidence Centre, X-Way Forensic, R-Studio Network, etc.). Software, such as UFED, XRY, Oxygen, and MobilEdit! is used for the analysis of mobile devices; however, there is there is insufficient provision of these programs. Police analysts need such tools; at the moment, they are equipped with Analyst's Notebook software. There is a need to increase the number of licences.

The Czech Republic has overcome obstacles to cross-border cooperation by ratifying the Council of Europe Convention on Cybercrime and the associated legislative measures, as well as bilateral treaties on judicial and police cooperation, active work within Europol and Interpol, building, and maintaining of the network of police liaison officers in other states.

5.2. Procedural issues

5.2.1 Investigative Techniques

The investigative measures provided by national law are the following:

- **search and seizure of information system/computer data;**

According to the Code of Criminal Procedure, these are primarily:

Section 78 Liability to deliver a thing (production order)

Section 79 Taking away of a thing

Section 83 Search warrant

Section 83a Warrant for a search of other premises and plots of land

Section 83b Personal search warrant

Section 113 Examination (of an object)

- **real-time interception/collection of traffic/content data**

Section 88 Intercepting and recording the telecommunication operation

Section 88a Finding data on telecommunications traffic that are subject to telecommunications confidentiality or that are subject to protection of personal and intermediary data

Section 158d Surveillance of persons and objects

Procedures in accordance with Sec. 88 and 88a apply to all telecommunications traffic (i.e. ordinary telephony), but not to traffic via other means (various communication programmes and applications).

- **preservation of computer data;**

As per Sec. 97 (3) of Act No 127/2005 Coll. on Electronic Communication, a legal or natural person providing a public communications network or a publicly accessible electronic communications service is obliged to retain traffic and localisation data that are generated or processed in the course of managing the person's public communication networks and providing the person's publicly accessible electronic communications services, for six months.

Such a legal or natural person who stores traffic and localisation data is obliged, upon request, to promptly provide such information to law-enforcement authorities for the purposes and under the conditions stipulated by Act No 141/1961 Coll. on Criminal Court Proceedings (Code of Criminal Procedure). The police may thus request traffic and localisation data in the context of criminal proceedings under Sec. 88a of the Code of Criminal Procedure, as well as in the context of search for persons and objects under Act No 273/2008 Coll. on the Police of the Czech Republic, as amended.

Furthermore, on the basis of:
Section 88(a) Finding data on telecommunications traffic that are subject to telecommunications confidentiality or that are subject to protection of personal and intermediary data (see above)
Section 158d Surveillance of persons and objects (see the previous point)

- **order for stored traffic/content data;**

As per Sec. 78 and 79 of the Code of Criminal Procedure, the surrender of an item important for criminal proceedings can be ordered or, if needed, the item may be withdrawn. Although the Code of Criminal Procedure does not define 'an item important for criminal proceedings', and the related provisions of Sec. 84 and 112 of the Code of Criminal Procedure do not expressly provide for the seizure of computer data, the abovementioned stipulations can be applied to a given case, and this is being done in practice.

In addition:
Sec. 88(a) finding data on telecommunications traffic that are subject to telecommunications confidentiality or that are subject to the protection of personal and intermediary data (see above).

- **order for user information.**

See above; user information is not treated differently from other stored computer data.

Such procedure is regulated in Section 88 paragraph 9 and in Section 88a paragraph 2 and 3 of the Code of Criminal Procedure.

There are no special conditions or deviations from general circumstances.
The techniques used have been introduced by forensic and criminological practice. Most often, they consist of hashing mechanisms, which are used to ensure the integrity of electronic traces, creating bit copies of data storage media, providing that the original, from which the evidence is recorded, remains unchanged (it is appropriate to use Linux forensic distributions).

Furthermore, special techniques such as hacking can be used in justified cases to track people and objects. Specialist software is also used to secure electronic evidence, primarily from mobile devices; special forensic software is used to analyse evidence.

The basic tools are powerful computers (and laptops), data storage, reductions and connecting cables of all kinds and interfaces, hardware tools, and computer components.

Sometimes, the use of special techniques such as hardware access blocks and special bit copiers (e.g. Falcon, Talon etc.) is appropriate.

Special techniques are primarily used for mobile devices (e.g. UFED). The basic premise is that investigating cybercrime requires keeping the integrity of acquired information intact and ensuring that the device under investigation does not undergo any changes. Experience has shown that computer technologies and information systems are constantly changing. This requires adequate responses and continuous education. It is thus a continuous development, without which it would be impossible to investigate cybercrime.

Local criminalists involved in securing electronic evidence are certified for their tasks by the Institute of Criminalistics Prague of the Police of the Czech Republic. As regards standardised procedures, the adoption of relevant ISO norms is expected soon.

5.2.2 Forensics and Encryption

Electronic or remote forensic examinations are not performed. However, some specific tasks in securing evidence can be performed remotely or electronically (interception, tracking people and objects).

The National Security Authority/National Cyber Security Centre, within the scope of its functions as the governmental CERT (hereinafter as "GovCERT"), currently performs a limited forensic analysis of incidents detected within its constituency and provides ad hoc consultations, upon request, to law-enforcement authorities. In the future, an expert facility should be created, capable of contributing its technical expertise to the investigation of cybercrime.

The problems encountered with encryption mainly concern strong encryption tools such as TrueCrypt, but also WinRar or PGP, where decryption is usually not feasible. For this problem, we lack computing capacity, which could even be provided contractually in specialised institutions, as well as relevant software. If these conditions could be met, the probability of gaining access to encrypted data would be significantly higher.

A solution is being worked on by means of a research project, budgeted for by institutional financing, at the Prague Institute of Criminology. The project has not yet been completed.

Regarding cooperation between national authorities, it should be highlighted that investigations are carried out by the police of the Czech Republic. The Institute of Criminalistics Prague carries out expert examinations and occasionally gives expert opinions on a given topic to requesting law-enforcement authorities. Within these examinations, questions are asked that concern, for example, access to encrypted data, a device or an account. It is thus a type of cooperation that falls within the Code of Criminal Procedure, or within scientific research. Furthermore, it is possible to contact Europol, which offers, among other ways of supporting investigation in EU Member States, the possibility of using its sophisticated decryption facility.

Decryption is usually carried out in cooperation with private companies, and in exceptional cases with Europol; not as yet with Interpol. In exceptional cases, requests have been sent to academic circles. There has not yet been any direct cooperation linked to a specific case.

Strong encryption, when properly executed, including related measures, is by its nature realistically unbreakable (within a reasonable timeframe). In the attempt to solve such security issues, it is possible to apply known methods by using errors of data encryption. In using these methods, it is also important to have access to powerful IT technology and specialist software. In some cases, the use of several PCs is advisable. Sometimes results can be obtained through the cooperation of relevant persons, or through monitoring or interception.

5.2.3 E-Evidence

Computer data are not expressly defined in procedural criminal law (Code of Criminal Procedure), but do appear in the Criminal Code in relation to some crimes as objects of an attack. However, they are not defined in the Criminal Code; their definition is in the Council of Europe Convention on Cybercrime.

Information about content: tracking people and objects in certain situations implies identifying information on content of data records (Sec. 158 (d) (3) of the Code of Criminal Procedure). However, the term is not defined more specifically (to better protect all kinds of private records).

Operating data: as per Sec. 90 of Act No 127/2005 Coll. on Electronic Communications, operating data ('traffic data') are understood as any data processed for the purpose of transmitting a message of electronic communications networks or for their billing. The definition of traffic data also appears in the Council of Europe Convention on Cybercrime.
Inspection warrant/inspection and securing of an information system are not defined; general legislation (in particular on search, production and seizure) is employed.
Inspection and securing of an information system or a network operated or controlled by persons/subjects suspected of cybercrime are not defined; general legislation is employed.

Electronic evidence is not defined in the Czech legislation; general legislation is employed. The main rule is stipulated in Section 89(2) of the Code of Criminal Procedure, according to which 'everything which may contribute to clarification of a matter may serve as evidence'. (That does not allow the state to violate special restrictions in obtaining some forms of evidence, however.)
In practice, this concerns mainly bit copies of data storage, media, and the results of their analyses, data secured through surveillance or interception, and data on telecommunications traffic. This information is made available to the public prosecutor and the court as a part of the case file; in a format that allows direct scrutiny, or presentation at the court, as an expert statement or an expert opinion.

The Czech legislation has no specific rules for electronic evidence; general legislation is applied. The basis is forensic science and practice. An identical evaluation procedure is used for electronic evidence procured abroad.

Sec. 89 (2) and (3) of Act No 141/1961 Coll., the Code of Criminal Procedure:
It shall be possible to use as evidence anything that may contribute to properly clarifying the matter and that has been obtained in a lawful manner from admissible evidence. Admissible evidence shall include, in particular, interrogation of the defendant, examination of witnesses and expert statements, verification of the testimonies on the scene, identification line-up, re-enactment, investigation attempts, examination, things and documents materially relevant for criminal proceedings, and examination.

Sec. 89 (4) of Act No 141/1961 Coll., Code of Criminal Procedure:
Evidence obtained by means of unlawful duress or threat of duress cannot be used in the proceedings with the exception of the case in which it is to be used as evidence against a person who has used duress or threat of duress.

5.3. Protection of Human Rights/Fundamental Freedoms

Protection of fundamental rights and freedom on the internet is primarily based on the Constitution of the Czech Republic, including the Charter of Fundamental Rights and Freedoms, where both global and European democratic principles are defined. Complaints about violations of their fundamental rights and freedoms may also be submitted by individuals to the Constitutional Court. Another integral aspect is membership of the European Union and the Council of Europe.

Inviolability of a person and of their privacy, home, personal freedom and freedom of expression is guaranteed. Records retained in privacy and sent messages also enjoy protection.

These rights may be limited only to the extent necessary and in a manner provided for by law. Everyone has the right to judicial and other legal protection. These principles also fully apply to the procedures in combating cybercrime.

Execution of wiretapping (including electronic communications), obtaining data on telecommunications traffic, and house searches and similar searches may be undertaken only in respect of particular criminal offences by the established official procedures, on the order of a court, whose independence is granted by the Constitution. The legislation of the Czech Republic also takes into account the European legislation, including decisions of the Court of Justice of the European Union and the European Court for Human Rights.

The Criminal Code, which codifies criminal offences, and the Code of Criminal Procedure, which regulates procedures during their investigation, may be included among the elements of protection. They both also cover cybercrime. General police procedures (which are not directly linked to criminal proceedings) are established by the Police Act. These are complemented by the Electronic Communications Act, in conjunction with its implementing provisions, which, inter alia, establish the confidential character of communications and regulate the gathering, retention and provision of data on electronic communications.

The Czech Republic has approved and ratified the Convention on Cybercrime (Council of Europe Convention on Cybercrime (the Budapest Convention)).

The Public Defender of Rights (Ombudsman) is established by law in the Czech Republic and so is the Czech Telecommunication Office. The Office for Personal Data Protection has competence to control the processing of personal data within both the civilian sector and the police and judicial structures. The Certain Information Society Services Act implements the e-commerce directive.

Czech legislation expressly allows exceptions from the protection of fundamental rights and freedoms, especially for the purpose of protecting democratic society, protecting society from crime, and detecting and prosecuting crimes. Interference with fundamental rights and freedoms can only be carried out by a state power if this interference is necessary. In terms of protecting privacy in the process of detecting, investigating or prosecuting crime, the safeguards are established mainly in the Code of Criminal Procedure. They concern mainly the following:

House searches	**- only with a court order if there is reason to believe that items or persons important for criminal proceedings may be found. See Section 83.**
Personal searches	- upon order of a court or public prosecutor, or with their consent, or if it cannot be postponed, or the person is caught in the act, or a warrant was issued for the person. See Section 83b.
Searches of other premises and land	- only with a court order or with its post-facto consent (if it cannot be postponed and the order cannot be procured immediately); without post-facto court consent the results of the search may not be used as evidence. See Section 83a.

Interception and recording of communication traffic	- only with a court order while investigating certain highly serious (at least up to eight years of imprisonment) and other specific crimes. In some cases, may be based on consent of the owner of the phone (e.g. for child kidnappings). Strictly regulated (see Section 88).
Securing data on telecommunication traffic	- only with a court order while investigating certain serious (at least up to three years of imprisonment) and other specific crimes. See Section 88a.
Issue or withdrawal of an item	- obligation to surrender an item important for criminal proceedings, at the request of law-enforcement authorities (including the police) - withdrawal of an item with the consent of the public prosecutor, which is usually given beforehand (the person is requested to surrender an item; if they do not comply the item is withdrawn immediately). See Sections 78, 79.
Summons, presentation at court	- in order to carry out an interrogation or other acts related to criminal proceedings
Detention of an accused / person charged (against whom criminal proceedings have been initiated)	- only in justified cases where there are grounds for custody (see below) - this is a short-term restriction of personal freedom of a person, who must be presented at the court within 48 hours See Section 75.

Detention of a suspect (not yet prosecuted)	- only in justified cases where there are grounds for detention, usually with the consent of the public prosecutor (if it can be obtained beforehand), or if the person was caught in the act or while running away - in certain conditions, anybody may do this - this is a short-term restriction of personal privacy of the person, who must be presented at the court within 48 hours See Section 76.
Arrest of a person	- only with a court order, if reasons for arrest are given and the presence of the person cannot be ensured otherwise - this is a short-term restriction of personal freedom (if it does not become custody) See Section 69.
Custody	- possible only for an accused person and in more serious crimes, if there is reasonable concern that the accused will persist in committing the crime, influence witnesses, or run away - only with a court order and only for the time necessary, with regular evaluation and limited time period See Sections 67-74a.
Securing money in a bank account, securities, real estate, intangible possessions, replacement value	- possible in the context of criminal proceedings, if there are reasons to believe that the items in question are proceeds of crime See Sections 79a-81b.

Ban on contacting certain persons, ban on entering a dwelling, ban on travelling abroad, ban on remaining in a designated place, ban on holding and storing things that can serve to commit crime, ban on performing specified tasks	- types of preliminary measures that can prevent the accused from committing further crimes See Section 77a and Sections 88b-88o.
Mental health examination	- only in justified cases, if it is necessary to examine the mental health of the accused
Surveillance of persons and objects	- only with prior consent of a judge if the inviolability of the home may be breached, as well as secrecy of correspondence and that of other documents and records kept private, using technical means. If it cannot be postponed, consent must be granted within 48 hours after commencement; otherwise the information must be destroyed and must not be used in any way. - only with the prior written consent of a public prosecutor in other cases when recording (audio, video, etc.) takes place See Section 158d.
Act on the Police of the Czech Republic – powers outside of framework of particular criminal proceedings	
Searching for persons and objects	- the police may request telecommunication traffic and localisation data from a provider for the purpose of searching for suspects, disappeared persons, etc. and for identification of a corpse Section 68 of the Act on the Police.

