Council of the
European Union

Brussels, 22 September 2015
(OR. en)

9761/1/15
REV 1 DCL 1

GENVAL 18
CYBER 52

DECLASSIFICATION

of document:	9761/1/15 REV 1
dated:	7 September 2015
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Slovakia

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, 7 September 2015
(OR. en)

9761/1/15
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 18
CYBER 52

REPORT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Slovakia

ANNEX

Table of Contents

1 Executive summary ____ 4

2 Introduction ____ 6

3 General matters and Structures ____ 9

3.1 National cyber security strategy ____ 9
3.2 National priorities with regard to cybercrime ____ 10
3.3 Statistics on cybercrime ____ 12
3.3.1 Main trends leading to cybercrime ____ 15
3.3.2 Number of registered cases of cyber criminality ____ 15
3.4 Domestic budget allocated to prevent and fight against cybercrime and support from EU funding ____ 15
3.5 Conclusions ____ 16

4 NATIONAL STRUCTURES ____ 18

4.1 Judiciary (prosecution and courts) 18
4.1.1 Internal structure ____ 18
4.1.2 Capacity and obstacles for successful prosecution ____ 18
4.2 Law enforcement authorities ____ 21
4.3 Other authorities/institutions/public-private partnership ____ 24
4.4 Cooperation and coordination at national level ____ 25
4.4.1 Legal or policy obligations ____ 25
4.4.2 Resources allocated to improve cooperation ____ 26
4.5 Conclusions ____ 28

5 Legal aspects ____ 29

5.1 Substantive criminal law pertaining to cybercrime ____ 29
5.1.1 Council of Europe Convention on Cybercrime ____ 29
5.1.2 Description of national legislation ____ 29
5.2 Procedural issues ____ 36
5.2.1 Investigative Techniques ____ 38
5.2.2 Forensics and Encryption ____ 38
5.2.3 E-Evidence ____ 40
5.4 Jurisdiction ____ 59
5.4.1 Principles applied to the investigation of cybercrime ____ 59
5.4.2 Rules in case of conflicts of jurisdiction and referral to Eurojust ____ 61
5.4.3 Jurisdiction for acts of cybercrime committed in the "cloud" ____ 62
5.4.4 Perception of the Slovak Republic with regard to legal framework to combat cybercrime ____ 63
5.5 Conclusions ____ 64

8 Training, awareness-raising and prevention ____ 93

8.1 Specific training ____ 93
8.2 Awareness-raising ____ 98
8.3 Prevention ____ 104
8.3.1 National legislation/policy and other measures ____ 104
8.3.2 Public Private Partnership (PPP) ____ 117
8.4 Conclusions ____ 117

9 Final remarks and Recommendations _____ 119

9.1. Suggestions and considerations from Slovakia 119
9.2 Recommendations 124
9.2.1 Recommendations to Slovakia 124
9.2.2 Recommendations to the European Union, its institutions, and to other Member States 128
9.2.3 Recommendations to Eurojust/Europol/ENISA 129

Annex A: Programme for the on-site visit and persons interviewed/met _____ 130

Annex B: Persons interviewed/met _____ 132

Annex C: List of abbreviations/glossary of terms _____ 137

1 EXECUTIVE SUMMARY

- The visit to Slovakia took place between 16 and 20 February 2015. The mission was organised very well by the hosting authorities, including logistics.

- The Evaluation Team has been able to meet and interview a large number of very committed representatives from the Ministry of Interior and the Police Force, in particular of the Cybercrime Unit, the Ministry of Justice, the General Prosecutor's Office, regional prosecutors´ offices and district prosecutors´ offices, the Ministry of Finance and CSIRT-SK, the National Security Authority, the Intelligence Service etc. The Slovak authorities made also possible interviews with third party entities, which was highly appreciated.

- The choice of representatives with which the Team could engage was appropriate, albeit it could have benefitted from the additional presence of representatives from the Courts.

- In Slovakia the Cybersecurity strategy is well advanced and currently being renewed ; however a comprehensive strategy on the fight against cybercrime and a dedicated action plan would be recommended.

- At the moment Cybercrime is not treated by law as a special category of crimes, which is also why statistics on cybercrime cases are not fully available. Slovak authorities highlighted that collecting statistics on cybercrime is cumbersome; however efforts are currently being made to upgrade the accuracy and interoperability of relevant public databases; in this context they mentioned the existence of different obligations from international and EU bodies that are not using the same common denominator as a basis to collect data on cybercrime.

- There are no specialised units in the Police or Prosecution Service carrying out investigations or prosecutions on cybercrime. However, Slovakia has set up recently a Cybercrime Unit for the main purposes of carrying out criminal intelligence activities, and support local authorities in their investigations by a) supporting exchange of information, ensuring that lessons learnt from casework are collected, b) facilitate training in this field. This Unit is a small one (currently consisting of 8 people), but the Evaluation Team was told that it is going to grow in time in terms of capacity and missions.

- Like other Member States, following the Court of Justice annulment decision of 8 April 2014, the Constitutional Court of Slovakia has issued a resolution (No. US 10.2014 of 23 April 2014) producing negative impact on detection, investigation and prosecution of computer crimes. The non-preservation of data following this resolution in connection with the lack of obligation to retain data is considerably hampering legal assistance in cybercrime cases.

- As a positive step towards swift action, Slovak prosecutorial authorities developed together with USA authorities a form to request expedited preservation of computer data.

- The evaluation team felt, and the Slovak authorities acknowledged that there is room for improvement in the area of training activities offered to practitioners. However the training sessions organised by the various academies seem to be of good quality.

- Particularly noticeable is the effort Slovakia put in the prevention and awareness of cybercrime, in primis by supporting the extremely interesting activities of the non-profit organisation E-Slovensko.

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, on 3 October 2013 the Working Party on General Matters including Evaluations (GENVAL) decided that the seventh round of mutual evaluations should be devoted to the practical implementation and operation of the European polices on preventing 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 which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas – cyber attacks, online child sexual abuse/pornography and online card fraud – and 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 and replacing Council Framework Decision 2004/68/JHA[2] (transposition deadline 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (transposition deadline 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] anticipated the swift ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 by all Member States and emphasised in their preamble that "the EU does not call for the creation of new international legal instruments for cyber issues". The Convention is supplemented by a Protocol on acts of xenophobia and racism committed through computer systems[6].

Experience from past evaluations shows that Member States will be in different positions regarding the implementation of the relevant legal instruments, and the current evaluation process could also provide useful input to Member States that may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary and not to focus solely on the implementation of various instruments relating to fighting cybercrime, but also on the 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 those organisations is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to the suppression of cyber attacks, fraud and child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to people who fall victim to cybercrime.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Slovakia was the fifth 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 to delegations from the Chairman of GENVAL on 28 January 2014.

[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 January 2003, entered into force on 1 March 2006.

The evaluation teams consist of three national experts, supported by one or 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 Slovakia were Mr Jan Fort (Czech Republic), Mr Rogério Bravo (Portugal) and Mr Savin Svet (Slovenia) - the latter being excused. Two observers were present: Ms Anna Danieli (Eurojust) and Mr Gary McEwen (Europol/EC3), together with Ms Claire Rocheteau from the General Secretariat of the Council. The Commission and ENISA were not represented.

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 Slovakia between 17 and 20 February 2015, and on the detailed replies from the Slovak authorities to the evaluation questionnaire, together with their detailed answers to ensuing follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National cyber security strategy

A new *Conception of Cyber Security of the Slovak Republic* is being prepared under auspices of the Government Office of the Slovak Republic in cooperation with: the National Security Authority, Ministry of Interior, Ministry of Finance, Ministry of Defence, Ministry of Foreign Affairs, Ministry of Education, Science, Research and Sport, Ministry of Transport, Construction and Regional Development of the Slovak Republic and Slovak intelligence service. The Conception of Cyber Security of the Slovak Republic will be based on the Strategy of Cyber Security of the European Union and the Strategy of Cyber Defence of NATO. It should contain the measures in the area of prevention, reaction and restoration for the purposes of creation of the security awareness, raising of the level of the national and international cooperation and capacity building.

However, the major document that currently addresses the information security of the information systems of the public administration is entitled "**National Strategy for Information Security in the Slovak Republic**"[7]. This document was adopted by Resolution of the Government of the Slovak Republic No 570/2008, and it includes the sum and substance, competences, suggested direction, priorities and actions to achieve the goal. The document also provides description of measures to be taken to ensure the protection of digital space of the Slovak Republic. These include in particular the measures against information leakage and unauthorised use, impairment of data integrity, violation of citizens' rights to privacy, protection against damaging and exploitation of information and communication systems, damaging a good reputation of the governmental and private institutions, as well as the measures for enforcement of relevant legal regulations of the Slovak Republic and the European Union.

[7] The National Strategy for Information Security in the Slovak Republic in English language can be found on the Internet on the following website: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf

Seven fundamental national strategic priorities in the area of information security are defined. They include:

- protection of human rights and freedoms in connection with using the national information and communication infrastructure,
- raising awareness and capabilities in the field of information security,
- building of safe cyber environment,
- streamlining of information security management,
- ensuring sufficient security of the national information and communication infrastructure,
- national and international cooperation,
- extending national competence.

The National Strategy for Information Security of the Slovak Republic was supplemented by the Action Plan adopted by Resolution of the Government of the Slovak Republic No 46/2010. The Action Plan, available only in Slovak language, can be found on the Internet on the following website: http://informatizacia.sk/ext_dok-akcny_plan_k_strategii_pre_ib/6790c

3.2 National priorities with regard to cybercrime

The Slovak Republic has not yet adopted a specialised comprehensive document dealing exclusively with cybercrime. Slovak authorities indicated that, however, the objectives and methods of combating cybercrime are part of the general strategies and action plans, for example, the *Strategy on the Prevention of Crime and Other Antisocial Activities in the Slovak Republic for the years 2012 - 2015*. According to the said strategy the reduction of rate and seriousness of cybercrime has been set out as a priority in the Slovak Republic.

Legal aspects. Slovak authorities stressed that a national priority in the fight against cybercrime consists in sufficient transposition of the Directive of the European Parliament and of the Council 2013/40/EU on Attacks against Information Systems, which will ensure more effective enforcement of the law and the identification of a wider complex of cybercrime acts. It means an extension of the legal regulation under Section 247 of the Criminal Code, as well as making the legal regulation of criminal liability of legal entities more precise under a separate law. At the same time it will result in more effective prosecution of perpetrators of such criminal offences.

Operational aspects. The Government Program of the Slovak Republic for the period 2012-2016 underlines, in its Article 4, the need "*to increase efforts to combat (...) computer crime and abuse of Internet"* and for *"an efficient and modern method* (which) *will contribute to raise the level of cybersecurity in the European Union*."

The Minister of Interior issued an Order elaborating on the above mentioned Government Program; it includes:

- Task. 23 "*Submit a draft of personal and technical development in area of combating against cybercrime in order to achieve a standard institutional level with other EU member states in terms of the Police Force to ensure consistent implementation of international commitments of the Slovak Republic in the field of computer crime"*;
- Task.42 "*Ensure the training of police officers aimed at detecting, documenting, summary investigation and investigation with emphasis on computer crime and car crime"*.

In their reply to the GENVAL questionnaire Slovak authorities mentioned also that national priorities in the field of combating cybercrime are currently focused on the following types of crime:

- Fight against online child sexual exploitation (CSE) and fight against possession, dissemination and production of child abusive material (CAM);
- Fight against cyberattacks;
- Fight against online payment card fraud.

Slovak authorities also mentioned that priorities in the area of international cooperation include the proper implementation of the Convention on Cybercrime and addressing practical problems of the Convention application (currently with the Swiss Confederation). The Slovak Republic participates in the work of the Committee of Parties to the Convention on Cybercrime (T-CY). International cooperation is also provided under other international agreements, legal acts adopted within the European Union, or on a reciprocal basis.

3.3 Statistics on cybercrime

The term "cybercrime" is not explicitly defined in the Slovak Criminal Code or in a similar normative legal act. The Criminal Code, however, recognizes and stipulates the facts of individual criminal offences, which together form cybercrime in Slovakia. These are criminal offences having a computer as a target, but also criminal offences committed by means of a computer.

Statistics in the Prosecution Service are compiled separately from the statistics of the Police Force, Slovak courts, or the private sector. There is not separate statistics of cybercrime. Under the current system of statistics compilation, it is not possible to show all the criminal offences related to computer crime. In particular, when crimes are committed using a computer as a tool (especially property crime – the criminal offence of fraud under Section 221 of the Criminal Code) and using the computer system is not an element of the facts of the case, it is not reflected in the statistics.

Prosecution services. The statistics used in the Prosecution Service in the system called *Patrícia* apply a catalogue of crimes in which the code "700" implies cybercrime. However, since the term "cybercrime" as defined in Table 1 on page 6 of the questionnaire can be understood as a wide range of different types of crime, as a general practice prosecutors enter into the statistics the code related to the crime on question but not the code 700 implying that the crime was committed through a computer.

Having such method of keeping records, it is impossible to determine which different types of criminal offences were committed by computer and thus they fall under the concept of "cybercrime" as defined in the questionnaire.

Police services. Statistics in the Interior Ministry are compiled separately at the Section of Information Systems Administration of the Presidium of the Police Force in the information system called the Crime Registration and Statistics System. After the establishment of the Cybercrime Unit of the Criminal Police Bureau at the Presidium of the Police Force, for the purposes of cybercrime recording by virtue of the Convention on Cybercrime, there was transposed the European Parliament and Council Directive 2013/40/EU on Attacks against Information Systems (hereinafter referred to as "DAIS"), which replaced Council Framework Decision 2005/222/JHA and the statistics system was adjusted as to 1 April 2014 based on amending letter No 28.

On the basis of these changes there were by virtue of the Criminal Code modified statistics for:

- Misuse of devices (Art. 5 of the Convention on Cybercrime, Section 247 par. 1 subpar. c) of the Criminal Code)
- Computer-related forgery (Art. 7 of the Convention on Cybercrime, Section 247 par. 1 subpar. d) of the Criminal Code)
- Computer-related fraud (Art. 8 of the Convention on Cybercrime, Section 226 of the Criminal Code)
- Criminal offences related to child pornography (Art. 9 of the Convention on Cybercrime, Sections 368, 370 of the Criminal Code)
- Criminal offences related to infringements of copyright and related rights (Art. 10 of the Convention on Cybercrime, Section 283 of the Criminal Code)
- Criminal offences related to content (using cyber networks, in a public manner)
- Criminal offences related to child pornography (Art. 9 of the Convention on Cybercrime, Section 369 of the Criminal Code))
- Criminal offences concerning extremism (set forth in Section 140a of the Criminal Code)
- Other criminal offences (Sections 194a, 196, 197, 198, 201a, 249a/2c, 360a/1c, 376 of the Criminal Code)
- Criminal offences against information systems (critical infrastructure)
- Illegal access to information systems (Art. 3 of DAIS, Section 247 par. 1 of the Criminal Code)
- Illegal data interception (Art. 6 of DAIS, Section 247 par. 2 subpar. a) of the Criminal Code)
- Illegal data interference (Art. 5 of DAIS, Section 247 par. 1 subpar. c) of the Criminal Code)

There were added statistics for:

- Illegal system interference (Art. 4 of DAIS, Section 247 par. 1 subpar. d) of the Criminal Code)
- Tool used for committing offences (Art. 7 of DAIS, Section 247 par. 1 subpar. c) of the Criminal Code)

Judicial services. Here statistics fall within the competence of the Section of Statistics and Reporting at the Ministry of Justice of the Slovak Republic and are kept separately from both Prosecution and LEA statistics.