Prevention of particular terrorist threats	- special anti-terrorist police unit may request telecommunication traffic and localisation data from provider for the purpose of prevention and detection of particular threats Section 71 of the Act on the Police.
Other possible interferences with the rights and freedoms are possible on the basis of the Act on the Police of the Czech Republic	- basic police powers concerning, e.g. the identification of persons, summons, presentation at court, and detention for 24 hours - in the context of cybercrime, these interferences come into consideration especially in the early stages of an investigation

5.4. Jurisdiction

5.4.1 Principles applied to the investigation of cybercrime

Concerning jurisdiction with regard to acts of cybercrime committed outside the territory, apart from the broad understanding of the principle of territoriality (paragraph 4(1) and (2) of the Criminal Code and Sec. 2 (1) and (2) of the Act on Criminal Liability of Legal Persons), the following also applies:

- the principle of active personality (Sec. 6 of the Criminal Code and Sec. 3 of the Act on Criminal Liability of Legal Persons);
- the principle of passive personality (protection) (Sec. 7 (2) of the Criminal Code);
- the principle of universality (Sec. 7 (1) of the Criminal Code, Sec. 4 (1) of the Act on Criminal Liability of Legal Persons) for a limited group of crimes;

- the subsidiary principle of universality (Sec. 8 (1) of the Criminal Code), subject to the condition of de facto dual criminality;
- jurisdiction over acts in favour of a legal person with its headquarters or its branch in the Czech Republic (Sec. 8 (2) of the Criminal Code, Sec. 4 (2) of the Act on Criminal Liability of Legal Persons);
- jurisdiction under an international treaty (Sec. 9 of the Criminal Code, Sec. 5 of the Act on Criminal Liability of Legal Persons), usually specific and of a complementary nature.

5.4.2 Rules in the event of conflicts of jurisdiction and referral to Eurojust

According to available information, there has as yet been no conflict of jurisdiction with other states in the field of cybercrime.

Should they arise in the future, they will be addressed under the general legislation and in accordance with the Council of Europe Convention on Cybercrime.

There is no information to indicate that Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercising jurisdiction in criminal proceedings in relation to cybercrime cases has been explicitly used.

However, it may be assumed that the police and judicial authorities act in the spirit of this decision. According to available information, no cases have been forwarded to Eurojust for the purpose of resolving a conflict of jurisdiction.

5.4.3 Jurisdiction for acts of cybercrime committed in the 'cloud'

According to available information, there have as yet been no problems regarding the establishment of jurisdiction for cybercrime acts committed in the 'cloud' or for the collection of related electronic evidence which is stored there.

5.4.4 Perception of Czech Republic with regard to legal framework for combating cybercrime

National authorities do not consider the existing legal framework for investigating cybercrime committed outside the Czech Republic to be sufficient.

The main drawback is that a number of European countries have not ratified the Council of Europe Convention on Cybercrime, which provides tools and procedures for efficient international cooperation.

It is also evident that a number of countries have not signed international agreements or other useful instruments for direct police and judicial cooperation.

5.5. Conclusions

- Because the existing legislation on cybercrime is relatively new, the Czech Republic does not feel the need to amend existing legislation or to introduce new legislation at this moment. But in the future it would be appropriate to consider whether the legal protection of children and minors on the internet could be enhanced and to consider a more accurate definition of prosecuting DDoS cyber-attacks.
- CZ authorities explained that their definition of cybercrime is wider than that presented in the questionnaire (as understood wider than in Budapest Convention), but the subject of child sexual exploitation online is briefly mentioned in the CZ replays to the questionnaire and in presentations. The evaluation team considers that there is a need for the national authorities to take significant steps to establish relevant units with sufficient personnel, technical equipment and training to deal with child protection online.
- National authorities should reconsider that child sexual exploitation online is also a serious crime in cyberspace and should take appropriate steps to have sufficient capacity and capability to tackle it as well as cyber card fraud and cyber-attacks, which are understood as serious cybercrimes.
- The evaluation team considers that national authorities should evaluate the legal and practical possibilities for investigating, prosecuting and trying offenders who have committed crimes against the sexual integrity of children abroad, especially in third countries, when these crimes are within the scope of Article 9 of the Budapest Convention and relevant provisions of the Lanzarote Convention, and implement relevant findings in police and judicial practice, including the principle of universality as defined in national legislation.

- Evaluate the legal, practical and technical issues (e.g. exchange relevant data on persons who are at high risk of committing future crimes, preventive measures against their risky behaviour) in close cooperation with the international community related to transnational child sexual offenders, on how to monitor their movement in order to prevent them from committing future crimes against the sexual integrity of children within CZ or abroad, with respect for the human rights of victims on one side and the human rights of the offenders on the other.
- There are problems with encryption in cases of strong encryption tools because of a lack of computing capacity. According to the CZ Code of Criminal Procedure it is possible to cooperate with private companies, and Europol or Interpol. National authorities should enhance their computing capacity to gain access to encrypted data in more investigations.

6. OPERATIONAL ASPECTS

6.1. Cyber-attacks

6.1.1 Nature of cyber-attacks

According to reports processed by GovCERT, the most common attacks were those based on social engineering, such as phishing and spear-phishing. Other attacks investigated in 2014 included DoS and DDoS attacks on information systems of government institutions and a possible presence of malware/spyware in Czech systems. More information, including the number of incidents within the GovCERT constituency, is available in the annual report on the state of cybersecurity and on the information portal www.govcert.cz.

The Czech Republic experienced large-scale cyber-attacks in 2013. Since then, only local attacks (especially attacks targeted at specific companies) have been recorded. However, a certain level of latency can be assumed – some companies or organisations are perhaps afraid to publicise the fact that they had been the victims of a cyber-attack.

6.1.2 Mechanism to respond to cyber-attacks

Sec. 21 of the Act on Cyber Security defines the state of cyber-emergency as a sui generis emergency situation, where the attack cannot be managed by standard means and the safety of the Czech Republic could be compromised. The coordination mechanism for reacting to serious cyber-attacks functions mainly on the basis of ad hoc cooperation between the national CERT, GovCERT, the police of the Czech Republic, intelligence agencies and the army.

In situations of cyber-emergency, affected subjects such as the National Security Authority/GovCERT, the national CERT, KII and VIS administrators have specific responsibilities, just as in other emergency situations defined by law that are characterised by escalating gravity. The exact procedures for the field of cyber security are currently being drafted. The generic plan will serve as a methodological tool for developing specific plans by individual subjects.

The biggest local peering centre, NIX.cz, is an important player in this field, as it oversees a large part of the internet connectivity in the Czech Republic. It was within this organisation that the FENIX project was initiated, bringing together the biggest local telecommunications companies, hosting companies and service providers, as well as some subjects from Slovakia.

In the event of a massive attack from abroad, the project is capable of ensuring at least the basic functions of the internet. Its members operate trusted networks and can, if necessary, filter out foreign traffic.

Most frequently, international judicial cooperation is conducted on the basis of international instruments adopted in the Council of Europe, such as the European Convention on Extradition of 13 December 1957 and the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959.

National authorities make use of MLA where offenders outside the EU are implicated in cybercrime. However, CZ has not yet done so in investigating cyber-attacks.

6.2. Actions against child pornography and sexual abuse online

6.2.1 Software databases identifying victims and measures to avoid re-victimisation

There are no software databases developed specifically for the purpose of identifying victims in the cyber-environment in the Czech Republic. In priority cases, however, the international Interpol database ICSE is used; 13 police officers have been trained in its use. At the moment, the systematic use of ICSE is not adequate due to technical barriers and insufficient personnel capacities; the situation should improve further with the strengthening of the numbers of specialists on cybercrime.

In principle, it may be stated that inappropriate content which is not used as evidence is removed. If such inappropriate content reappears, it represents another criminal case and elicits another order for removal.

The right to protection from secondary victimisation (secondary harm) by the authorities involved in criminal proceedings consists mainly of limiting contact with the offender; special rules for interrogation of victims and for providing an explanation by victims are set out in Sections 17 - 22 of Act 45/2013 Coll. on victims of crimes. In the context of criminal proceedings, strict restrictions are applied for informing about juvenile victims and other cases under Section 8a - Section 8d of the Code of Criminal Procedure.

6.2.2 Measures to address sexual exploitation/abuse online, sexting, cyber-bullying

Amendment No 141/2014 Coll. introduced a new offence in the Criminal Code (Section 193B) - establishing unlawful contacts with a child.

The abovementioned projects have their own websites and include lectures and conferences. In an interactive manner, their creators make efforts to engage children with the aim of developing their interest in this issue.

The police of the Czech Republic also participate in these activities; in particular, police officers assigned to the issue of cybercrime and officers from prevention departments engage in awareness-raising at schools and youth organisations. The campaign has had excellent results, and a number of offences against children were detected precisely as a result of those activities.

6.2.3 Preventive actions against sex tourism, child pornographic performance and others

Preventive actions consist in increased attention on the part of the police, raising awareness, lectures in schools, information in the media and accompanying legislative changes such as, for example, some changes to the Criminal Code, also with respect to child pornography.

Regarding specific measures to counteract real time web-based child pornographic performances, amendment No 141/2014 Coll. introduced a new offence to the Criminal Code (Section 193a) - participation in pornographic performances, which also includes legal persons as perpetrators in accordance with Section 7 of the act on criminal liability of legal persons. By definition, it does not apply to offenders pursuant to Section 191 - 193, where this new offence has a supportive character only.

Following the adoption of the legislation given above, all police officers, particularly those assigned to the fight against cybercrime, are involved in combating this type of crime. They may encounter such conduct in the context of reported cases, but also in browsing and examining the internet and processing findings.

The police of the Czech Republic have also established a hotline; however, every police station is obliged to accept all notifications.

There are several projects, such as, for example, SaferInternet, run by the National Safer Internet Centre, Get acquainted safely, by Seznam.cz Ltd - these major projects inform the public about safe internet use and harmful online behaviour, with their main focus being on child protection.

6.2.4 Actors and measures countering websites containing or disseminating child pornography

Neither content filtering nor blocking of access is performed. Removal of contents and websites are carried out at the request of the police within criminal investigations involving child pornography. Such procedures take place especially in cases where the police do not immediately proceed to the seizure of content or do not secure the relevant content as evidence. If necessary (e.g. in the case of a house search), a court order is issued. Unlawful content may be reported by anyone directly to providers of information society services. A case must then be handled by the service provider.

Software for online filtering of internet websites to find material involving child pornography is not used. There have been efforts on the academic ground to create such an instrument in the desired online regime (Auriga); however, it was not suitable for use by law-enforcement authorities as regards desired outcomes. On the other hand, software for offline searching and filtering content is used.

Blocking of access by the police is out of the question (there is no legal instrument). In general, blocking of access to information may be ordered by the court, or it can be performed by a service provider in accordance with responsibilities of service providers according to the Certain Information Society Services Act.

Content removal / website removal are carried out in the context of criminal proceedings - appeals for removal of content, seizure, and securing as evidence. If it is necessary to carry out a house search or to breach any similar freedom, a court order is issued. The private sector either acts in compliance with a police request or it is obliged to perform and accept a court decision.

In practice, if content involving child pornography is secured, criminal proceedings are initiated. If the offender is also a holder of the content, the content is confiscated.

In the case of other entities, the evidence is secured and removal of content is requested. There are no problems with the application of this procedure.

There are no problems with removal of content; this also includes child pornography content located outside a Member State. It is then mainly the securing of evidence that is problematic - often there is only a request for content removal, but securing of evidence is not achieved.

In the Czech Republic, there are no specialised units dealing exclusively with child pornography. Existing communication is effected mainly along the lines of departments of general crime and information crime.

6.3. Online card fraud

6.3.1 Online reporting

Citizens and private companies generally report online card fraud. These cases are checked subsequently; latency is not expected. Reporting of such cases does not differ from reporting of any other offences or other unlawful behaviour. If a victim (a natural person or a representative of a legal person) detects a payment card fraud, they have to

contact either the police (in person, in writing, by telephone, etc. - every police station is obliged to accept such notifications) or their bank, which usually recommends, or even requires, the filing of a complaint with the police. Reporting is usually followed by procedural steps - interrogation, instruction, obtaining evidence, or even money (if applicable), and the results will determine what further action is taken.

6.3.2 Role of the private sector

Cooperation between industry, banks, private sector and LEAs exists and is sufficient. The general objective is to prevent and combat internet fraud with payment cards.

A certain unwillingness on the part of financial institutions is evident - the banking business has always been based on trust; according to banks, publishing and media coverage of security incidents, assaults and similar incidents is not good for the credibility of the institution concerned.

As regards the detection of abuse of new payment instruments, the police usually have the necessary information.

Security of cashless payments is gradually increasing; the usability of magnetic-strip cards is decreasing. In Europe, the Czech Republic is in the vanguard as regards contactless payments. There are also abuses of contactless payments not requiring a PIN code (limit of payments to CZK 500); in the case of card misuse, the overall damage is negligible.

After the banks' initial reluctance to tighten verification of online transactions, the situation has improved. At the moment, at least two-factor authentication is used by all banks and internal software has gradually also been deployed. It allows suspicious transactions to be monitored and blocked in a timely manner.

6.4. Other cybercrime phenomena

Software and hardware at the disposal of law-enforcement authorities are at the minimum level necessary to ensure operational capability, as well as capacity and knowledge; therefore, it would be appropriate to reinforce their resources, including the Institute of Criminalistics Prague and OKTE.

In particular, it is necessary to strengthen human resources, the numbers of police officers who deal with the issue of cybercrime, and enhance the education of specialists already involved. This applies to police officers involved in the fight against cybercrime, as well as those from economic crime departments and units with republic-wide competence, especially UOOZ.

It is also necessary to further strengthen international police cooperation (according to some findings, payment card fraud is typically carried out by foreign gangs). It would be appropriate to introduce targeted monitoring of hidden or 'grey' areas of the internet, where business with data facilitating payment card fraud occurs.

Raising awareness among parties concerned with cyber security may improve the security of e-shops, retailers' servers, or payment gateways, thus potential targets including theft-prone payment information.

Finally, by intensifying routine patrols of the Public Order and Traffic Police Services (which also includes raising awareness among the public), criminal activities such as 'skimming' (copying of payment card data) may be reduced - technical equipment will not be installed by criminals on cash machines, etc.; such equipment may already be detected during transfer. Criminals sometimes stay near cash machines and wait for information detected from payment cards. Police officers investigating this criminal activity must be equipped with conventional but powerful (portable) computers, supplemented by high-quality internet connections. It is also appropriate to use mobile technology (mobile phones, tablets), again accompanied by the option of high-quality internet connections.

As regards software - standard Microsoft Windows operating systems, a forensic version of the Linux operating system (e.g. DEFT, CAIN), forensic examination and evaluation software (e.g. EnCase, FTK, Belkasoft Evidence Centre, X-Way Forensic, R-Studio Network, etc.). Software such as UFED, XRY, Oxygen, and MobilEdit! is used for the analysis of mobile devices; however, there is insufficient provision of these programs. Police analysts need such tools; at the moment, they are equipped with Analyst's Notebook software. There is a need to increase the number of licences.

Same as in the previous case. If the planned strengthening takes place, it will be possible to spend more time monitoring the internet, which offers components and devices for the extraction of data from payment cards. As regards access by criminal groups to financial data and credentials, this issue does not represent a problem in the Czech Republic at the moment. In terms of know-how, monitoring of the internet is appropriate (mostly hidden and 'grey' areas) in order to detect publication of such practices and determine possible buyers.

6.5. Conclusions

- CZ police is connected to the International Child Sexual Exploitation Image Database (ICSE DB), maintained by GS Interpol in Lyon, and there are 13 police officers trained in its use. The ICSE DB offers many possibilities for identifying children in CZ and around the world and secure them against further sexual abuse; additionally, to secure evidence and locate offenders.
- The evaluation team understood that technical barriers and insufficient personnel capacities are obstacles to the systematic use of the ICSE DB; on the other hand, the reorganisation of the CZ police could be seen as a great opportunity to deal with these obstacles and implement better solutions.
- The evaluation team encourages national authorities to ensure that all trained police officers use the ICSE DB on a daily basis as part of their ordinary workflow, or to find ways to train more police officers to achieve the goals of the ICSE DB.
- The evaluation team also encourages competent authorities to take relevant steps such that investigators can carry out victim identification activities.
- Any reappearance of the inappropriate content (e.g. pictures of sexually abused children) on the internet represents another criminal offence, and a new order is obtained for its removal. Additionally, during the evaluation visit it was explained that removal of content and websites can be carried out at the request of the police; if the police request is not complied with, the court would issue an order.

- National authorities are encouraged to examine the legal, practical and technical possibilities for implementation of practical measures (e.g. content removal, access blocking and other) to prevent children and people becoming victims by viewing websites with child sexual abusive material (i.e. sexually exposed children, sexual assaults and raped children), and, to that end, to examine these questions in close cooperation with national stakeholders and international organisations (e.g. LEAs, Interpol, Europol).
- The evaluation team did not very clearly understand the meaning of notion 'the use of the ICSE DB system is limited to priority cases only' mentioned in the replies to the questionnaire, since the aim of the ICSE DB is to identify as many child victims as possible without any priority.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

7.1.1 Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA

As regards Eurojust, there are no special procedures, compared to other criminal activities, for its involvement in cybercrime cases. Any prosecutor within the framework of the public prosecution service (and also a police authority, with the knowledge of a supervising state prosecutor) can contact the Czech representation at Eurojust with a request for intervention (via telephone, e-mail, or other means of remote communication). The Czech representation can in fact be contacted 24/7.

Sec. 30 of the Act on International Judicial Cooperation obliges courts and, during preliminary proceedings, the prosecutor, to inform the national member of cases that directly concern at least three Member States, and where at least two of the Member States have been sent requests for international judicial cooperation, and where the crime is punishable by a prison sentence with a maximum penalty of at least five years (or a protective measure by deprivation of personal liberty) and consists of an attack against an information system.

Cooperation with ENISA focuses on questions of cyber security, their outreach into the realm of cybercrime currently being de facto null.
Neither does Czech law provide for any formal or special requirements as regards cooperation with Europol/EC3 – general legislative rules are applied.

7.1.2 Assessment of the cooperation with Europol/EC3, Eurojust, ENISA

The Czech representation has intervened in cybercrime cases (among them several concerning the breaking up of paedophile networks – see below) at the request of both Czech and foreign bodies. However, there are still fewer than 10 such cases per year. The Czech representation, for example, cooperated in the large-scale international intervention in the 'ONYMOUS' case, where, at the initiative of the USA, it provided communication with the relevant Public Prosecutor's Office in the Czech Republic. It also took part in several coordination meetings at Eurojust and provided relevant information necessary for carrying out an MLA request to the requesting and requested bodies. Subsequently, it provided assistance within the Eurojust Coordination Centre, which was in operation on the day of the intervention.

The Czech Republic does not have specific experience in relation to ENISA in this regard.

Nevertheless, international cooperation in this field will be strengthened by the ongoing reorganisation, which has been already mentioned above several times, especially by a constant increase in personnel and strengthening of educational activities on the efficient use of international cooperation and its methods.

Regarding the contribution of the abovementioned agencies in dealing with cybercrime, the Czech Republic gives them a decidedly positive assessment. It is due to these agencies that it is possible to set up JITs, share know-how and communicate through a network of liaison officers and contact points. These agencies have also made a significant contribution to drafting legislation, providing education and training and introducing new investigative methods.

Eurojust facilitates international judicial cooperation in prosecuting serious cross-border crime. It is, therefore, also an asset for prosecuting serious cross-border crimes in the field of cybercrime.

As regards Eurojust, it is necessary to highlight the possibility of establishing contacts abroad very rapidly, verifying specific requirements/formalities needed for granting MLA in cases of cybercrime requests for MLA, and also coordinating judicial cooperation. Not least, there are advantages stemming from Eurojust financing JITs.

Generally, cooperation with ENISA can be evaluated positively. However, we do not perceive cybercrime as a particularly important area in this context.

The capacity of the Czech Republic to exploit the opportunities offered by these agencies will improve with the strengthening of the police in terms of personnel.

Nevertheless, it is also necessary to keep expanding the awareness within law-enforcement authorities of the possibilities that the abovementioned agencies offer so as to use them in the most effective manner.

As regards ENISA, we do not have any proposals for its better use. However, the agency should not splinter its activities, but instead should focus on what it does best, especially since it is probable that with the adoption of the forthcoming Network and Information Security (NIS) Directive, it will acquire additional tasks in the field of cyber security.

As regards specific cases as a matter of priority, national authorities cooperate with both the public sector and foreign police counterparts, including Europol's EC3 and Interpol.

7.1.3 Operational performance of JITs and cyber patrols

The Czech Republic has participated in JITs in relation to cybercrime. Cyber patrols as such are not established in the Czech Republic; however, police officers assigned to cybercrime, in particular, do monitor, within the framework of their operational tasks, the public internet space and, therefore, execute the activities of cyber-patrols, including public sector support.

To give a specific example, the Czech Republic participated in the JIT entitled 'ATELIER', which was established for a case of trafficking in human beings, particularly an international network profiting from child pornography. The JIT included representatives of the Czech Republic, Sweden, and Spain. Nevertheless, the international cooperation involved authorities from the USA, UK, Ireland, and other countries. The case is a good example of functioning cooperation between Europol and Eurojust. Europol assisted particularly in the initial phase of the operation, during the exchange of operational data and in organising operational meetings, but it continued providing support throughout the entire exchange and information analysis. Consequently, Eurojust significantly sped up international cooperation, when its coordination meeting contributed to the rapid establishment of the JIT. Eurojust continued to provide assistance during the following phases of the criminal proceedings.

Based on the experience of the supervising prosecutor, this JIT can be summed up as fully functional, even after its expansion by a third member. From the perspective of all three participating countries, its goal was successfully reached.

The JIT made it possible to exchange copies of data carriers containing child pornography that had been secured during coordinated house searches in a form usable as evidence. Interception of electronic communication that was permitted in one of the states participating in the JIT helped to apprehend one of the Czech offenders and consequently served as evidence in criminal proceedings.

Indictments have already been filed in all three states participating in the JIT (the last in July 2015) and the case is currently before the court. No doubts as to the evidential applicability of evidence secured by members of the JIT abroad have been raised so far during the trial, nor have any of the other JIT members signalled any problems related to evidence that has been obtained in the Czech Republic.

Financial resources in the 'ATELIER' case were provided by Eurojust in order to support the functioning of the JIT.

Police officers assigned to cybercrime, in particular, do monitor, within the framework of their operational tasks, the public internet space and therefore perform cyber-patrol activities. Should they encounter illegal content from the perspective of criminal law as regards cybercrime, the necessary measures are adopted and criminal proceedings are initiated. They may also forward the case to another competent department. However, no specialised unit has been established whose main task would be to systematically dedicate itself to such activities.

The possibility of JITs being financed by Eurojust is believed to be absolutely crucial. Conclusions from pilot JITs where such a possibility did not exist, showed that funding was the main reason for their failure, or for its being impossible to establish them at all. As regards cybercrime, we welcome the efforts of Eurojust as regards the foundation of the network of public prosecutors for cybercrime with the aim of exchanging experience, legal opinions, etc. and the functioning of this network under Eurojust. However, it is not only in the area of combating cybercrime that we advocate a more intensive use of existing tools and communication channels (see the answer to question 8A/4).

It would also be useful to increase the number of police officers who actually carrying out cyber-patrol duties. Recently, the number of xenophobic and extremist manifestations on the internet has increased, and propaganda related to the crises in Ukraine and the so-called Islamic State has surfaced. Furthermore, fraudulent e-shops and phishing attacks pose a problem especially on social networks. Persons interested in or offering child pornography are active on discussion fora and on dating sites, often contacting and luring potential victims. There is a risk that the current number of police officers assigned to cybercrime will be overwhelmed in dealing with reported cybercrime and will not have sufficient staff and resources for monitoring and prevention.

7.2. Cooperation between the Czech authorities and Interpol

In each analytical department or general crime department of the Criminal Police and Investigation Service of Regional Police Directorates, a police officer is assigned who has access to the relevant ICSE database and, to the extent possible, participates in relevant training opportunities.

If unlawful child pornography material is detected during the investigation of individual cases, it is forwarded to this specialist, who then inserts or extracts such material into / from the database. If a match is found it can be determined where else there has been a case involving the material examined and what kind of victim it concerned, and accordingly determine the next steps or notify other police departments. The whole procedure is time-consuming, so the use of the system is currently limited to priority cases only. Given the planned increase in personnel, which will aim to expand the numbers of such specialists, we assume that the extent to which the international database will be used in the period following the reorganisation, will increase.

National authorities take notice of cybercrime reports issued by Interpol and also enter the international database for child sexual abuse. In addition, they actively participate in conferences organised by Interpol as well as working groups.

The ICSE database is currently being used only in a limited number of priority cases. Use of and contribution to the ICSE database are carried out by an officer of the Department of International Police Cooperation of the Police Presidium of the Czech Republic.

7.3. Cooperation with third states

Cooperation with third countries that have ratified the Convention on Cybercrime (Budapest, 23 November 2001) is anchored primarily in this document. With other countries, cooperation is ad hoc and is based primarily on bilateral agreements on police and judicial cooperation in criminal matters. These agreements are being concluded on the basis of a general criminal law perspective; they do not have specific provisions on cybercrime.

The involvement of European agencies has been beneficial with regard to sharing information and, at the same time, increasing pressure on third countries as regards their cooperation. Eurojust facilitates cooperation with third countries in a similar manner as with Member States. The physical presence of liaison public prosecutors from the USA, Norway, and Switzerland in Eurojust (and the addition of a specialised liaison public prosecutor on cybercrime is expected soon) is an immense benefit.

7.4. Cooperation with the private sector

Operators of systems of critical information infrastructure and important information systems are obliged to retain specified technical data on the activities of a particular information system for three months pursuant to the Decree on Cyber Security. However, in the context of criminal proceedings, the National Security Authority, specifically GovCERT, cannot request the blocking of access, removal of content or websites. Similar competences would only come into consideration in emergency situations defined by the law as part of an ongoing case of attack management.

A special responsibility/duty applies to the internet service providers. They either operate under Act No 127/2005 Coll. on Electronic Communications, or under Act No 480/2004, Coll. on Certain Information Society Services. Both norms define duties and obligations, including sanctions, in detail.

Blocking of access – a general blocking of access can be ordered by a court on the basis of the Act on Certain Information Society Services. Removal of content or websites is carried out in the context of criminal proceedings – requests for removal of content, seizure, forfeiture for the purpose of providing evidence. Where it is necessary to impinge on domestic freedom or similar, the order is issued by the court. The private sector either complies with the request of the police or else is obliged to perform and accept the court order. Often, blocking of access or removal of content can be achieved by alerting the company about illegal content, where the entity that uploaded such content is also simultaneously violating the company's rules. An alert can be given in accordance with the Act on the Police of the Czech Republic or the Code of Criminal Procedure.

Through the services they render, the internet service providers (ISPs) allow internet users to access varied content and therefore share responsibility for this content.

Based on European regulations, the responsibilities of ISPs are defined by Act No 480/2004 Coll. on Certain Information Society Services. An information society service is any service rendered through electronic means, i.e. where it is sent using electronic communication networks and retrieved by the user from an electronic device for storing data (computer, smartphone, tablet etc.). This somewhat tricky definition includes services provided on the internet, such as webmail, search engines, discussion sites, advertising sites, blog hosting sites, and other hosting services (providers of storage space), etc.

According to the degree of liability for the provided content, the relevant act differentiates between 3 types of ISPs in Secs. 3, 4 and 5. The first two types are ISPs providing transfer and a temporary storage of data. The third type is responsible for information content provided by users in cases where the ISP, due to the scope of its activities, circumstances, and the nature of the case, may have been aware that the content of stored data or behaviour of a particular user are illegal, or if the ISP has demonstrably found out about the illegal nature of stored content or illegal behaviour of the user and has not, without delay, taken all steps required to remove or block access to such information. Services such as discussion and advertising sites, web-hosting and others that offer space for uploading data by their user, fall into this category.

One very important point is that according to Sec. 6 ISPs are under no obligation to monitor information and actively seek out illegal content. This is because it would be technically extremely difficult and costly for the ISPs to monitor and filter all content that passes through their infrastructure and because it would gravely violate the constitutionally guaranteed right to user privacy. The reason for the attribution of responsibility to ISPs is that it would be very difficult (almost impossible) to request the correction of an infringement solely from the user who caused it. The current concept makes it possible to alert ISPs to an illegal situation, after which they have a legal obligation to deal with the problem, or they can be ordered by a court to correct the infringement. Moreover, ISPs can be very helpful during investigations, because they keep all kinds of records of electronic communications and access to services, making it easier to track the offenders.

A situation where user X-Anonymous-X posts a rumour about John Smith on a discussion server can be used as an example. Mr Smith feels that his right to protection of his person is violated by the rumour, but does not know who X-Anonymous-X is and therefore whom he should request to remove the information. This is where the responsibility of the ISP comes into play. Mr Smith may contact the ISP of the discussion server and demand the removal of the information. If the ISP considers that the law has been breached by the post, it will remove it. If it does not, Mr Smith has the right to enforce removal via court order.

Another practical example, which is very common, is that of so-called DMCA takedown notices. This instrument originates in US law, specifically in the Digital Millennium Copyright Act (hence the acronym), and functions as a mechanism enabling copyright holders to notify ISPs that their pages contain illegally disseminated works protected by copyright. Google, for instance, has set up a formalised way of sending DMCA takedown notices for its video service (YouTube) through the internet form, which is also available in Czech.

It certainly comes into consideration that private companies have their headquarters in a third state; this is where requests need to be addressed, whether directly or using legal assistance. The usual situation, however, is that local branches of such large companies are either not established at all, or they are intended to handle business affairs and do not cooperate with the police. The largest of these companies are, for example, Google and Facebook. Due to the possibility of communicating through national contact points as per the Convention on Cybercrime, however, this does not pose a major issue.