Private sector. Slovak authorities indicated that they were not able to comment on the share of input of private sector into public statistics.

Slovak authorities acknowledged the need to pay special attention to the issues of statistical data. They mentioned that integration of statistics is currently being reviewed by the Inter-ministerial Expert Coordinating Body for Combating Crime. Upon its resolution No 14 of 4 December 2014, an inter-ministerial working group of experts was set up, whose activities are aimed at addressing the issue of interconnecting various relevant registers (including statistics), and it consists of permanent members - representatives of the Presidium of the Police Force, Ministry of the Interior of the Slovak Republic, General Prosecutor's Office of the Slovak Republic, Ministry of Defence of the Slovak Republic - Military Police, Slovak Intelligence Service, Ministry of Finance of the Slovak Republic - Financial Directorate of the Slovak Republic (Tax and Customs Section, Financial Administration Criminal Office), Ministry of Justice of the Slovak Republic and the Corps of Prison and Court Guard.

Slovak authorities find it necessary to analyse the requirements of the Council of Europe, United Nations and of the European Union altogether, and to integrate output statistics of the police, prosecution service and the courts, including the use of a common methodology. New information systems are currently introduced, in the Prosecution Service within the project OPIS. UNODC has adopted a new international classification of crimes, which should be taken into account. In relation to the obligations arising out of the Council of Europe activities, it is also needed to improve the management of statistical data. Slovak authorities underlined that obligations imposed by directives at the level of the European Union including, inter alia, statistical data, suffer from a lack of harmonised methodology, methods for data collection and evaluation.

3.3.1 Main trends leading to cybercrime

The statistical data are not produced in the extent which would enable to determine the share of such criminality towards the total criminality in the Slovak Republic. However Slovak authorities consider clear that the share of cybercrime is increasing, taking into account the increase of a spread of technical devices and the access to internet.

In their reply to the questionnaire they specified that the percentage of online fraud with payment cards may be estimated at about 35% out of the summary of criminal offences concerning payment cards total incidence of the criminal offence defined under Section 219 of the Criminal Code (for the illustration, there are 1674 crimes concerning payment cards in the Slovak Republic in the year 2014).

3.3.2 Number of registered cases of cyber criminality

Official statistics were provided by Slovak authorities within the questionnaire; however the number of reported cases appeared to be fairly low and the evaluation team was not able to check their consistency.

During the visit it was also indicated that the police have the capability to, and do, flag cases under various crime types for statistical purposes; however at some stage this marker is lost as the case progresses due to system incompatibilities. As mentioned above the prosecutors are also able to similarly mark a case in their own statistical system but this is not routinely done.

CSIRT.SK does produce good statistics on cyber threats however again these bear little correlation with the statistics that the police provided, despite “daily” communication with the Presidium. The statistics related to a wide variety of sophisticated cyberattacks, however the only example of a case where the CSIRT and the Cyber Crime Unit had collaborated related to "ID Theft", "data leakage" and DDos attack".

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

Under the European Commission’s general call for proposals entitled “Prevention of and Fight against Crime - ISEC", the Cybercrime Unit of the Criminal Police Bureau at the Presidium of the

Police Force was approved grant EC No HOME/2013/ISEC/AG/INT /4000005300 for a project entitled "Building Capacity for Combating Cybercrime / Cybercrime Training".

3.5 Conclusions

- A National Strategy for Information Security in the Slovak Republic, adopted in 2008, is currently in force; this document appears to be of very good quality; a new "Conception of Cyber Security of the Slovak Republic" is being prepared under auspices of the Government Office.

- There is no specific national strategy in place concerning the fight against cybercrime. The evaluation team is of the opinion that such a document would be of help to the competent authorities in identifying and achieving their objectives.

- Slovak law enforcement, prosecution and judicial authorities use different statistical databases managed with different criteria. Offences under the category of "Cybercrime" are not systematically marked as such. As a result there are significant discrepancies on statistical figures presented to the evaluation team, notably when comparing those of the police forces with the prosecution office results.

- The Slovak authorities are aware of these problems and currently working on the development of interconnected databases to be managed with a common methodology (an inter-ministerial working group of experts was set up in December 2014).

- There is also a discrepancy between the statistics on cyber threats provided by the CSIRT and the very low volume of cases dealt with by the police; it is unclear to the evaluation team where the disconnect is. During the visit the Slovak authorities indicated that Slovakia is not a major

source or target of sophisticated cybercrime – although CSIRT's figures suggest otherwise. However, in relation to payment fraud, it is the view of Europol that Slovakia is indeed not a target for organised crimes groups compared to some of its neighbours.

- The Slovak authorities also mentioned, and the expert team acknowledged, that there is a lack of harmonised methodology, methods for data collection and evaluation at EU level, and that the definition of common statistical denominators in the field of cybercrime would be of great help.

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

Although the Slovak Republic has established the Office of Special Prosecution and the Specialised Criminal Court, these authorities have not been designed to deal with cybercrime.

There is no specialised authority to deal with cybercrime acts within the internal judiciary structure of the Slovak Republic.

Cybercrime acts are dealt with by prosecution offices and courts of all instances.

4.1.2 Capacity and obstacles for successful prosecution

For now no specific measures have been taken in Slovakia for building capacity to prosecute cybercrimes, although during a working meeting of prosecutors - specialists in juvenile crimes and crimes against children, a proposal for specialisation of the prosecutors in crimes committed through computer systems was put forward. The aspects of such specialisation and its possible form are to be reviewed by the Prosecution Service.

Slovak authorities said in general, there is a need to increase the number of staff members in the Prosecution Service which has been suffering from negative consequences of legislative change in 2011 that led to the cancellation of the positions of trainee prosecutors what resulted in a motion filed with the Constitutional Court. The above legislative change caused discontinuation of the natural process of recruiting new prosecutors what negatively affected performance of the Prosecution Service. Act n° 322/2014 reintroduced the positions of trainee prosecutors. It will therefore be feasible to fill vacant posts of prosecutors over several years span.

As for the main obstacles to successful prosecution of cybercrimes, the Slovak authorities said cybercrime is undoubtedly the type of crime where the conviction of a particular person believed to have committed such crime is the process of extremely demanding nature due to its sophisticated character. There is very often uncertainty about the end result of the investigation. They mentioned that, for example, during the inquiry of a case of manufacturing, distribution and possession of child pornography, the information on the payment for downloading child pornography was secured, the owner of the bank card was identified, a house search was performed, an expert opinion was drawn up, but the offender has not yet been identified.