As for Microsoft, there is a company in the Czech Republic that represents its interests and through which it is possible to settle requests from the police.

There have been cases of a large web-hosting company having its headquarters in the US, where, for the purpose of securing proof inside one of its local branches, coercive measures were used – warrants to search other premises and land; however, they were applied in order to maximise the lawfulness of the acquired evidence for a foreign judicial authority, not because the companies did not want to cooperate.

Any measures that considered can be requested via MLA; none are ruled out in advance. The most frequent requests are those asking for retention of computer data, interception, storage of computer data (bit copies of storage media), local investigation, questioning of people, searches of premises, and removal of data. Requests for carrying out measures relating to cybercrime are not subject to special arrangements; general regulations are used.

7.5. Tools of international cooperation

7.5.1 Mutual Legal Assistance

For MLA in cases of cybercrime, the general provisions of Title I of Act No 104/2013 Coll. on International Judicial Cooperation in Criminal Matters (AIJC), i.e. sections 39 to 77, apply. Their use does not present special (legal) problems because, even at national level, electronic data and evidence are accessed in accordance with the general provisions of the Code of Criminal Procedure, like any other evidence.

However, several provisions of the Criminal Code (in particular Sec. 8(1), which expresses the principle of subsidiary universality, and Sec. 11, which concerns the effects of foreign criminal judgments in the Czech Republic) are significant, as well as the Act on Criminal Records, the Constitution of the Czech Republic and the Charter of Fundamental Rights and Freedoms.

Internal regulations are also important for the work of judicial authorities in this area, in particular: Ministry of Justice instructions dated 9 April 2014, ref. No. 37/2013-MOT-J/65, on the procedure of courts in relation with foreign countries in criminal matters (published as No 14/2014 SIS) and the Ministry of Justice instructions dated 30 April 2014 , ref. No 42/2013-MO-J/60, on the procedure of courts in relation with the EU Member States, as regards criminal matters (published as No 17/2014 SIS); and finally, the general guidelines of the Supreme Public Prosecutor No 10/2013, on international judicial cooperation in criminal matters.

In a wider context, international cooperation can be divided into:

- police cooperation concerning particularly the exchange of information:

Within the framework of international police cooperation, the Europol/Interpol channels can be used (processed by the police authority), as can contact points established as per the Council of Europe Convention on Cybercrime (in relation to contracting parties). Other appropriate tools for police cooperation can also be employed (bilateral agreements, EU regulations), as well as SIS and SIRENE if the person or objects concerned are being searched for through SIS.

- standard legal assistance aimed especially at securing evidence:

As per Sec. 40 (1), and Sec. 48 (1) of AIJC, the Supreme Public Prosecutor's Office is in charge of sending and receiving requests for MLA, not excluding cybercrime cases, based on a suggestion made by the police authority submitted to the relevant Public Prosecutor's Office (preparatory proceedings) or the Ministry of Justice (court proceedings). In the case of countries whose direct contacts are governed by international treaties, public prosecutors (or the courts) send MLA requests directly.

Reception of MLA requests in cases of direct contacts is centralised at the level of Regional Public Prosecutor's Offices (for specific requests, e.g. cross-border tracking, a specific Public Prosecutor's Office is specified for the entire Czech Republic). The centralisation of requests contributes to increasing the efficiency of handling these requests from abroad.

None of the available police statistics systems is designed to provide this kind of data. Such statistics are not kept, and there has not yet been a need to keep, evaluate, or register them. Requests sent and received are dealt with continuously as needed; no issues have been registered yet.

An overview of communications received and sent by the central contact point for police cooperation is included in the answer to question 1.6. As for the statistical definition of requests sent within the framework of the so-called contact point according to the Convention on Cybercrime, in 2015, a total of 16 requests were received and a total of six requests were sent to other contact points abroad via this channel.

Specific procedures or conditions concerning MLA requests related to cybercrime are not regulated by the national legislation, i.e. MLA requests related to cybercrime are dealt with according to the general provisions described under the answer to question 1 in this section.

If requests are addressed to the contact point, urgent requests are answered within hours. The average response time is a few days.

The average response time depends mainly on whether the MLA is provided on the basis of an international agreement or an assurance of reciprocity – in the latter case the response time is longer because it is necessary first to receive/grant an assurance of reciprocity.

Any measures considered can be requested via MLA; none are ruled out in advance. The most frequently handled requests are those asking for the retention of computer data, interception, storage of computer data (bit copies of storage media) and local investigation, questioning of people, searches of premises, and removal of data. Requests for measures relating to cybercrime are not subject to special arrangements; general regulations are used.

Informal consultation with foreign requesting/requested states is common. Most often, it is conducted between national contact points as per the Budapest Convention, via e-mail correspondence, or personal contacts of individual police officers. Contact points of the European Judicial Network for Criminal Matters within the EU can also be used for this purpose.

Specific problems in providing/requesting MLA relating to offences committed in the so-called cloud have not been encountered.

Most frequently, international judicial cooperation is conducted on the basis of international instruments adopted in the Council of Europe, such as the European Convention on Extradition of 13 December 1957 and the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959.

MLA is used where offenders outside the EU are implicated in cybercrime. However, this has not yet occurred in the investigation of cyber-attacks.

7.5.2 Mutual recognition instruments

Judicial authorities have the authority to use all mutual recognition instruments (European protection order, mutual recognition of supervision measures, of custodial sentences and measures involving deprivation of liberty, recognition and execution of confiscation orders, mutual recognition of financial penalties, execution of orders freezing property or evidence), as these fall directly within their competence. However, in practice, relevant international agreements are often used instead of these instruments. There are no statistics on these instruments; therefore, it is impossible to give specific examples.

7.5.3 Surrender/Extradition

a) The EAW may be issued for an offence punishable by a prison sentence with a maximum duration of 12 months or more, or a protective measure involving deprivation of liberty with a maximum duration of 12 months or more, or if a prison sentence or protective measure lasting at least four months is to be applied. Cybercrime offences may include those listed under Sec. 230 - Unauthorised access to a computer system and/or data carrier; Sec. 231 - Procurement and storage of access instruments and passwords to a computer system and other such data; Sec. 232 - Damaging records on a computer system and/or a data carrier and interference with computer equipment by negligence; and also offences consisting of disseminating illegal content (child pornography – Sec. 191, 192, online hate crime – Sec. 403 – 405, or hoax – Sec. 357); offences against copyrights as per Sec. 268 and 270; and various fraudulent actions. All the listed offences meet the conditions for issuing an EAW.

   In the Czech Republic, no formal correspondences between offences under the Czech Criminal Code and offences under Art. 2 of the Framework Decision on the EAW are established. Therefore it is at the discretion of the issuing court whether, in a specific case, it places the offence in question in one of the categories listed above. Some of the abovementioned offences applicable to cybercrime would probably be listed elsewhere than under cybercrime in an EAW form – this depends on the assessment of the issuing judge (e.g. fraud or sexual abuse and child pornography, etc.).

b) As per Sec. 90 (1) of the AIJC, extraditable offences are those punishable under Czech law by a prison sentence with a maximum duration of 12 months or more. National legislation does not list specific extradition criteria for offences relating to cybercrime.

1. Which authorities are responsible for sending/receiving surrender/extradition requests and for deciding on such requests in relation to cybercrime? What communication channels are used?

The authority competent to issue an EAW is the court. The EAWs are entered by the Czech National SIRENE Headquarters (the 1st unit of the Department for International Police Cooperation of the Police Presidium of the Czech Republic) into the SIS. As regards the requests of other Member States relating to searches and arrests of persons based on an EAW, SIS is also used. For the purpose of detecting and detaining a person, it is the Regional Public Prosecutor's Office that is responsible for receiving the EAW, depending on the place of detention of a person. Where an EAW is sent directly between two judicial authorities, the Regional Public Prosecutor's Office receives it and then forwards it to the police (SIRENE) for further measures if it is needed to track the person down. The Czech Republic has fully implemented the relevant provision of the Framework Decision on the EAW stating that an entry in SIS is equivalent to an EAW.

The authority competent to request extradition of a person from a foreign country and to receive such a request from a foreign country is the Ministry of Justice, as per Sec. 80 (1) and 88 (1) of the AIJC.

Where needed, the contact points of the European Judicial Network on criminal matters within the EU can be used.

None of the available police statistical systems are designed to provide the number of requests sent or received. Such statistics are not kept and there has not been the need to keep, evaluate, or register them as yet. Sent and received requests are dealt with continuously as needed; no problems or issues have been registered yet.

Specific procedures and conditions concerning requests related to cybercrime are not regulated by national legislation, i.e. requests related to cybercrime are dealt with according to the general provisions laid down by the AIJC.

Urgent requests are dealt with first; however, the law does not set out a response deadline.

Provisional arrests are possible. As per Sec. 94 (1) of the AIJC, a person may be taken into custody if the established facts justify concerns that they might escape. Likewise, as per Sec. 81 of the AIJC, the Ministry of Justice may request a foreign country for provisional detention of a person whose extradition is sought.

The average response time depends mainly on whether the MLA is provided on the basis of an international agreement or an assurance of reciprocity – in the latter case the response time is longer because it is necessary first to receive/grant an assurance of reciprocity.

In the case of the EAW, a person may be detained and placed in temporary custody in accordance with Sec. 204 of the AIJC.

The Agreement on the surrender procedure between EU, Member States, Iceland and Norway is not yet effective in the Czech Republic. The Czech Republic follows the European Convention on Extradition of 1957 with respect to Iceland and Norway.

7.6. Conclusions

- Eurojust is known to CZ competent authorities and used in particular in cases of conflicts of jurisdiction and complex cases requiring coordination. Eurojust funding of JITs is particularly welcomed by national authorities. In addition, CZ welcomed the efforts of Eurojust as regards the foundation of the network of public prosecutors for cybercrime with the aim of exchanging experiences, legal opinions, good practices, etc. and the functioning of this network under Eurojust. Prosecutors in Brno also commented that they expected Eurojust to facilitate the setting up of a EU network of cyber-prosecutors and support its functioning.
- During the visits, the evaluation team appreciated the presentation of the CZ part of JIT Case Atelier, where the role of Eurojust (in particular regarding JIT funding) and Europol was emphasised. The prosecutor has filed indictments against four suspects in the case, facing sentences of between eight and 15 years imprisonment.
- The CZ authorities cooperate with the various international bodies, authorities and institutions, e.g. Europol and Interpol. At Europol the EMPACT initiative has been established, which consists of the EU Policy Cycle 2014-2017 to fight serious organised crimes and counter terrorism. Within this policy, strategic goals have been set for every crime area found relevant to the EU in protecting people for a safer Europe. On top of the strategic goals, there was one priority within EMPACT, called Cybercrime (priority G), which has three subgroups: cyber-attacks (CA), child sexual exploitation (CSE) and cyber-card fraud (CF). The evaluation team encourages the CZ authorities to join the EMPACT initiative, especially in all cybercrime areas.
- The national authorities should also be reconsidering participation in the EU Policy Cycle in combating serious and organised crimes, as an equal partner and member in joining EMPACT groups, especially those related to cybercrime, in order to obtain information relevant to dealing with cybercrime issues, and to share their knowledge and experiences.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

Both the Cyber Security Strategy and the upcoming 'Conception of education in the area of cyber security' address the reform of education of judicial bodies involved in combating cybercrime and ensuring cyber security. Primary responsibility, however, lies and will remain with the competent authorities. Methodological support will be provided, and specifically focused exercises on cyber security may be organised. NBÚ / NCKB is also involved in the activities of C4E (Czech Cybercrime Centre of Excellence), which seeks to raise awareness and increase the efficiency of prevention and investigation of cybercrime, including a practical element in the form of the KYPO simulation environment at the Faculty of Informatics of Masaryk University.

To a limited extent, professional training as regards cybercrime for law-enforcement and judicial authorities is provided; its expansion and intensification is planned for the future. The aim is to establish standard practices and knowledge in the detection and investigation of cybercrime. The main focus is on securing of digital traces and evidence. A basic course, whose outcome is certification for the securing of digital traces and evidence, takes two weeks. The course concludes with an expert examination at the Institute of Criminalistics Prague (the top expert institution). Courses are led by experts from the IT field. It is presumed that the course should be repeated at least once every three years. In the meantime, however, professional training is carried out via active and passive participation in lectures, conferences and workshops focusing on cybercrime. Certain educational activities also take place at Secondary Police Schools of the Ministry of the Interior. Participation in national and international exercises in the field of cyber security, organised by GovCERT, also serve as professional training.

Regular offers by Interpol and Europol to participate in training courses for experts from the police are also used.

Police College and Secondary Police School of the Ministry of the Interior in Holešov

Secondary vocational education

Within the four-year secondary education, the issue is taught cross-sectionally throughout the whole course; in particular in the modules on Law, Crime Control, Security Activities, and Information and Communication Technology (topic: work with information and data and their misuse for corruption with the use of computer technology).

Further vocational education

Within the Police College, the issue is taught cross-sectionally from the first year through the third year, in particular in the modules on Substantive Criminal Law, General Crime Detection, and Economic Crime Detection. Considerable attention as regards this issue is paid to the field of informatics and computer science, which is an integral part particularly of the fight against cyber-terrorism. The content of the curriculum of the module on Data Protection relates to work on the internet and intranet —trafficking in human beings, cybercrime, cyber bullying, cyberterrorism, social networks and their pitfalls.

Basic police training

As a part of the module on Information Systems of the Police of the Czech Republic, the topic of Personal Data Protection, which includes principles of personal data protection and prescribed procedures as regards processing and use of information by information and communication technology, processing of personal data by the police, the obligation of confidentiality, cyberspace security.

Projects:

In the framework of the EU - ISEC (Prevention of and Fight against Crime), the Police School in Katowice has contacted partner schools, the Secondary Vocational School of the police force in Pezinok (SOŠ PZ Pezinok) and the Police College and Secondary Police School in Holešov with a request to join a project entitled 'The use of existing information systems to enhance effective cross-border information exchange in the field of crime prevention'. The Police School in Katowice is the submitter and coordinator of the project. The school cooperates with the Department of International Police Cooperation of the Police Presidium.

The main objectives of the project are as follows:

• Development of activities for the evaluation and comparison of communication channels and their accessibility for EU Member States in connection with the Prüm agreement.
• Sharing experience and practical knowledge in the field of cooperation between police and joint centres for police and customs cooperation.
• Evaluation of current trends in education which concern cross-border information exchange between the EU Member States.

The Police College of the Ministry of the Interior in Prague

Further vocational education

The issue of cybercrime depending on context is included in the following modules / subjects: Operational and Investigative Activities; Criminalistics; Organised Crime; General Crime Detection; Criminal Law; Substantive Criminal Law; Detection and Documentation of Criminal Activity; Economic Crime Detection; Protection and Backup of Data; Specialised Informatics; Conditions of Access to Information.

The content of education, beyond the abovementioned issue, includes the following other topics: computer architecture and operation systems, operational programs, electronic mail, word processors, spreadsheet processors, presentation software, database systems, application software, etc., which are always based on competences of the relevant accredited educational programme.

Module: Criminal Law

• Economic crimes

• Crimes against property

• Crimes against families and children

• Generally dangerous crimes

Module: Specialised Informatics

• Personal data protection, security of systems principles, protection and backup of data, information security.

Module: Informatics in Transportation

• Protection of data and information, the legal basis of data and personal data protection, information security.

Conferences:

On 9 and 10 October 2014, the Secondary Police School of the Ministry of the Interior in Prague held an international conference entitled 'Solving electronic violence and cybercrime against children and among them' in a congress hall of the Vysočina Region. The conference was organised in collaboration with the Vysočina Region and its main themes were the elimination of child cybercrime, its legal aspects, and trends in education, research, prevention and strategies for cyber and information security. The conference was intended for the expert public, representatives of the local police, representatives of local OSPODs, crime prevention coordinators and assistants, management and staff of local schools.

The conference had an international character and contributions were presented by representatives of police forces from the United States, Spain, Slovakia, Estonia, Ireland and United Kingdom. The aim of the conference was to bring together experts from the security forces, specialists in the field of prevention and education, information and communication technology, government, corporate and non-profit sectors, as well as professionals working with children and youth - especially experts on prevention and social workers. The conference was attended by 120 people.

Secondary School for the Criminal Police of the Ministry of the Interior

The issue of cybercrime is covered in possible combinations incorporated in educational subjects: Operational and Investigative Activities; Criminalistics; Criminal Law (Penal Code - Chapter 5: Crimes against Property, Chapter 6: Economic Crime); Detection and Documentation of Criminal Activities (Detection and Documentation of General Crime and Detection and Documentation of Economic Crime). Ways of committing crimes, their detection and documentation are discussed.

Nowadays, there is a foundation course for so-called IT specialists at the Secondary Police School for the Criminal Police in Čeperka (Opatovice). The course is provided by the Institute of Criminalistics Prague and should, therefore, meet existing certification of persons engaged in securing data at the crime scene.

The responsibility for providing professional training on cybercrime within the Police of the Czech Republic is in the competence of the Department of Information Crime of the Unit for Combating Organised Crime of the SKPV , in cooperation with the Institute of Criminalistics Prague. Through the Department of Security Research and Police Education of the Ministry of Interior and the Department of International Cooperation and the European Union and the Police of the Czech Republic, training under the auspices of CEPOL is made accessible. Activities within the ECTEG were not recorded. In May 2015, the Europol Roadshow was held, which also included the EC3 workshop devoted to the issue of cybercrime; other events will follow.

The task of the European Police College (CEPOL) is the exchange of experience and training of police officers and middle and senior management and experts at an international level. CEPOL supports and develops a European approach to the main problems which Member States face as regards the fight against crime, crime prevention, including in the context of cybercrime. CEPOL creates a network which links Member States' national training centres and develops extensive educational and training activities (courses, seminars, conferences, e-learning, etc.) in the area of prevention and fight against crime. In the past, CEPOL has run the following professional courses: 'Member-State and Union Capacities to Detect, Investigate and Prosecute Cybercrime', 'Cybercrime vs. Cybersecurity', 'Cybercrime Forensics and Digital Evidence'.

An international element is often present in an investigation of cybercrime; the inclusion of police officers on this issue therefore undoubtedly plays a role in the process of international cooperation. There is no other specific professional training provided.

Some prosecutors specialising in the field of cybercrime, however, attend lectures, conferences, seminars and workshops related cybercrime; it gives them a better insight into the issue, including matters linked to international cooperation, in which they participate.

CEPOL annually organises several residential and e-learning activities on cybercrime and the fight against it. These activities are intended for representatives of EU Member States, thus creating an environment for knowledge-sharing across the Member States on an international and European level. The length, objectives and requirements for participants of CEPOL activities on the issue of cybercrime vary (two hours for e-learning courses, approximately three to five days for residential activities).

Combating cybercrime is one of the priorities of the EU Policy Cycle and, therefore has also become an education and training priority area at present as well as for the future. CEPOL activities on cybercrime will be organised annually.

Competent staff responsible for the exchange of information in the context of international cooperation in the department of international police cooperation (OMPS) as regards cybercrime participate in the instruction and methodology employment (IMZ) seminars or attend international training courses on cybercrime.

The National Czech Cyber-Crime Centre of Excellence (C4E) functions rather like an academic establishment. The main objective of the C4E is to enhance general awareness and efficiency of work in the prevention and investigation of cybercrime via:

- strengthening awareness of cybercrime via conferences and workshops organised for partners, target groups and other publics;
- enhancing training and know-how of target groups, in particular police, prosecutors and judges;
- preparation / development of efficient and available tools for target groups, particularly the police but also administrators of critical infrastructure;
- development and distribution of guidelines, best practices and standards in the area of electronic evidence (obtaining, analysis, reporting, use), investigation of relevant cases, use of digital evidence in court.

The fundamental task of the C4E is to support the Czech Republic in the fight against cybercrime. The C4E works to bring together the best experts in the field of cybercrime, for example in the area of obtaining, analysis, investigation and implementation of electronic evidence. C4E, therefore, aims to become a centre of knowledge, i.e. a specific type of think-tank. All these efforts are carried out with close international cooperation. C4E wants to become one of the key members of the international network of similar national centres.

The National Security Authority, in cooperation with several universities, participates in the preparation of training programmes in cyber security and its personnel give lectures in specialised courses of existing curricula. Further development of educational activities depending on target groups will follow the abovementioned conception of education. Special courses on cybercrime, however, fall primarily within the competence of institutions directly participating in the investigation and prosecution of cybercrime.

Specifically:

This year, Brno University of Technology launched a study programme dealing with cyber security, including cybercrime. It also works with Masaryk University Brno, where the Institute of Law and Technology, which conducts research on the organisation of studies focusing on cybersecurity and cybercrime, is based. This year, the Cyber Exercise & Research platform (KYPO) was launched at Masaryk University Brno as a security research project. It created a unique environment for research and development of methods for protection against attacks on critical infrastructures. In a virtualised environment, it is possible to run complex scenarios of attacks on critical infrastructures and to analyse their progress. This environment is used for applied research and testing of new security methods, tools and training for members of security teams. The police also cooperate with the project. Further cooperation between law-enforcement authorities and academia has already been proposed; specific projects and educational programmes will be launched next year.

Accredited degree programmes at the Police Academy (PA CR):

The issue of cybercrime is addressed in all taught undergraduate courses (B 60 Security and Law Studies, 61 B Criminal Science and Other Forensic Disciplines, B 71 Security Management in Public Administration).

Courses include 'Information Security' as a optional module. The issue of cyber security and cybercrime is incorporated into several modules taught. In criminalistics and criminal law as such, the subject of criminal investigation is highlighted (Section 230 of the Criminal Code) - Unauthorised Access to Computer Systems and Information Media, (Section 231 of the Criminal Code) Obtaining and possession of Access Device and Computer System Passwords and other such Data and (Section 232 of the Criminal Code) Damage to Computer Systems and Information Media Records and Interference with Computer Equipment out of Negligence. The module on Criminal Protection against Cybercrime (B62) immediately follows the module on Criminal Law. The aim of the module is that its students gain detailed knowledge about ways of committing crimes occurring in connection with the use of information technologies as well as merits of offences. Furthermore, the course focuses on the characteristics of the procedure of law-enforcement authorities in criminal proceedings, the specifics of detection and investigation of cybercrime, and international legal aspects of this phenomenon. In criminology, aspects of criminological phenomena such as incidence, development tendencies, cybercrime prevention and knowledge in the field of crisis management (protection of critical information structures) are clarified (bachelor's degree B71 and master's degree programmes N71, etc.).

Lifelong learning programmes at the Police Academy (PA CR) – Cybercrime:

Participants in the course are primarily officers assigned to the SKPV. This is a basic course. Participants must be officers who need to gain knowledge in the area of cybercrime and crimes committed with the use of information technology.

The course aims to inform participants about the latest trends in cybercrime, such as computer fraud, theft of funds from banking institutions, etc. The course focuses mainly on criminal aspects of this category of crime.

Programme of the course:

1. Definition of basic concepts and terminology
2. Protection and security of data, anonymity
3. Outline of the developments and trends in cybercrime
4. Definition of individual manifestations of cybercrime and their criminal qualification
5. International legal aspects of combating cybercrime
6. Cooperation with other entities
7. Discussion and exchange of experience

Conferences in 2014

- Security seminar: Cyber security. Prague: The Police Academy of the Czech Republic in Prague and AFCEA Czech Republic, 27. 2. 2014
- iED Colloquium on an electronic identity of citizens; organised by the working group on cyber security of the Czech branch of AFCEA, in cooperation with the Faculty of Security Management of the Police Academy of the Czech Republic in Prague, 23. 4. 2015 at the PA CR (69 participants)
- Security seminar: Security of Multimedia Communications. Prague: The Police Academy of the Czech Republic and AFCEA Czech Republic, 4. 6. 2014
- 16th annual international conference of AFCEA Information and communication technology – ITTE: Future Crises 2014, 15. – 17. 10. 2014
- Cyber Security – Challenges and Achievements. Security seminar of the Police Academy of the Czech Republic in Prague, National Security Authority and AFCEA, 13. – 14. 5. 2014 (232 participants)

- AFCEA International student club meeting: event co-organised by AFCEA and the University of Defence Brno, which took place on the university premises in Brno, 14. 5. 2014 (presentations were also given by students, 30 participants)
- Multimedia communication and security: security seminar of the Police Academy of the Czech Republic in Prague and AFCEA, 4. 4. 2014 (45 participants)
- Conference 'Increasing the efficiency of the educational system in crisis management in the area of internal security', 8. 10. 2014
- Cybercrime and other cyber threats. Conference held within the framework of the European Cyber Security Month and in cooperation with the National Safer Internet Centre and AFCEA, 30. 10. 2014 (presentations were also given by students); 62 participants
- Cyber Security Strategy of the Czech Republic, practical implementation of the law on cyber security and education: security seminar of the Police Academy of the Czech Republic in Prague, National Security Authority and AFCEA, 27. 11. 2014 (110 participants)

Projects:

As part of the integrated research assignment of the Police Academy of the Czech Republic in Prague No 4: Analysis and prediction of selected topical issues of public administration, leading researcher Oldřich KRULÍK; there are two research tasks particularly relevant to the issue of cybercrime.

Research task 4/4: Information security and cybercrime within an organisation, leading researcher: Josef POŽÁR

The focus of this research task responds to dynamic changes in contemporary society. Threats, their consequences and potential liquidation, as well as prevention, raise the need for specific scientific and research support.

Research task 4/9: Laboratory: Security Management Research Centre
Leading researcher: Josef POŽÁR

Currently, the efforts of the research team focus on ensuring the material and technical security of their centre. The equipment was continually being upgraded, the assumption being that it was to be upgraded and put into operation during 2014, as well as its software and updates, and their subsequent use within programmes of doctoral studies.

Publication output of the academic staff of the school devoted to issues of cybercrime in 2014 are listed below (including abstracts and keywords):

Monographs:

JIRÁSEK, Petr; NOVÁK, Luděk; POŽÁR, Josef. Cyber Security Explanatory Dictionary, 2nd Ed., Prague: The Police Academy of the Czech Republic and the Czech branch of AFCEA, 2014. ISBN 978-80-7251-397-0.
https://www.govcert.cz/en/info/events/cyber-security-explanatory-dictionary---second-edition/

• Abstract: In every industry, terminology is an important means of rational communication and consistent understanding of communicated contents. Due to the interconnectedness and complementary character of the disciplines, their specific technical language has no exact boundaries; in addition, the language is enriched interdisciplinarily. Changes in contemporary society in which science and modern technology occupy an increasingly more important role, ICT is obviously also reflected in the range and terminology of vocabulary in the field of cyber security.

A significant result of this influence as regards its users is the process, often very critically and perceptively assessed, of taking over words found in foreign languages. Another integral part is the emergence of new phrases and new, or previously only marginally recorded, meanings of words. All of these changes generate a need for modern people to understand words of foreign origins well and use them accurately and concisely.

• Key words: Cybercrime, cyber security, terminology, etymology.

Collections – national:

POŽÁR, Josef; HNÍK, VÁclav; KRULÍK, Oldřich; JIRÁSEK, Petr. Protecting cyberspace in the post-Soviet states. In: Petr JIRÁSEK and Milan KNÝ (Eds.). Future Crises 2014 Focused on Cyber Security and Defence and Crisis Management. Collection from the 16th annual international conference of AFCEA Information and communication technology – ITTE. Pp. 69 – 101, ISBN 978-80-7251-423-6. Note: In 2014, the publication was awarded the 'Jury Prize for the Electronic Dictionary of the Year' by the Union of Interpreters and Translators.

http://www.jtpunion.org/spip/article.php3?id_article=4166

• Abstract: The paper describes the situation concerning certain aspects of the development and protection of cyberspace within the former Soviet republics - including Central Asia. Entities responsible for cyber security issues are mentioned where possible. This does not always concern establishments like CSIRT / CERT in the true sense of the word. Useful contact information and points of interest on the topic are included.

• Key words: Information security, former Soviet Union republics, international cooperation, information exchange.

KRULÍK, Oldřich; KRULÍKOVÁ, Zuzana; POŽÁR, Josef. Information Crime and its Trends Through the Lens of Prominent Think-Tanks. In: Electronic collection: 'European Cyber Security Month' (Sarka SOUDKOVÁ; Milan KNÝ, Eds.). Safer Internet. 2014. ISBN 978-80-7251-427-4.

http://www.saferinternet.cz/ecsm-2014/328-evropsky-mesic-kyberneticke-bezpecnosti-2014.html

• Abstract: The area of cybercrime is evolving dramatically. Therefore, it is useful to pay attention to the outputs of foreign or multinational security 'visionaries' in the field of 'cyber security'. It is striking how similar the various estimates are when describing virtually the same phenomena though in different words.
• Key words: Information security, cybercrime, trends, estimates.

POŽÁR, Josef. The Issue of Cybercrime in Information Systems. In: Prerequisites of Information Systems in System Engineering: virtual conference SYSIN 2014. (Milan KNÝ and Miloš VÍTEK, Eds.). Prague: The Police Academy of the Czech Republic in Prague, 2014. Pp. 147 – 151. CD-ROM. ISBN 978-80-7251-417-5.

• Abstract: The paper focuses on some aspects of cybercrime and presents various conceptions of this issue. It concerns types of cybercrime, cyber-attacks, etc. It attempts to categorise perpetrators of cybercrime. It also describes selected trends in cybercrime in 2014.
• Key words: Information and communication technologies, information security, cybercrime, cyber trends.