The Slovak authorities also mentioned that, after the Court of Justice of the European Union decided on 8 April 2014 that the Directive 2006/24/EC of 15 March 2006 (so called "Data retention" Directive) is null and void, a major barrier for successful investigation and prosecution of this crime consists in the current absence of legal regulation governing the retention of computerised data. As a follow-up to this ruling, the Constitutional Court of the Slovak Republic has suspended the effect of several provisions of the national law implementing the Directive, with a view to assessing the compliance of these legal provisions with the national Constitution, the Charter of Fundamental Rights and Freedoms, the Convention for the Protection of Human Rights and Fundamental Freedoms, the Charter of Fundamental Rights of the European Union.

Slovak authorities stressed the negative impact of the above mentioned decisions on the detection, investigation and prosecution of computer crimes in the Slovak Republic, as well as on cross-border communication (limited capacity to provide / obtain evidence). Particularly in the context of these decisions resulting in non-preservation of some data or in their retention only for a limited short period of time, the securing of computer data through application of the standard procedures (legal assistance, translation, and suchlike.) is almost impossible.

They also pointed out that, time being a crucial factor in cybercrime investigations, and due to the absence of obligation to retain data even the modern instruments governing legal assistance in this area are not sufficient enough; a further problem is that, in many cases, a criminal offence is reported after a certain lapse of time what frustrate the ability of the law enforcement agencies to react. A positive shift towards accelerated action is a standardized request for urgent preservation of computer data what is a good basis for accelerated cooperation, in particular with the USA.

In their opinion, the proposals for direct cross-border access to data without using legal assistance or judicial cooperation do not offer the solution to this problem.

They mentioned another set of difficulties related to international cooperation, especially to the limited application of obligations arising out of international treaties by some Parties to the relevant conventions (the application of the *de minimis* rule) although such a restriction is not legally justifiable and makes the punishment of perpetrators of certain offences difficult (money obtained by deception though advertising fictitious car sales, etc.). In addition to the *de minimis* rule, the obligation imposed upon the requested state to bear the costs associated with the provision of computer data (e.g. IP addresses) also makes the cooperation difficult.

Further barriers mentioned to successful cooperation represent constitutional limits of some states regarding the protection of freedom of expression that make it impossible to execute a request for legal assistance in such criminal matters as, for example, the criminal offences of defamation, infringement of rights, or criminal offences related to extremist materials.

In order to effectively investigate these crimes, it is necessary to provide the police authorities, prosecution service, courts, forensic institutes with sufficient technical equipment, with enhanced training in this field (including international) and with a reasonable level of specialisation. Training delivered at the EU level (e.g. using European Judicial Training Network, Europol and Interpol) could also be an option.

Other reported problems are caused by delays in drawing up of specialist knowledge statements and expert opinions assessing seized computer data due to insufficient capacity of the specialised police department. It should be noted that due to the problems caused by experts who failed to work out their expert opinions in time, certain criminal prosecutions had to be discontinued on the ground that they were barred by the statutes of limitations.

Technical barriers of investigations consist in technical impossibility to review and monitor communications within Facebook, Skype, Viber, etc., as well as the problems related to overcoming barriers to access to computer data, which are often encrypted or otherwise protected (in one practical example, Slovak prosecutors faced the difficulty of accessing to the content data encrypted probably by the tool DM crypt with LUKS extension or encryption software tool TrueCrypt 7.1a). Slovak authorities encounter the cases where individuals deny to disclose passwords to decrypt the content what in turn prevents the expert examination of the content. No option exists to force a person to divulge his password. Such a constraint emerged in the particular case of child pornography.

4.2 Law enforcement authorities

There is no specialised body for investigation of cybercrime established within the Police Force of the Slovak Republic. The investigation of cybercrime is carried out by local investigators who investigate autonomously.

However, a Cybercrime Unit has been established within the Criminal Police Bureau of the Presidium of the Police Force for criminal intelligence activities, support investigations and for purposes of international cooperation.

The Cybercrime Unit of the Criminal Police Bureau at the Presidium of the Police Force (CCU)

This new department for combating cybercrime has been created as from 1 July 2013 under the Ministry of the Interior and falls within the structures of the Criminal Police Bureau of the Presidium of the Police Force. The tasks assigned to the Criminal Police of the Presidium of the Police Force, as set forth under Regulation of the President of the Police Force No 16/2008 on the Structure of Organisation of the Presidium of the Police Force, shall apply mutatis mutandis to this new Department. Officers of the Criminal Police Bureau of the Presidium of the Police Force of the Slovak Republic are involved in the investigation of serious criminal offences of infringement of

intellectual property rights and cybercrime, which have links to more regions or to the whole territory of the Slovak Republic. They cooperate in particular with Internet service providers, domain administrators, associations for the protection of copyright and similar rights, forensic and expertise units, and in this way they create the conditions for addressing the challenges related to intellectual property rights and cybercrime.

In general, all the above tasks may be summarised into the core one – to provide methodological guidance, detect and investigate cybercrime, as well as to gather experience on the situation related to cybercrime, including online child abuse.

The issues related to credit cards fall within the competence of the Economic Crime Department of the Criminal Police Bureau at the Presidium of the Police Force. Slovak authorities plan to include also this card crime unit in the CCU.

The Police Force also hosts an Institute of Forensic Science responsible for collecting digital tracks and carrying out forensic examination. The Institute is involved in technical expertise and training activities in the field of criminalistics. Expertise is carried out on request of law enforcement agencies and courts. The Institute of Forensic science of the Police Force does not have an exclusive position in expertise for criminal proceedings. A number of private experts meet the legal requirements and may be involved in the criminal proceedings. it was said during the on-site visit that, as a general practice a priority is given to the Institute, however competent authorities regularly make use of private computer forensics companies, due to limited capacity within their own capability. The evaluation team believes this situation is not uncommon among Member States.

To the question as to the main obstacles to successful investigation of cybercrimes, Slovak authorities answered as follows.

- In offenses relating to the copyright infringement, specifying the damage caused by the unlawful action, is problematic.
- In many cases finding IP addresses of the offender is not sufficient, either due to the dynamic nature of the address, or possibly due to the use of public Wi-Fi networks. Another factor complicating the work is that entities providing free Wi-Fi as an added value to other services and activities (café, store, etc.) do not hold the traffic data for the time period sufficient to identify at least the terminal, which was used for communication.

- We know from practice that within the legal international assistance on obtaining electronic evidence is not fast enough. For example, if it was faster, the data could have resulted to obtain additional evidence in Slovakia in the particular case but due to the transmission after 13 months, the evidence (due to the period of storing in the Slovak Republic) did not exist anymore (speaking of the cases from the period before the decision of the European Court of Justice). It seems that providing the data after several months can not lead to an effective prosecution.
- The response from judicial structures to the urgent need to obtain court order to identify IP address users and practice of different courts varies.
- The lack of first responders to secure and/or seize electronic evidence affects ulterior results in cybercrime investigations.
- There is a need to develop handbook of best practices for police officers for each procedure that will comprehensively clarify the issues of cybercrime.
- The complexity of the examination the volume of the data.
- Before securing the evidence, the risk of high offender's technical abilities is underestimated, this means underestimation of the risk of suppression of computer data perpetrator (e.g. encryption). Possibility of interception of telecommunications before securing the digital data is not used.
- The information obtained from the Internet service provider is incomplete or incorrectly required.
- Because of the respect of the investigators to the cybercrime problematic the questions for forensic expert and the procedure at the scene and the investigation in complicated cases are not consulted in all cases with the specialized police services designed to combat cybercrime or with older forensic experts from the Institute of Forensic Science or with the private forensic expert registered in the field Forensic IT science.
- In case of doubts about the contents of the information, it happens sometimes that no consultation takes place with staff of the specialized units designated for it in order to verify how the information should be used or where to obtain further information necessary to assess the lessons learned.

4.3 Other authorities/institutions/public-private partnership

In addition to the judiciary and law enforcement agencies, other government bodies are involved in the prevention and fight against cybercrime as well. Particularly Ministry of Finance designs and issues legislative and strategic documents in the field of information security, technical standards for the protection of national information and communication infrastructure, and, it is involved in the education and awareness activities. It is also a national point of contact for reporting security incidents and provides assistance and incident response services, whereas these specific activities are done by CSIRT.SK. Other special authorities dealing with cyber incidents are SK CSIRC (the National Security Authority of the Slovak Republic like a contact point for NATO) and MIL CERT (the Ministry of Defence of the Slovak Republic). Intelligence services are also involved in the fight against cybercrime. Their missions are governed by Act No. 46/1993 Coll. on the Slovak Information Service as amended and Act No. 198/1994 Coll. on Military Intelligence as amended.

The Ministry of Finances is very active in cybercrime matters, for instance by having drawn in 2008 a document in the field of information security, and by contributing to establish CSIRT.SK the same year. It appears to be the main body in charge of strategy for information security. Already since 2001 the Ministry of Finance was the central body for information society (e.g. e-government). The Ministry was also responsible for the National Strategy. Due to rapid evolvement of cyber matters, the team was informed that the Ministry **is participating on preparation of a new draft strategy document** that it is hoped will be adopted in 2015. It also started a pilot project on cooperation with academia and private sector aiming at educating public administration.

The Computer Security Incident Response Team Slovakia (CSIRT.SK).

CSIRT.SK is the national and governmental Computer Emergency Response Team (CERT) of Slovakia. It was established by the Slovak Government Resolution No 479/2009 of 1 July 2009 in accordance with the National Strategy for Information Security in the Slovak Republic of 2008 and is placed under the Ministry of Finance of the Slovak Republic.

Its main tasks include the prevention and monitoring of security incidents in the information systems of governmental agencies and in the critical information infrastructure of the country. The CSIRT.SK staff provide the services related to managing security incidents and dealing with their aftermath, with subsequent recovery of these information systems in cooperation with their owners and the operators of national information and communication infrastructure, telecommunications operators, Internet service providers and other governmental authorities.

CSIRT.SK is also involved in raising public awareness in selected areas of information security, actively cooperate with international organisations and represent the Slovak Republic in the field of information security at the international level.

During the visit the evaluation team was told that CSIRT.SK would soon be given certain powers with a view to mitigating security incidents. This could, potentially, overlap with police powers under an on-going investigation, however this is intended to be avoided by planned interministerial consultations and legal harmonisation.

4.4 Cooperation and coordination at national level

4.4.1 Legal or policy obligations

Slovak authorities underlined that, as regards the cooperation with other institutions / bodies, the Ministry of the Interior cooperate actively in particular with the organisation CSIRT.SK (Computer Security Incident Response Team Slovakia)[8]. They stated also that the Slovak legislation, however, is not focused solely on suppression of crime through applying the provisions of the Criminal Code and Code of Criminal Procedure. The separate legislation also provides for specific conditions for standardisation of information security, and for the management of the security of information and communication technologies in the cyberspace.

It is worth mentioning that Governmental authorities, higher territorial units, municipalities and other legal entities and natural persons are obliged to provide law enforcement agencies and courts synergies in the performance of their duties related to criminal proceedings.

[8] https://www.csirt.gov.sk/doc/CSIRT.SK.pdf

4.4.2 Resources allocated to improve cooperation

Memorandum of understanding between the Datacentre (CSIRT.SK) and National Security Authority of the Slovak Republic (SK CSIRC) in the field of information security in the Slovak Republic, was signed in 2013. The subject of the Memorandum is closely cooperation and sharing information both centres dealing with the cyber security incidents.

At the moment the contract between Ministry of Interior of the Slovak Republic dealing with cybercrime and Ministry of Finance of the Slovak Republic responsible for running national computer security incident response team CSIRT.SK is in the adoption process. The main aim of the contract is to define a mechanism of cooperation, system of early warnings and process of capacity and information sharing in the prevention of and fight against cybercrime.

The National Security Analysis Centre (NBAC)

NBAC serves for the purpose of sharing information, early warning and response to security incidents, including cyber threats. NBAC was established on 1 January 2013 under the project, which was approved by Government Resolution no. 75 of 7 March 2012. The initiator of the project was the Slovak Information Service (SIS) that took responsibility of it. Establishing the NBAC in the organizational structure of SIS is based on the tasks set out in the NAP on Combating Terrorism in the Slovak Republic, for the period 2011 - 2014. NBAC activities are controlled by the Government, as stated in the Resolution no. 700 of 12 December 2012 and in the amendment of the approved Government Resolution no. 337 of 26 June 2013. NBAC is defined as analytical, communication and cooperation nationwide SIS department in the field of security threats. Its main tasks include complex analytical evaluation of security incidents based on reports received from the national authorities of the Slovak Republic, monitoring the security situation in the Slovak Republic from the exposed resources, and providing analytical products of security threats in the Slovak Republic to the intended recipients.

NBAC operates as analytical department based on the active participation of key government bodies of the Slovak Republic, working in the security field – Slovak Intelligence Service, Ministry of Defence, Ministry of Interior, Ministry of Finance, Ministry of Foreign and European Affairs and National Security Authority. Other participating organizations provide information support by reporting the security incidents recorded. Information products processed in the analytical department of NBAC are provided to all participants.

Law enforcement authorities in Slovakia are not entitled to monitor activities related to the means of payment in the banking sector. This does not prevent the exchange of good practices. In fact cooperation with SBA includes exchange of malware samples and other practical information. Within the active cooperation in the field of software attacks, there is a form of cooperation built between Police Force and companies dealing with the indication of malware. This ensures the exchange of information and subsequent investigation procedures or prevention, if necessary. Police Force of the Slovak Republic said they have sufficient technical equipment for combating this crime but a specialised unit combating this kind of crime does not exist within the structure.

An extremely effective measure developed in Slovakia to limit the access of criminal groups to financial data and credentials, skimming devises and software was the establishment of the already mentioned Safety Commission for payment cards with SBA and addressing identified individual cases on this platform. Based on the active cooperation of the members of the Commission, including the rapid exchange of information identified several threats of attacks related to credit cards. Preventive measures are adopted almost exclusively on the side of each commercial bank individually. These measures, respectively details of such measures are not provided to the Police Force.

4.5 Conclusions

- In the Slovak Republic the following authorities are involved in the prevention of and fight against cybercrime: Ministry of the Interior (Police Force), Slovak Information Service, Military Intelligence, Office for Personal Data Protection, National Security Authority, Telecommunications Office, Financial Administration Criminal Office, Ministry of Finance, Financial Directorate, tax authorities, customs authorities, Ministry of Transport, Construction and Regional Development, Council for Broadcasting and Retransmission and the Industrial Property Office.

- Cybercrime cases are dealt with by district and regional police forces, prosecution offices and courts in accordance with their jurisdiction.

- The Cybercrime unit (CCU) based with the Presidium of the Police Force provides an intelligence and support function to competent police services. Currently only CSE and cyber attacks are under the umbrella of the CCU. However motions are in place to also include payment card frauds.

- Commendable efforts are currently made within the public administration, the law enforcement agencies and the General Prosecution Office to create or improve coordination mechanisms in the interest of preventing and combating cyber criminality. These efforts should be continued and enhanced.