Other periodicals, including electronic periodicals:
POŽÁR, Josef. Modelling of the Investigation of Cybercrime. Science and Military Journal, 2014. vol 9, No 1, s. 63 – 69. ISSN 1336 – 888-5.
http://connection.ebscohost.com/c/articles/96842997/modelling-investigation-cybercrime
• Abstract: The ongoing technological revolution in communications and information exchange has created an entirely new form of crime: cybercrime. Cybercrime forces law-enforcement agencies to develop new areas of expertise and ways to gather and analyse evidence. The article deals with some aspects of cybercrime, with an emphasis on some areas of a judicial investigation of this phenomenon. It also describes some typical ways of committing cybercrime with regard to investigative situations. The process of acquisition, exploration and use of digital evidence is critical to the success of the prosecution of cybercriminals. In the conclusion, the author refers to the subject of the necessary training for police officers, not only in relation to cybercrime.

• Key words: cybercrime, investigation, evidence.

POŽÁR, Josef; HNÍK, Václav; KRULÍK, Oldřich. Protection of cyberspace in Western Balkan countries. Protection & Security 2014 – 2015, 3 (2, summer), ISSN 1805-5656 (2014 – 2015_B_01).
http://ochab.ezin.cz/O-a-B_2014-2015_B/2014-2015_B_01_pozar-hnik-krulik.pdf

• Abstract: Rather little-known in the Czech Republic, the paper maps entities, which are responsible for cyber security issues within the Western Balkan countries. It does not always concern establishments like CSIRT / CERT in the true sense of the word. In many cases, it is probably the first comprehensive information on this topic in the Czech language.

• Key words: Information security, Western Balkan countries, international cooperation, information exchange.

POŽÁR, Josef. Some Aspects of Cybercrime on Social Networks. Law – Security – Information. 2014, Special edition: International Conference in Jihlava. ISSN 2336-3657.
http://www.teorieib.cz/pbi/files/99-Požár_Některé%20aspekty%20KK%20na%20sociálních%20sítích.pdf

Associated PowerPoint presentations in EN: POŽÁR, Josef. Some Aspects of the Cyber Crime Committed on Children. Law – Security - Information. 2014, Special edition: International Conference in Jihlava. ISSN 2336-3657.
http://www.teorieib.cz/pbi/files/100-Požár_prezentace_AJ.pdf

• Abstract: The paper deals with some aspects of cybercrime on social networks. It highlights the threats and risks of the internet connection, a danger to juveniles and adolescents. These include breaches of confidentiality, integrity and availability. It is a flagrant violation of basic safety procedures and security features on computer networks. Prevention is possible only through relevant guidance of users at all levels of the education system.

• Key words: Cybercrime, threats, internet crime, upbringing, education.

POŽÁR, Josef. Some aspects of the Cybercrime Committed on Children. Law – Security – Information. 2014, Special edition: International Conference in Jihlava. ISSN 2336-3657.
http://www.teorieib.cz/pbi/files/85-Požár%20prezentace.pdf

Associated PowerPoint presentation in EN: POŽÁR, Josef. Some Aspects of the Cyber Crime committed on Children. Law – Security – Information. 2014, Special edition: International Conference in Jihlava. ISSN 2336-3657.
http://www.teorieib.cz/pbi/files/96-Požár_prezentace_AJ.pdf

• Abstract: The paper mentions new types and ways of committing cybercrime. It emphasises the need for training of users and managers, in order to limit the potential for a human error as well as deliberate attacks from within the organisation.

• Key words: Cybercrime, education, attacks from within.

Based on the possibilities of Operational Programme Employment 2014 - 2020 the police of the Czech Republic became involved in the implementation of projects on the theme of Effective Public Administration, which have financed and will continue to finance soft educational activities. The project Efficient Development of the Police (ERP II) has been established: implemented since 2014 and including several specific IT sessions, attended by members of the Institute of Criminalistics Prague assigned to the Department of Data and Documentation Analysis (ADD). The project 'Effective Development of the Police,' continues with its second phase (ERP II). ERP II is now preparing for the years 2015 - 2020 and will again involve still further IT training, which will be attended by members of both ADD and OKTE.

The Czech Judicial Academy:

As regards the reporting period, the Judicial Academy's educational events observe and reflect trends of crime in recent years: the loss of conventional crime in the real world and its greater displacement to a 'virtual', thus computer, world. It has to do with the fact that most criminals are generally among the thirty-year-olds and, therefore, belong to a generation that is much more familiar with the world of computer technology than previous generations of offenders. At present, serious property and economic crime is perpetrated through the internet, computers, mobile phones and similar devices. Therefore, all seminars of the Judicial Academy focused on this area could not ignore the topic of cybercrime (4-6 seminars per year).

Furthermore, there is a higher incidence of offences such as trafficking in human beings (1 seminar per year), abuse of a child for production of pornography - Section 193 of the Criminal Code of the Czech Republic (Act 40/2009 Coll.), participation in pornographic performance - Section 193a, establishing illicit contact with a child - Section 193b, through the use of cyber tools.

Regarding seminars on vice crime, it is possible to record a tendency in the sense of more active participation by victims and persons aggrieved by vice crimes committed via the internet, which was also reflected in the educational activities of the Judicial Academy. It must also be noted that seminars of the Judicial Academy, focusing on the topic of aggrieved persons and victims of crimes (5 seminars in 2014 and 4 seminars in 2015), highlighted a sensitive approach of law-enforcement authorities, which is also given by the inclusion of these victims into categories of particularly vulnerable victims pursuant to Section 2 (4)) of the Act 45/2013 Coll. on victims of crimes.

Other areas of crime which occur in cyberspace are offences linked to threatening pursuant to Sections 324, 326, 353, extortion pursuant to Section175, fraud pursuant to Section 209 and particular categories of fraud pursuant to Sections 210 and 211 (2 seminars per year). The crime committed via the internet is also relevant to the issue of seizure of assets, confiscation of proceeds of crime and the related issue of legalisation of proceeds of crime (2-3 seminars a year).

Finally, related to cybercrime are educational events focused on hate crime, extremism and terrorism (2 seminars per year).

Digital technology was also a topic of seminars focused on evidence and expert issues: exploring digital techniques in the process of producing evidence (on average 2 seminars per year).

As regards seminars focused on procedural issues, the most relevant in terms of cybercrime were seminars focusing on operational means and covert investigations, and seminars on international judicial cooperation (on average 2-3 workshops per year).

In 2014, the following educational events were organised:

22 - 24 January 2014 - a three-day seminar on the Code of Criminal Procedure, focusing, among other things, on an area linked to computer crime: gathering data from telecommunications operation and its relationship to interception and recording of telecommunication operations after the last amendment.

4 March 2014 - one-day seminar on the Code of Criminal Procedure focusing on the topic of 'Standard procedures for securing and analysing forensic data from computers and mobile devices' - a combination of technical aspects of forensic analysis and lawful procedures to secure data. Operational means and covert investigation (Section 88, Section 88 and, Section 158 of the CCP, etc.).

12 - 14 March 2014 - a two-day seminar entitled 'Right-wing extremism'. This seminar was also focused on manifestations of extremism on the internet and options for using such data for crime management. The seminar included following topics:

Current trends in the right-wing extremist scene in the Czech Republic and in Europe. The concept of self-defending democracy. Manifestations of the current extremist scene, focusing on racial and right-wing extremism. The issue of extremism in the Czech Republic from the perspective of the police - methods of investigation and producing evidence. Cooperation between Czech and foreign extremist groups. Current trends in extremist criminal activities from the perspective of a public prosecutor. The role of the expert in proving crime of extremist nature. Political radicalism and youth. Crimes committed at gatherings of right-wing extremists (with a focus on the so-called Anti-Roma marches). Criminal liability of legal persons for crimes of an extremist nature. Act on victims of crimes. Victims of hate crimes and the system of help, case studies. A system of help to victims of hate crimes pursuant to the new Act on victims.

14 to 15 April 2014 in Prague and 6 to 7 October 2014 in Kroměříž - a two-day seminar on the topic of expert examinations - criminalistics, focusing, among other, on exploring the possibilities of digital technology in the process of producing evidence:
Part I. Digital Technology - a part of a person's life, i.e. an irreplaceable source of relevant traces in the process producing evidence. Expert conclusions - answers to questions.
Part II. - the issue of communication technology (mobile phones) and skimming.

13 to 14 October 2014 - a two-day seminar on extremism, focused on two areas:
Extremists and their criminal activity in prisons. Possibilities for legal recourse with regard to left-wing extremist activities and other selected issues from the area of hate crime from the perspective of a public prosecutor. Terrorism and its conception in Czech law: current manifestations of violent extremism from the perspective of possible prosecution using counterterrorism standards. Selected casuistry in the area of terrorism in the Czech and European legal environment. Current trends on the left-wing extremist scene in the Czech Republic.

Legal aspects of sanctions of left-wing extremists in the Czech Republic with regard to already investigated cases, which occurred in the Czech Republic. A ban on attending sports, cultural and other social events and its execution - practical problems associated with imposing and execution of this sanction. The phenomenon of outlaw motorcycle clubs and criminal activity of these groups.

10 November 2014 – a one-day seminar entitled 'A victim of a crime; an aggrieved individual'
The rights of victims of crime (e.g. the issue of providing financial assistance to victims of crime by the state).Relationship between the state and entities that provide services to victims of crime. Code of Criminal Procedure in relation to victims and aggrieved individuals. Confidants and their role during procedural activities. Preliminary proceedings (especially the interim measures). Particularly vulnerable victims. The Code of Criminal Procedure in relation to victims and aggrieved parties. Confidants and their role in procedural activities. Preliminary proceedings (especially interim measures).

The issue of cautionary damage. Brief impacts of the New Civil Code on the situation of aggrieved parties in criminal proceedings. Regulation 119/2013 Coll. on the quality standards of the services provided under the Act on victims of crimes. Briefly on compensation for damage in criminal proceedings - connecting aggrieved parties and the proper exercise of their rights. Non-material damage.

Furthermore, all events mentioned above related to economic and property crimes, seminars on financial investigations, seizure of assets and confiscation of proceeds of crime and expert issues - producing evidence in relation to the exploration of the resources of digital technology.

Educational activities in 2015:

In 2015, approximately the same number of events were held as in 2014. In addition, there were also two events expressly and specifically focused on criminal activity on the internet:

22 January 2015, one-day seminar on internet crime, in Prague. Focused on information crime - trends in unlawful behaviour. Expert examination of evidence and the issue of producing evidence of cybercrime from the perspective of an expert witness. A particular topic relates to the area of interest: the issue of securing evidence on crimes committed using the internet. Typical tasks of an expert investigation (focusing on a computer analysis: methods and procedures for effective expert analysis of digital footprints - evidentiary options of digital footprints). Current developments in case-law as regards the protection of digital content. Cyber security - the issue of active defence against cyber-attacks.

29 September 2015, one-day seminar in Prague on the topic of cybercrime. Focusing on topics: Presentation by a representative of Europol - cybercrime, threats, tools, legislation. International legal assistance in cybercrime. Legal issues regarding cyber security. Taxonomy of cyber-security incidents. Presentations were given by speakers from: the European Cybercrime Centre, International Department of the Supreme Public Prosecutor's Office, National Security Authority, National Cyber-Security Centre, Institute of Law and Technology of the Faculty of Law of Masaryk University, Faculty of Informatics of Masaryk University.

8.2. Awareness-raising

The Cyber-Security Strategy identified the need for cyber-security awareness-raising, as this may be considered a precondition for cybercrime prevention. To that end, the National Security Authority organises awareness events such as the CyberCon annual conference; in addition, it prepares campaigns against cyber-bullying and organises cyber-security exercises, the results of which are made available to the wider public. At present, we are exploring the possibility of drawing funds from selected EU programmes such as Horizon 2020 or IROP. As regards the implementation of the Cyber Security Strategy, information and awareness campaigns are planned in cooperation with relevant organisations from the IT sector, and awareness-raising material is developed, tailored to the needs of various target groups, and cooperation with the private sector and with the police in their awareness-raising projects is enhanced.

Both EU and national funds are used for this purpose. Specifically, EU funds were used, for example, in the development of the National Cyber-Security Centre (GovCERT) and the Cyber-Polygon of Masaryk University in Brno.

The prestige of the Czech Republic on the international scene is also increased by the organising of national and international exercises as well as by participation in EC3 projects. The media regularly provide information and discuss ways to prevent cybercrime. The private sector operates primarily in the area of prevention, some expert departments and also in the framework of the National Centre of Excellence C4E.

Activities aimed at attracting and raising the general awareness of threats related to cybercrime are an integral part of education in cyber security. With that in mind, envisaged activities are identified in the conception of education prepared by the National Security Authority. In that context, it is necessary to underline the need for reform of elementary (primary and secondary) and high-school education, i.e. the need to integrate the issue of cyber security into general curricula in an adequate manner, both at the kindergarten / elementary (primary and secondary) school level and at universities and programmes that are not primarily technically oriented.

As regards the current system of education, from second grade at elementary schools (from age 11 or 12) the Information Technology subject is taught in the Czech Republic, in which pupils become familiar with the basics of cyber security and risks linked to the internet and social media. In this sense, further education continues at high schools, including regular visits by police spokesmen and specialists in combating cybercrime. Education in schools is also included in the National Cyber Security Strategy.

8.3. Prevention

8.3.1 National legislation/policy and other measures

Cybercrime prevention is also related to the issue of cyber security, which is coordinated by the National Security Authority; strengthening the capabilities of the police to investigate and prosecute cybercrime, and specialised training of relevant constituents of justice is, therefore, included in the Cyber Security Strategy and its Action Plan. From this perspective, relevant education in cyber security also represents an important part of prevention; the national concept of such education is currently being prepared by the National Security Authority.

The upcoming concept of education on the issue of cyber security in the Czech Republic is structured according to target groups, which cover different categories of persons from the general public (all age groups) through specifically targeted academia and public authorities to the relevant components of the executive power. The concept of education, as well as the general activity of the NBÚ / NCKB, will only support targeted activities within the competence of the authorities which are directly responsible for the investigation and prosecution of cybercrime and is intended to provide them with methodological support, rather than to take their place.

The main objectives, therefore, are:

- Education, awareness raising and information society development;
- modernising the existing primary and secondary school curricula and supporting new university study programmes designed to produce cyber security experts;
- providing relevant education and training to public administration staff involved, but not exclusively, in the field of cyber security and cybercrime.

The National Cyber Security Strategy includes in its scope all public, private and academic sectors and, in conjunction with the Action Plan of the National Cyber Security Strategy, it is a significant preventive tool in the fight against cybercrime.

NBÚ / NCKB is currently preparing a new web portal GovCERT, which will include an awareness-raising component, together with an e-learning platform for target groups identified in the abovementioned concept of education in cyber security. At the same time, the NBÚ actively cooperates with several universities in the preparation and development of new disciplines and courses on cyber security; it also participates in the activities of AFCEA, organises annual conferences for students, cooperates with the non-profit sector in the development of methodological materials and the organising of activities (e.g. the National Safer Internet Centre: projects Kyberfest, Safer Internet Day / Month, Social Web - Social Work, No Hate Speech Movement online, Get Online Week, etc., Safer Internet projects, Safely Online, eSafety Label, etc.).