- The complexity of the forensic examination, and the backlog caused by the volume of the data compromises effective investigations and prosecutions and ultimately the course of justice.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on Cybercrime

The Slovak Republic is a Party to the CoE Convention on Cybercrime, the Convention itself was ratified by the Slovak Republic on 12 December 2007 and it has entered into force on 1 May 2008.

5.1.2 Description of national legislation

Criminal liability of legal persons. The legislation currently in force in Slovakia provides for the criminal liability of legal persons with legal consequences in the form of protective measures (Section 83a of the Criminal Code, Confiscation of an amount of money and 83b of the Criminal Code, Confiscation of property). A separate law on criminal liability of legal persons that introduces the so-called real criminal liability of legal persons and significantly extends the range of sanctions, has been drafted. It is proposed to come into effect on 1 July 2015.

Serious and large-scale cyberattacks. The Criminal Code provides for stricter sanctions based on the specific criteria set forth under qualified elements of the criminal offences. To determine the amount of damages, amount of benefit, value of a thing and the scale of the offence, the general provisions of the Criminal Code (Sections 124 - 126 of the Criminal Code)[9] shall apply. Majority of

[9] Damage

Section 124

(1) For the purposes of this Act, damage shall mean harm to property or actual loss of assets or prejudice to the rights of the injured party or other harm, which has a causal relationship with the criminal offence irrespective of whether the harm has been caused to a thing or to the rights. For the purposes of this Act, damage shall also mean advantage gained in causal relationship with the criminal offence.

(2) Damage within the meaning of paragraph 1 shall also mean the loss of profit to which the injured party, considering the circumstances and his personal situation, would otherwise be entitled or could reasonably expect to obtain.

(3) In case of criminal offences against the environment, damage shall mean the combined environmental harm and property damage; property damage shall also comprise the costs of restoring the environment to its original state. In case of the criminal offence of illegal handling of waste pursuant to Section 302, the scope of the offence shall be determined on the basis of customary price charged at the time and place of the offence for the collection, transport, export, import, recycling, disposal or dumping of waste, and the price charged for the removal of waste from the site that is not designated for dumping.

Section 125

(1) Small damage shall mean the damage amounting to more than € 266. Larger damage shall mean the damage which is at least ten times higher than the aforesaid amount. Substantial damage shall mean the damage which is at least one hundred times higher than the aforesaid amount. Large-scale damage shall mean the damage which is at least five hundred times higher than the aforesaid amount. These criteria shall also be used to determine the amount of benefit, the value of a thing, and the scope of the offence.

(2) Where the Special Part of this Act requires that the basic elements of the criminal offence include infliction of damage as a property consequence of the criminal offence without specifying its amount, such damage shall be understood as at least a small damage.

Section 126

(1) The amount of damage shall be determined on the basis of customary price at which the damaged thing is sold at the time and place of the offence. Where the amount of damage cannot be determined as stated above, it shall be determined on the basis of costs that would be reasonably incurred to obtain an identical or a similar thing, or to restore the thing to its original state.

the above crimes are adjudicated in more severe manner (stricter penalty) if the criminal offence caused more serious consequence, for example in the form of substantial damage, large-scale damage, or if death was caused through its commission, or if the offence was committed acting in a more serious manner (Section 138), against a protected person (Section 139), by reason of specific motivation, or in public (Section 122 par. 2), etc.

The valid wording of Section 247 of the Criminal Code, Misuse of information stored on data carrier, makes the imposition of a stricter sanction possible for this criminal offence if through its commission substantial or large-scale damage was caused, or if the perpetrator is a member of a dangerous group.

Legislation concerning cybercrime is variable. A cyber attack is classified as "serious" or "extensive" depending on the method of its commission. For example, the extent of the effects of damage and misuse of recording on information carrier is reason to apply a stricter prison sanctions. If the offender causes substantial damage, he shall be liable to a term of imprisonment of one to five years. If the offender causes large-scale damage, he shall be liable to a term of imprisonment of three to eight years. Substantial harm attracts the term of imprisonment of three to eight years. The same applies, if the offender commits such offence as a member of a dangerous group. This also applies to other crimes committed by interference with the software (the criminal offence of unjust enrichment pursuant to Section 226 of the Criminal Code, the criminal offence of misrepresentation of business records pursuant to Section 259 of the Criminal Code). The interfering with hardware or software is more heavily sanctioned if the offender caused particularly serious disturbance in the running of economy of the state or other particularly serious consequence.

(2) In case of environmental damage, harm to protected species of animals and plants, specimens or wood species, or damage to the things protected as monuments, or the things of historical, artistic or scientific value, the degree of harm or the amount of damage shall be determined also taking account of the value of such thing as defined by a law, or other generally binding legal act issued on the basis of a law.

(3) Where the amount of damage or the degree of harm cannot be determined by applying any of the provisions of paragraphs 1 or 2, or where there are serious reasons to doubt the accuracy of the amount of damage or the degree of harm thus determined, they shall be established on the basis of a professional opinion or a certificate issued by a legal entity whose competence or line of activity offers a guarantee of objective determination of damage or harm; otherwise, the amount of damage shall be determined on the basis of an expert opinion.

Minor cases. For the cases which accomplish the elements of the criminal offences referred to under Special Part of the Criminal Code, the procedures followed when dealing with minor cases of cybercrime do not differ from those followed when dealing with crimes of a different nature. An alternative solution is a discontinuation of criminal prosecution in pre-trial, or even in court proceedings, through the so-called diversions - conditional stay of criminal prosecution or termination of criminal prosecution after the reconciliation agreement has been approved with the injured party. In court proceedings, an alternative is a waiver of punishment (Section 40 of the Criminal Court) or imposition of sentence other than a imprisonment sentence (Section 39 of the Criminal Code). When selecting the alternative method of treating a criminal case, seriousness of the crime is a crucial aspect finding its reflection in the severity of punishment. For the sake of illustration, the criminal offence of possession of child pornography under Section 370 of the Criminal is frequently committed on a computer. The legislator classifies this criminal offence as a minor one what means that all the above alternatives come into consideration.

Minor offences that do not reach the seriousness of the criminal offence may be sanctioned as infractions under the general misdemeanour law, i.e. Act No 372/1990 Coll. on Misdemeanours as amended (infractions in the field of culture, concerning the right of access to information, those against public order, of extremist nature, those of disturbing the peace and quiet of occupants of a dwelling house) or infractions under a separate regulation (e.g. infractions under Section 78 of Act No 215/2004 on Protection of Classified Information and on amending and supplementing certain acts.

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

The Slovak Republic currently prepares a law on information security, the adoption whereof is planned in 2015. This Act shall govern:

a) competence of the government authorities and the rights and obligations of natural persons and legal entities in the field of information and communication technologies,
b) status and scope of competence of a specialised unit for solving of computer security incidents in the digital space of the Slovak Republic CSIRT.SK, and the requirements to be met by the operators of services for solving of computer security incidents,
c) classification of information and categorization of the information systems in the public administration,
d) security of information systems in the public administration during their life cycle,
e) information security management,
f) minimum requirements for the security of information systems in the public administration,
g) education in the field of information security,
h) framework for notification and solving of computer security incidents, minimum requirements for internet security
i) checking of the security of information systems in the public administration and information system security auditing.

The reason for this legislation under preparation is the transposition of the above mentioned Directive, which will ensure more effective law enforcement and the identification of a wider complex of unlawful acts in the area of cybercrime. It consists of an extension of the regulation under Section 247 of the Criminal Code, as well as more precise rules concerning the criminal liability of legal persons under a separate law.

As for the time being, criminal offences related to information systems, in particular cyber attacks, are as follows in the Slovak legislation.

- Section 196 of the Criminal Code, Breach of mailing secret
- Section 219 of the Criminal Code, Unlawful manufacturing and enjoyment of electronic payment means of other payment card;
- Section 221 of the Criminal Code, Fraud;
- Section 226 of the Criminal Code, Unjust enrichment (unlawful interventions into all sale and services systems, e.g. in cases of unlawful credit for online betting);
- Section 247 of the Criminal Code, Misuse of information stored on data carrier;
- Section 283 of the Criminal Code, Infringement of copyright.

- Criminal liability of offenders of all the above criminal offences requires intention of the offender;
- For the purposes of an a appropriate legal qualification and determination of the sanction the ratio of mitigating / aggravating circumstances pursuant to Sections 36 through 38 of the Criminal Code is considered;
- Minimum/maximum criminal sanctions:

  Section 196 of the Criminal Code – 0 to 10 years of imprisonment

  Section 219 of the Criminal Code – 1 to 12 years of imprisonment

  Section 221 of the Criminal Code – 0 to 15 years of imprisonment

  Section 247 of the Criminal Code – 6 months to 8 years of imprisonment

  Section 283 of the Criminal Code – 0 to 8 years of imprisonment
- Multiple offences/recidivism always lead to tougher sanctions;
- Inciting, aiding and abetting, instigating and attempted criminal offences are regulated under Sections 14 and 21 of the Criminal Code

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

Criminal offences related to the content, in particular criminal offences of online sexual exploitation of children and child pornography, are as follows.

- Section 368 of the Criminal Code, Production of child pornography;
- Section 369 of the Criminal Code, Dissemination of child pornography;
- Section 370 of the Criminal Code, Possession of child pornography and participation in child pornography performance;
- Sections 201a and 201b of the Criminal Code, Sexual abuse (grooming).

- Criminal liability of offenders of all the above criminal offences requires intention of the offender;
- Minimum/maximum criminal sanctions:

  Section 368 of the Criminal Code – 4 up to 20 years of imprisonment

  Section 369 of the Criminal Code – 1 up to 12 years of imprisonment

  Section 370 of the Criminal Code – 0 up to 2 years of imprisonment

  Section 201a of the Criminal Code – 6 months up to 3 years of imprisonment

  Section 201b of the Criminal Code – 0 up to 2 years of imprisonment

C. Online card fraud

Criminal offences in commission whereof computer/information networks were used as a tool or target, on particular online bank/credit card fraud are as follows.

- Section 219 of the Criminal Code, Unlawful manufacturing and enjoyment of electronic payment means of other payment card;
- Section 221of the Criminal Code, Fraud;

Additional amendments of legislation related to the Directive transposition.

5.2 Procedural issues

The protection of fundamental rights and freedoms is guaranteed by the Constitution of the Slovak Republic, international treaties in the field of fundamental rights and freedoms, as well as by the laws of the Slovak Republic. The limits for the fundamental rights and freedoms may be set up under conditions regulated by the Constitution and only by means of law. The Code of Criminal Procedure under Section 2 paragraph 2 provides for the principles of restraint and proportionality: „Fundamental rights and freedoms of persons may be, in cases permitted by law, interfered with to the extent necessary to achieve the purpose of criminal proceedings with due respect to the dignity of persons and their privacy."

The provisions of criminal procedural law applied to cybercrime are identical to those governing procedures followed in respect of any other crimes. The provisions of criminal law allow restrictions of fundamental rights and freedoms, in particular regarding the privacy of personal information and freedom of expression for the purposes of investigation/criminal prosecution of cybercrime. Investigation and prosecution of criminal offences is primarily governed by Act No 301/2005 Coll., the Code of Criminal Procedure as amended:

1) Request to surrender a thing and its withdrawal when surrender is refused (Section 89 and 91 of the Code of Criminal Procedure

2) Preservation and surrender of computer data pursuant to Section 90 of the Code of Criminal Procedure

„(1) If the clarification of facts relevant for criminal proceedings requires the preservation of stored computer data, including operational data saved through the computer system, the presiding judge of a panel or, prior to the commencement of criminal prosecution or in pre-trial proceedings, a prosecutor, may issue an order substantiated also by the merits of the case against the person who is in the possession of or control over such data, or to the provider of such services, requesting them to: a) preserve and maintain integrity of such data,

b) enable making and keeping copies of such data,

c) prevent access to such data,

d) remove such data from the computer system,

e) surrender such data for the purposes of criminal proceedings."

3) House search, body search and the search of other premises and property (Section 99 et seq.)

4) Crime scene inspection pursuant to Section 154 of the Code of Criminal Procedure

5) Search of other premises and plots of land pursuant to Section 101 of the Code of Criminal Procedure

6) Interception and recording of telecommunications pursuant to Section 115 – 116 of the Code of Criminal Procedure

7) Remanding into custody based on a custody decision (Section 72), arrest warrant (Section 73), remanding into provisional custody or custody pending extradition pursuant to Chapter Five of the Code of Criminal Procedure or pursuant to a separate law (Act No 154/2010 Coll. on the European Arrest Warrant).

8) Taking evidence in a dwelling, other premises and on the plot of land (Section 107)

„The provisions under Sections 100, 101, 104 through 106 shall also apply if a crime scene inspection, reconstruction, recognition, verifying testimony on the spot or investigation experiment or any other procedure are to be conducted in the places set out therein, and if such procedures cannot, in view of their nature, be conducted elsewhere and the person concerned did not give his consent."

9) Surveillance of persons and things (Section 113)

10) Making visual, audio or audio-visual records (Section 114)

11) Comparison of data in information systems (Section 118)

These procedures can be implemented while meeting all statutory conditions, and it is particularly necessary to emphasize that they require the consent / decision of the prosecutor or the court.

5.2.1 Investigative Techniques

Under the Slovak national law, there are permissible

a) search and seizure of information system/computer data – as a rule, during the house search in the presence of a computer expert (e.g. an forensic expert) the selection whereof is conditional upon his knowledge of the producer and the type of computational and operating system used; there are also used the provisions concerning the preservation and surrender of computer data

b) real-time interception/collection of traffic/content data – as a rule, via interception and recording of telecommunications

c) based on the prosecutor's order, it is permissible to preserve computer data for the period the length whereof, however, may not exceed 90 days; a new order for data preservation shall have to be issued for any extension of that period

d) order concerning stored traffic and content data (as a part of computer data preservation and surrender)

e) order concerning the information on user is permissible pursuant to the provisions of Section 90, eventually Section 116 of the Code of Criminal Procedure.

5.2.2 Forensics and Encryption

Apart from the law enforcement agencies, a specialised unit of the Ministry of Finance of the Slovak Republic - CSIRT.SK, is also involved in the process of inquiry into crimes. But its activities in such process are exclusively linked to the activities of the law enforcement agencies, and CSIRT. SK has set up a unit/laboratory for the purposes of forensic analysis.

Investigation is conducted by an investigator (body involved in criminal proceedings) who, in order to clarify facts relevant for criminal proceedings, may engage a forensic expert from the Institute of Forensic Science (or any other person who can act as an expert according to relevant legislation) to provide an expert opinion in the form prescribed by law. As regards the examination in the laboratory, a forensic expert in the branch of Digital Forensics examines submitted items based on the tasks assigned to him by requesting party and he analyses only the data located on standard memory media of the submitted items. When it comes to forensic examination at the site of forensically relevant event, a forensic expert gives focus strictly to procedures conducted at the site (determined by police, prosecutor or court) or the search of a house or of other premises, and only in relation to the data located on standard memory media of the objects found at the site of inspection. No remote forensic expert examination is performed. Moreover, pursuant to Section 145, par. 1 of the Code of Criminal Procedure, a forensic expert is neither entitled to resolve legal issues, weigh the evidence, nor to draw legal conclusions.