The Ministry of the Interior[7] supports prevention programmes with grants under the Crime Prevention Programme in various regions and cities on an annual basis. In the period 2012 - 2015, 14 projects related to this topic were supported. Four of these projects were carried out in 2015. These are mostly preventive projects carried out in collaboration with the National Safer Internet Centre: Safely Online and Regions for Safe Internet.
Support for these projects will continue further under the abovementioned grant programme.

Every year (this year being the sixth), an expert conference is organised in the Senate of the Parliament of the Czech Republic. The conference is organised under the auspices of the Chairman of the Committee on Legal and Constitutional Affairs in collaboration with the National Safer Internet Centre. This year, the conference was held on October 20 2015, with the theme 'Cooperation of the police and the non-profit sector against cybercrime in practice.' The central themes of the event were the threats associated with online communication and ways to solve them.

[7] Prevention of cybercrime is also included in the Evaluation of the Crime Prevention Strategy for 2012 – 2015 and the new Crime Prevention Strategy for 2016 – 2020. The government will adopt these documents at the end of January 2016. The Action Plan for the new Strategy for 2016 – 2020 is to be submitted by the end of June 2016 and will also include specific objectives as regards the issue of cybercrime. A meeting of the National Committee for Crime Prevention, which will be dedicated to the prevention of cybercrime, is planned for 28 January 2016.

The conference focused on the employees of the police of the Czech Republic and the municipal police, police prevention specialists, investigators and other experts from public administration, social workers, teachers and ICT school methodologists, educational consultants, a staff of public and municipal libraries, NGO representatives, the interested public and the media.

Similarly (also for the sixth time in 2015), there was a conference of the 'KYBERPSYCHO' series with the title 'Addressing cybercrime and electronic violence against children' held on 23 November 2015. This conference was organised by the National Safer Internet Centre with the support of the City of Prague and the Ministry of the Interior and the CZ.NIC association. In particular, the conference focused on a practical knowledge of professionals working with juveniles.

In October 2015, there was a conference under the auspices of the Regions for Safer Internet project called 'Latest findings in the field of cybercrime' held in Jihlava.

The conference brought together experts from the security forces, specialists in the fields of prevention and education, information and communication technology, government, and the corporate and non-profit sectors, as well as professionals working with children and youth - especially prevention specialists and social workers. Presentations were given by qualified representatives of the Department of Information Crime of the police of the Czech Republic, the Child Protection Authority (OSPOD), the Czech School Inspectorate, internet service providers, and other specialists.

The contributions focused, inter alia, on the legal status and powers of schools, OSPOD, and the police in solving and prosecuting electronic violence among pupils and targeting teachers, as well as on cooperation between these entities. Also discussed was the criminal-law treatment of the phenomena associated with online pathology and criminal liability of juvenile perpetrators of internet crime and their legal representatives, the possibility of prevention of these negative phenomena, ways to assist victims of cybercrime and other related phenomena.

On 6 and 7 October 2015, the first edition of the national cyber-security exercise Cyber Czech 2015 took place; it was organised by the National Security Authority (NBÚ) in collaboration with the Institute of Computer Science of Masaryk University Brno (ÚVT).

The exercise took place in the special environment of the Cyber Exercise & Research Platform (KYPO) on the premises of the ÚVT. KYPO is the result of research, development and innovation by the Security Research Programme of the Czech Republic in the period 2010 - 2015 (BV II / 2-VS).

The exercise involved practical simulations on specially adapted machines, with the aim of countering cyber-attacks and solving the resulting events and incidents. The intention of the exercise was to practise technical skills and information-sharing between teams of trainees. The exercise was based on a prepared scenario reflecting real incidents and the application of the Act on Cyber Security. The scenario and background story are entirely fictional and were created by NBÚ with the support of ÚVT.

Another cyber-security exercise, entitled Cyber Czech 2015, was held at the seat of the National Security Authority from 16 to 18 June 2015. The exercise was prepared and organised in cooperation with the European Cyber-Security Initiative and the European Defence Agency.

The aim of the exercise, in the form of a round table, was to examine the state's ability to make decisions and effectively use available resources to address a crisis in cyberspace. The exercise focused on practice in using communication channels, information exchange and the ability to coordinate cooperation in solving cyber-security incidents.

The realistically prepared scenario formed a continuous storyline, gradually escalating from simple cyber-attacks to a combination with kinetic operations. Within each phase of the exercise, trainees were assigned tasks that needed to be solved, from the perspective of their competence and authority, as effectively as possible. The content of individual tasks and time requirements within the exercise were increased as the scenario developed.

In October 2014, a joint conference entitled 'Kyberpsycho in the viewfinder of the police: cooperation in preventing and addressing cybercrime' was held under the auspices of the National Safer Internet Centre in cooperation with the City of Prague. Traditionally, the conference is a part of the autumn activities of the NCBI and was organised within the European cyber-security month campaign.

The Kyberpsycho conference, held with the support of the Capital of Prague within the European Cyber Security Month, is a traditional technical conference focused on prevention and tackling cybercrime and cyber violence. It is designed specifically for police officers, ICT specialists of state and local administration, ICT school coordinators and assisting entities as well as relevant professional public.

The conference offered the latest research findings of prominent Czech and foreign institutions and focused on specific emerging threats in the online environment. It also covered the strategic development and training in cybercrime, existing criminal legislation and cooperation of the police and other entities with providers of online services.

Contributions were devoted to topics such as:

- cybercrime in police practice, a system of intervention and cooperation;
- cyber-attacks from the perspective of ICT units of state and local administration;
- cyber security from the perspective of the NBU, new legislation and its implications;

- cybercrime from the perspective of service providers and associated legislation;
- professional training of future, as well as existing, police officers on the issue of cybercrime;
- professional training of experts on the issue of cyber security;
- hotlines: A European network of INHOPE hotlines and its cooperation with the police.

The conference was accompanied by a range of interesting activities:

- exhibition of organisations providing support and services to victims of cybercrime and cyber-violence;
- exhibition of activities focused on the safety of users from the perspective of online service providers;
- seminar 'Don't be afraid of social networks';
- theatre performance 'Generation FB' with a subsequent discussion with representatives of Facebook.

The main objective of the C4E is to enhance general awareness of work in the area of prevention and investigation of cybercrime and the efficiency of that work, by:

- strengthening awareness of cybercrime via conferences and workshops organised for partners, target groups and other publics;
- enhancing the training and know-how of target groups, in particular, the police, prosecutors and judges;
- preparing / developing efficient and available tools for target groups, particularly the police but also administrators of critical infrastructure;
- developing and distributing guidelines, best practices and standards in the area of electronic evidence (obtaining, analysis, reporting, use), investigating relevant cases, bringing digital evidence before the court.

C4E's fundamental task is to support the Czech Republic in the fight against cybercrime. The intent of C4E is to bring together the best academic experts in the field of cybercrime, e.g. in the areas of obtaining, analysis, investigation and execution of electronic evidence. C4E thus aims to become a centre of knowledge, i.e. a specific type of think-tank. All these efforts are carried out with close international cooperation. C4E wants to become one of the key members of the international network of similar national centres. Most of the outcomes of its work will be developed in cooperation and coordination of these centres.

In May 2015, a conference on cyber security entitled CyberCon 2015 and focusing on topics such as cyber-battlefields, cybercrime, legal aspects of cyber security, cyber-threats and society, was held in Brno, organised by the National Security Authority.

A seminar carried out in cooperation with the US Federal Bureau of Investigation (FBI), was held at the Police Academy in Prague from 19 to 23 May 2014 following a cooperation agreement in the field of cybercrime and corruption, which was concluded within the framework of a visit of the former 1st Deputy Minister of the Interior in the US on 6 and 7 November 2012, and after the first similar training programme from 7 to 14 October 2012 (standard expertise training).

The seminar represented an advanced level (advanced training) of the previous training effort within the ICWG (International Cyber Working Group) and was prepared by the Security Policy and Crime Prevention Department of the Ministry of the Interior and the Department of Information Crime of the Police Presidium of the Czech Republic in cooperation with the Police Academy of the Czech Republic, which provided suitable premises on the basis of a series of meetings between the Security Policy and Crime Prevention Department with the US representatives over the course of 2013 and early 2014.

The specific content of this strictly technically-oriented seminar was open to the needs of the Czech experts who participated (in this case police officers assigned to the detection and investigation of cybercrime, a representative of the Security Policy and Crime Prevention Department and a representative of the Security Information Service). The substantive content of the seminar corresponded with the training and methodological process of investigating cybercrime by FBI agents.

The seminar was held from 19 to 23 May 2014, and was led by two FBI Special Agents from the Houston Area Cyber Crime Task Force; it was intended for specialists with advanced technical knowledge of computer science and its security framework and current forensic ICT tools. The seminar was practically oriented and ran for five working days on a stand-alone basis; the FBI experts presented realistic cases, which were then solved by the participants.

Public Private Partnership (PPP)

The Czech Republic does use Public Private Partnership (PPP) in preventing and combating cybercrime. There is a whole range of projects that aim to disseminate information and prevention with regard to both users and organisations, with the aim of raising knowledge and awareness of the issues of cyber security and cybercrime.

An important role is played by the Ministry of Education – from primary schools to universities. The police of the Czech Republic, judicial authorities and government agencies participate in lectures, conferences and workshops. The National Cyber Security Strategy for the period from 2015 to 2020 is also very important in this regard, as it directly assumes and establishes cooperation with the private sector.

The main objectives are to:

- cooperate with the private sector;
- continue engaging in cooperation with the private sector and raise awareness of the work and activities of the National Security Authority in cyber security;
- develop, in cooperation with the private entities, unified safety norms, standardise cooperation and establish a mandatory level of security for operators of critical information infrastructure;
- ensure, in cooperation with the private sector, a cyberspace providing a secure environment for sharing information, research and development, and ensure a safe information infrastructure stimulating private businesses with the aim of promoting the competitiveness of all private businesses in the Czech Republic and protecting their investments;
- educate and raise awareness within the private sector of cyber security issues. Provide necessary guidance to private entities on appropriate behaviour, not only in emergency situations, i.e. cyber-incidents, but also during everyday activities;
- raise confidence between the private sector and the state, including by the creation of a national platform/system for sharing information on threats, incidents, and actual situations of insecurity.

At the moment, the National Security Authority is not implementing any specific form of PPP. However, cooperation takes place on an ad hoc basis within the framework of specific projects. The National Security Authority cooperates closely with the CZ.NIC association, which serves as the National CERT, and also, for example, with Microsoft in connection with operating the Botnet Feed tool, and with the Czech Banking Association. The Action Plan for the Cyber Security Strategy assumes further deepening of cooperation, including on research projects.

8.4. Conclusions

- Presentations on training for the police, prosecution and judiciary were delivered to the evaluation team. Regarding the police, cybercrime studies are part of several modules as it is *per se* a cross-sector issue. A project is on going on raising awareness on prevention of cyber bullying in schools. The objective is to draft guidelines to unify terminology of cybercrime for the police, and improve communication with social services for children.
- The Police Academy also takes cybercrime into account in lifelong training for officers. These training activities are also organised with CEPOL (many of the courses are the result of the EMPACT initiative).
- The Judicial Academy also organises training activities on cybercrime in cooperation with the Police Academy. The evaluation team understood that workshops are being organised on crimes committed via internet, with the participation of police officers and prosecutors. National authorities explained to the evaluation team that these workshops could be extended to judges as well.
- National authorities should further raise the awareness of those involved in cyber security so as to achieve improvements in the security of, for example, e-shops, retailers' servers and payment gateways.
- National authorities should further strengthen cooperation with the private sector, e.g. the banking sector, telecommunication operators and internet providers.
- In order to ensure a higher level of prevention, national authorities should consider establishing a specialised police unit whose main task should be systematic cyber-patrols on the public internet, and also on the deep web.
- The police (Police Academy) and NGOs have prepared lectures and presentations on the 'deep web' and the 'dark net', for teachers and school counsellors. The goal is to provide information to the personnel who are in most touch with children and to provide guidance as to how to deal with this information.

- The evaluation team encourages positive cooperation with relevant stakeholders, governmental bodies and NGOs, educational institutions, social services, financial institutions, tourism chambers, internet industries (internet service providers, information companies and others) and media in order to find the best possible solutions in awareness raising and prevention cooperation.
- National authorities should continue with preventive campaigns and awareness rising on different aspects of cybercrime, and such campaigns should be directed at various groups of people and institutions, with special attention to children from their first experiences of using information technologies.
- The National Centre for Safer Internet runs many preventive, educational and awareness raising projects, and initiatives for many different groups, e.g. children, parents, teachers, adults, seniors, social workers, police officers and others. As a good practice the evaluation team must cite the initiative dedicated to seniors. A peer-to-peer concept is taken: several small groups of seniors (elder population) were trained or given relevant information on the internet and related topics. After their training they return to their peers, where they are able to pass the information to their own groups. The goal is to eliminate concrete problems of older people with a variety of modern informational technologies and to be aware of the possibilities offered by them.
- The Police Academy in CZ organises sessions on VID and on protecting children online. In this matter they take an operational-investigative approach, where they gather relevant police officers from the whole country and observe, analyse and investigate crimes against the sexual integrity of children. In this situation Interpol's Crimes against Children Unit brought the VID lab (laboratory on images of real child-victims to be identified). Afterwards several children were identified and several new items of information were sent to other countries to secure the abused children concerned. The evaluation team considers this approach a good practice.
- Saferinternet.cz has two highlighted projects called iSejf (isejf.cz) and KyberFest programme. iSejf is an information website with teaching materials for parents and teachers interested in safe internet use. KyberFest was a two-day festival in November 2015, with different programmes for the wider public and for schools.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from the Czech Republic

In recent years, the Czech Republic has made great progress in its capacity to prevent and combat cybercrime. The awareness of the population is gradually increasing, although it has not yet succeeded at all levels - the deficit remains mainly among older generations.

There is a plan for a further increase in the numbers of police specialists on the issue of cybercrime, including budgetary measures on necessary technology at workplaces as well as the expansion and intensification of education and international cooperation.

The necessary legislation has been adopted and will further be updated as needed. This also includes the process of alignment with EU standards. Government, national, university and private CERT / CSIRT teams have been established.

There is well-established cooperation between the government, university, and private sectors. Overall, we assess the general ability of the Czech Republic in the area of prevention and combating cybercrime as very good. However, it is desirable to strengthen and improve preparedness by increasing the resources in order to increase the capacity to monitor trends in cybercrime and related misuse of technology.

An example of good practice that may be mentioned is the establishment and development of cybercrime departments staffed by police specialists. What is important is the continuous updating of legislation and prevention programmes. Without close cooperation between the government, private and university sector, the situation would be difficult.

Another important need is to provide personal, technical and educational support to experts and professional staff at the Institute of Criminalistics Prague and in departments of forensic technique and expertise, who, based on the requirements of law-enforcement authorities, provide expert assessments and examinations in the context of cybercrime.

At the moment, there are lively discussions as regards the legislation on retention and provision of electronic data (Data Retention). National authorities consider that the data retention period is too short in the Czech Republic (six months) and it would be appropriate to extend the circle of persons required to retain data. The ratification of the Council of Europe Convention on Cybercrime by the greatest possible number of countries would also be very useful.

9.2. Recommendations

As regards the practical implementation and operation of the Framework Decision and the Directives, the expert team involved in the evaluation of the Czech Republic was able to satisfactorily review the system in the Czech Republic.

The Czech Republic should follow up on the recommendations in this report 18 months after the evaluation and report on the progress to the Working Party on General Affairs, including Evaluations (GENVAL).

The evaluation team thought it appropriate to make a number of suggestions for the attention of the Czech authorities. Related recommendations based on the various good practices are also addressed to the EU, its institutions and agencies, and to Europol in particular.

9.2.1 Recommendations to the Czech Republic

1. Consider collecting further statistical relevant data for child sexual exploitation and online card offences.
2. National authorities should proceed with police reorganisation and make relevant steps in terms of increasing the number of posts, more effective and intensive training of police specialists, and sufficient technical equipment. This applies to police officers involved in the fight against cybercrime, as well as those from economic crime departments and units with wide competences.
3. Consider creating a network of police officers specialising in cybercrime, following the example of the cyber-prosecutors' national network.
4. Consider joining the EMPACT initiative on cybercrime, in order to obtain relevant information, knowledge and intelligence for reorganisation and for the workflow of its police officers
5. Encourage the national authorities to improve use of the ICSE DB in order to facilitate the identification of child victims.
6. National authorities should further strengthen cooperation between the Regional Directorates, the Territorial Departments and the national Unit for Combating Organised Crime in combating cybercrime, as well as international police cooperation.
7. Continue to support the work of the National Centre for Safer Internet NGO and other initiatives, in particular in partnership with the police, and to promote public-private cooperation on a more regular basis.
8. Continue to promote and disseminate research results, including studies and materials in the area of digital evidence and data retention (for example by disseminating an extract in English of the Guidebook on Digital Evidence in Criminal Proceedings).

9. Continue organising the Cyber Czech exercise and inviting experts from other Member States.

10. Continue to organise training activities on the whole life-cycle of cybercrime cases with police officers, prosecutors and private sector and consider including judges as well.

9.2.2 Recommendations to the European Union, its institutions, and to other Member States

11. EU institutions should encourage and further support initiatives to organise training activities to cover the whole life-cycle of cybercrime cases by targeting police, prosecutors and judges.

12. Member States should be encouraged to appoint prosecutors and judges as experts to take part in the evaluation visits to other Member States.

13. Member States should be encouraged to present practical cases of cybercrime within the scope of the questionnaire during the evaluation visits as a way to illustrate and expand on the replies they have provided to the Questionnaire.

9.2.3 Recommendations to Eurojust/Europol/ENISA

14. Eurojust should continue supporting national authorities in the setting up of a EU judicial cybercrime network. Eurojust should further consider providing support to such network.

15. Eurojust should continue to expand possibilities to provide JIT funding.

9.2.4. Good practices in the Czech Republic

16. The General Prosecutors Office has produced a Handbook for Prosecutors containing more than 30 Annexes, including 38 templates, one of which focuses on a request for securing electronic data.
17. The Czech Cyber Crime Centre of Excellence has written a Guidebook on digital evidence in criminal proceedings, including a general overview of Czech procedural law relating to digital evidence handling and a guidance on handling specific types of evidence (e.g. email, personal profile data, website, mobile devices).
18. The Czech Cyber Crime Centre of Excellence has also produced a book on interception and data retention, including an analysis of the legislation and case-law related to interception of electronic communication and procedural tools for LEAs and international cooperation.
19. In October 2015 the Masaryk University Brno and the National Security Authority organised a joint Cyber Czech exercise focusing on defending a critical information structure. Participants were given the roles of CSIRT members and asked to recover compromised networks, secure simulated infrastructure, investigate attacks and cooperate with media and organisers.
20. A public prosecutors' network on cybercrime was recently created at national level.

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT

Monday 8 February 206

- PM arrival GENVAL experts in Prague
- 20.00 - 21.30 Informal meeting and introductions of experts team

Tuesday, 9 February 2016

9.30 - 9.45 *Official welcome speech* - Mr David Chovanec, director of the Security Policy and crime Prevention Department, Ministry of the Interior

9.45 - 10.15 *General information about cybercrime, main trends* - mr Petr Holý, Crisis Management Unit, Security Policy and Crime Prevention Department

10.15 - 10.45

Structure of the law enforcement and judicial authorities - Mr Petr Habarta, Security Law Unit Security Policy and Crime Prevention Department

Ongoing reorganisation of the Police - Col. Milan Komárek, Deputy Director, Unit for Combating Organised Crime of the Criminal Police and Investigation Service

10.45 - 11.00 Coffee break

11.00 - 12.30

Methodology, analysis and support of regional sections; investigation of relevant areas of cybercrime - Col. Milan Komárek, Deputy Director, Unit for Combating Organised Crime of the Criminal Police and Investigation Service and Lt. Col. Jiří Ráž, Head of Department, Department of Cybercrime Investigation and Analysis (V8), Unit for Combating Organised Crime of the Criminal Police and Investigation Service

Practical experience from regional sections - Maj. Stanislav Kovárník, Head of Unit, Cybercrime Unit Analytics and Cybercrime Department, Regional Directorate of the Police of the Southern Moravian Region

12.30 - 13.30 Lunch

13.30 - 14.15 *International cooperation, Interpol/Europol National* Units - Lt. Col. Petr Farník, Department of International Police Cooperation of the Police Presidium of the Czech Republic, Col.

Miroslav Tichák, Head of Unit, Department of International Police Cooperation of the Police Presidium of the Czech Republic

14.15 - 15.00 Expert/forensics activities, problematic areas - Col. Ľuboš Kothaj, Deputy Director, Institute of Criminalistics Prague, Col. Jaroslav Hüttl, Head of Unit, Data Analysis and Documentation Department of Technical & Natural Sciences Institute of Criminalistics Prague, Lt. Martin Záruba, Institute of Criminalistics Prague

15.00 - 15.15 Coffee break

15.15 - 17.00 *Introduction to criminal justice system, transposition of the Budapest convention, procedural issues* - Mr Tomáš Holý, Legislative Department, Ministry of Justice, Ms Kateřina Šrytrová, International Department for Criminal Matters, Ministry of Justice, Ms Lenká Habrnálová, Department of International Cooperation and the EU, Ministry of Justice, Mr Michael Vrtek, Criminal Division of the Supreme Court

17.00 - 17.30 Final remarks and conclusions

Wednesday 10 February 2016

7. 30 Transfer to Brno

10.30 - 12.00 *Strategic, legal and technical aspects of ensuring cybersecurity*, National Cyber Security Centre

12.00 - 14.00 Lunch and transfer

14.00 - 15.00 *Education, research and development in the area of cybercrime (tools, best practices)* - Mr Pavel Čeleda, Head of Department, Security Department, Institute of Computer Science

15.00 - 15.15 Coffee break

15.15 - 16.330 *Unique environment for researching and developing methods for mitigating attacks on critical information infrastructure, simulation on KYPO - Cyber exercise and research platform* - Mr Pavel Čeleda, Head of Department, Security Department, Institute of Computer Science

17.00 - 19.00 *Status and activities of the Supreme Public Prosecutor' Office* - Mr Pavel Zeman, Supreme Public Prosecutor, Mr Petr Klement, Department of Serious Economic and Financial Crime, Ms Světlana Kloučková, Head of Department , International Affairs Department, Mr Marek Vagai, Regional Public Prosecutor's Office in Brno and Mr Michal Píš, Metropolitan Public Prosecutor's Office in Brno

19.00 - 20.30 Dinner

20.30 Transfer to Prague

Thursday 11 February 2016

10.30 - 11.30 *Awareness raising, prevention and reduction of possible risks linked to the use of online environment, cooperation within non-profit sector, cooperation with INSAFE and INHOPE, project Saferinternet.cz* - Jiří Palyza, Executive Director, National Centre for Safer Internet

12.00 - 13.00 Lunch

13.00 - 14.15 *Introduction to CSIRT team, coordination of response to security threats in computer networks, cooperation with internet service providers, project FENIX* - Zuzana Duračinská, Computer Security Specialist, CSIRT.CZ Security Team and Jiří Průša, Project Coordinator, CZ.NIC association

14.15 - 14.30 Coffee break

14.30 - 15.30 *Training for law enforcement and judicial authorities*, Col. Milan Komárek, Deputy Director, Unit for Combating Organised Crime of the Criminal Police and Investigation Service, Lt. Col. Jiří Ráž, Head of Department, Department of Cybercrime Investigation and Analysis, Ms Helena Lišuchová , Department of International Cooperation and the EU, Ms Lenká Habrnálová, Department of International Cooperation and the EU, plk. Mgr. Lukáš Habich, Deputy Director, Police College and Secondary Police School of the Ministry of the Interior in Prague, Lt. Col. Jan Kolouch, Police Academy of the Czech Republic in Prague

15.30 - 16.30 *Final remarks and conclusions*

19.00 Farewell dinner

Friday 12 February 2016

9.30 - 10. 30 - *Evaluation of the mission*

ANNEX B: PERSONS INTERVIEWED/MET

Prague (Ministry of the Interior of the Czech Republic, Tuesday 9th and Thursday 11th February 2016):

MINISTRY OF THE INTERIOR OF THE CZECH REPUBLIC	
Mr Jiří Nováček	1st Deputy Minister of the Interior of the Czech Republic (Internal Security Section)
Ms Lenka Šindýlková *Head of Unit*	Police Training Unit Department of Security Research and Police Training
Mr Petr Klíma	Police Training Unit Department of Security Research and Police Training
Mr Petr Habarta	Security Law Unit Security Policy and Crime Prevention Department
Mr Petr Holý	Crisis Management Unit Security Policy and Crime Prevention Department
Ms Julie Buzalková	Crisis Management Unit Security Policy and Crime Prevention Department
Ms Zuzana Smolová	Crisis Management Unit Security Policy and Crime Prevention Department
Ms Simona Virglová	Security Law Unit Security Policy and Crime Prevention Department

POLICE OF THE CZECH REPUBLIC	
Col. Milan Komárek *Deputy Director*	Unit for Combating Organised Crime of the Criminal Police and Investigation Service
Lt. Col. Jiří Ráž *Head of Department*	Department of Cybercrime Investigation and Analysis (V8) Unit for Combating Organised Crime of the Criminal Police and Investigation Service
Col. Miroslav Tichák *Head of Unit*	Department of International Police Cooperation of the Police Presidium of the Czech Republic
Lt. Col. Petr Farník	Department of International Police Cooperation of the Police Presidium of the Czech Republic
Col. Ľuboš Kothaj *Deputy Director*	Institute of Criminalistics Prague

Col. Jaroslav Hüttl *Head of Unit*	**Data Analysis and Documentation Department of Technical & Natural Sciences Institute of Criminalistics Prague**
Lt. Martin Záruba	Institute of Criminalistics Prague
Maj. Stanislav Kovárník *Head of Unit*	Cybercrime Unit Analytics and Cybercrime Department Regional Directorate of the Police of the Southern Moravian Region
MINISTRY OF JUSTICE OF THE CZECH REPUBLIC	
Ms Helena Lišuchová *Head of Department*	Department of International Cooperation and the EU
Ms Lenká Habrnálová	Department of International Cooperation and the EU
Ms Kateřina Šrytrová	International Department for Criminal Matters
Mr Tomáš Holý	Legislative Department

SUPREME COURT OF THE CZECH REPUBLIC	
Mr Michael Vrtek	Criminal Division of the Supreme Court of the Czech Republic

NATIONAL CENTRE FOR SAFER INTERNET	
Jiří Palyza *Executive Director*	National Centre for Safer Internet

CZ.NIC z. s. p. o.	
Zuzana Duračinská *Computer Security Specialist*	CSIRT.CZ Security Team
Jiří Průša *Project Coordinator*	CZ.NIC association

POLICE ACADEMY OF THE CZECH REPUBLIC IN PRAGUE	
Lt. Col. Jan Kolouch	Department of Criminal Law

POLICE COLLEGE AND SECONDARY POLICE SCHOOL OF THE MINISTRY OF THE INTERIOR IN PRAGUE	
plk. Mgr. Lukáš Habich *Deputy Director*	Police College and Secondary Police School of the Ministry of the Interior in Prague

MASARYK UNIVERSITY BRNO	
Mr Pavel Čeleda *Head of Department*	Security Department Institute of Computer Science
+ other representatives of the Czech CyberCrime Centre of Excellence (C4E) and the KYPO Project	

SUPREME PUBLIC PROSECUTOR'S OFFICE	
Ms Světlana Kloučková *Head of Department*	International Affairs Department
Mr Petr Klement	Department of Serious Economic and Financial Crime
Mr Pavel Zeman *Supreme Public Prosecutor*	
Mr Marek Vagai	Regional Public Prosecutor's Office in Brno
Mr Michal Píš	Metropolitan Public Prosecutor's Office in Brno

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	CZECH REPUBLIC OR ACRONYM IN ORIGINAL LANGUAGE	CZECH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
AFCEA			Armed Forces Communications and Electronic Associations
AIJC			Act on International Judicial Cooperation
BIOS			Basic Input Output System
CAM			Child Abuse Material
CC			Criminal Code
CCP			Code of Criminal Procedures
CEPOL			European Police College
CERT			Computer Emergency Response Team
CIRT			Computer Incident Response Team
CSIRT			Cyber Security Incident Response Team
DDoS			Distributed Denial of Service
DMCA			Digital Millennium Copyright Act
EAW			European Arrest Warrant
EC			European Commission
EC3			European Cyber Crime Centre

ECTEG			European Cybercrime Training and Education Group
EJN			European Judicial Network
EMPACT			European Multidisciplinary Platform Against Criminal Threats
ENISA			European Union Agency for Network and Information Security
EPE			Europol Platform of Experts
FBI			Federal Bureau of Investigations
FP			Focal Point
GENVAL			General Evaluation
ICSE DB			International Child Sexual Exploitation Image Database
ICWG			International Cyber Working Group
INHOPE			International Association of internet Hotlines
IP			Internet Protocol
ISEC			Prevention of and Fight against Crime
ISF-P			Internal Security Fund for Police
ISP			International Service Provider
JHA			Justice and Home Affairs
JIT			Joint Investigation Team
KÚP			Institute of Criminalistics Prague
LEAs			Law Enforcement Authorities
MIS			Major Information System

MLA			Mutual Legal Assistance
MoI			Ministry of Interior
NGO			Non-Governmental Organisation
NIS			National Information System
OKTE			Department of Forensic Technique and Expertise
NSA			National Security Authority
PPP			Public Private Partnership
RETN			Regional Educational Television Network
SIS			Schengen Information System
ÚOOZ SKPV			Unit for Combating Organised Crime of the Criminal Police and Investigation Service
USA			United States of America
VID			Victim Identification Process
VIS			Visa Information System
V8			Department of Cybercrime Investigation and Analysis