When examining encrypted storage media (e.g. True Crypt), it is not possible to proceed directly to their logical data structure, and therefore it is necessary to decrypt the content. Without deciphering data, the Department of the Data Analysis does not carry out decryption, since it is not suitably technically equipped and staffed, and such activities are not envisaged to be carried out in the future. In the above case, the Department contacts the requesting authority to be provided with access data, decrypting key and suchlike. If the requesting authority is not able to do so, the item is excluded from examination.

The investigation of cybercrime requires extensive knowledge in the field of information (computer) technology. All the investigators and other staff working in the field of detection of and the fight against cybercrime may consult in advance the procedures they plan to follow with police officers of a recently established specialised unit for fighting cybercrime the Cybercrime Unit of the Criminal Police Bureau at the Presidium of the Police Force. Aspects of technical nature may be consulted with the staff of the Departments of the Data Analysis of the Institute of Forensic Science located in the cities of Bratislava, Slovenská Ľupča and Košice. As a part of methodological guidance, the Cybercrime Unit of the Criminal Police Bureau at the Presidium of the Police Force offers, at its web site, the best practice recommended to shorten the process of detection, checking and investigation of cybercrimes and to find new timely cybercrime prevention solutions. When requested so by other units, police officers of the above department participate in procedures.

Good practices / lessons learned with respect to the use of certain cybercrime investigation techniques are continuously made public on the Department's intranet site, namely in the document "Methodology Manual for the Detection, Documentation, Summary Investigation and Investigation of Crimes related to the Internet Use."

5.2.3 E-Evidence

The concept of „e-evidence" is neither defined under the criminal codes nor under other pieces of legislation.

For the purposes of judicial proceedings, it is required to produce the evidence in the form enabling their real adducing and weighing in the manner prescribed by law. Such evidence typically include:

- Personal evidence – hearings of persons (accused persons, witnesses, forensic experts or other experts),
- Documentary evidence – reports submitted by the requested institutions (e.g. providers of electronic and other services) based on the orders issued by the prosecutor or court, specialist knowledge statements and forensic expert opinions containing the analysis of seized computer traces,
- Real evidence – typically CD, DVD or other data carriers capturing e.g. pornography, extremisms, or proving the copyright infringement and suchlike. These are in particular the evidence on illegal computer content.

The Code of Criminal Procedure contains a general definition of the evidence which also allows the inclusion of electronic evidence. Pursuant to Section 119 par. 2 of the Code of Criminal Procedure: „(2) Anything that may contribute to properly clarifying the case and that has been obtained in a lawful manner in compliance with this Act or with the other acts can be used as evidence. The means of evidence are especially hearings of the accused, witnesses, experts witnesses, forensic expert opinions and specialist knowledge statements, verifying testimony on the scene, test identification parade, crime scene reconstruction, investigation experiment, site inspection, objects and documents relevant for criminal proceedings, criminal complaint, information collected using technical means or criminal intelligence checks."

In terms of criminology, the electronic evidence may be any information stored or transmitted in a digital (binary) form that is relevant for the purposes of criminal proceedings. Electronic means of evidence include emails, electronic documents, digital video files, audio files and images, instant message histories, databases, spreadsheet data, web client history, cookies, print outputs, electronic book-keeping, data geo-location from GPS, logs of banking operations performed, etc.. When being entered into criminal files, the electronic proofs are archived on data carriers, mostly on optical ones. Criminal files contain, in addition to the copy of electronic evidence on an optical carrier, also visual output of the evidence, such as a video, or printout of the document, SMS, or verbatim transcript of the content of communication. An analysis of the authenticity of electronic evidence is mainly made through a forensic expert opinion, rarely through the testimony of the originator of evidence, such as the sender of SMS.

The end result of an expert examination of computer data is a forensic expert opinion. In its annexes, there are special portable data carriers, which are adduced as evidence in criminal proceedings and in particular in the proceedings before the court. Original data carriers are as a rule seized throughout the pending criminal proceedings, particularly if they have been used for committing the criminal offence, when imposition of the penalty of forfeiture of a thing is envisaged. A special order under Section 118 of the Code of Criminal Procedure is the warrant to compare data in information systems. If the record made in the course of data comparison is intended to be adduced in evidence, provision under Section 115 par. 6 of the Code of Criminal Proceedings shall apply accordingly.

Almost without any exception, the immaterial evidence intended to be adduce in evidence in criminal proceedings are changed into a documentary form and, if that is not possible or desirable, they are stored on portable data carriers, which are then also handed over to judicial authorities.

The Prosecutor performs the procedures of collecting, storing and transmitting of electronic evidence in the form of real things (computers, data carriers, etc.) for the purpose of their producing before the court while he or she applies, in particular, the provisions under Sections 89, 91, 92, 99 and 101 of the Code of Criminal Proceedings (i.e. surrender of a thing, withdrawal and taking over of a thing, disclosing of a thing during the house search or search of other premises and property - often firm business premises, offices, server rooms) and the provisions under Section 90 of the Code of Criminal Procedure (preservation and surrender of computer data, typically saved on the respective data carrier); such data carriers are later handed over to the court after termination of pre-trial proceedings. Real evidences that have not been returned are left in the possession of a competent police officer until the final decision of the court.

Section 90 of the Code of Criminal Procedure - Preservation and Surrender of Computer Data

(1) If the clarification of facts relevant for criminal proceedings requires the preservation of stored computer data, including operational data saved through the computer system, the presiding judge of a panel or, prior to the commencement of criminal prosecution or in pre-trial proceedings, a prosecutor, may issue an order substantiated also by the facts of the case against the person who is in the possession of or control over such data, or to the provider of such services, requesting them to

a) preserve and maintain integrity of such data,

b) enable making and keeping copies of such data,

c) prevent access to such data,

d) remove such data from the computer system,

e) surrender such data for the purposes of criminal proceedings.

(2) The order referred to under paragraph 1 subpar. a) or c) shall have to specify the period during which the data shall be preserved, the length whereof may not exceed 90 days; a new order shall have to be issued for any extension of the period of their preservation.

(3) If the stored computer data, including operational data saved through the computer system, are no longer needed for the purpose of criminal proceedings, the presiding judge of a panel or, prior to the commencement of criminal prosecution or in pre-trial proceedings, a prosecutor, shall forthwith issue an order vacating the previous order to preserve the data.

(4) The order referred to under paragraphs 1 through 3 shall be served on the person who is in the possession of or control over such data, or on the provider of such services, who may also be imposed the obligation to keep the measures set out in the order confidential.

(5) The person who is in the possession of or control over computer data shall surrender such data, or the provider of services shall surrender the information related therewith that is in its possession or under its control to the authority that issued the order pursuant to paragraph 1.

Section 116 of the Code of Criminal Procedure

(1) In criminal proceedings held in respect of an intentional criminal offence, the warrant to disclose and provide telecommunications data covered by telecommunications privacy or personal data protection law may be issued, if such data are necessary to clarify the facts relevant for criminal proceedings.

(2) The warrant to disclose and provide telecommunications data shall be issued in writing by the presiding judge of a panel, prior to the commencement of criminal prosecution or in pre-trial proceedings by a judge for pre-trial proceedings upon a motion by a prosecutor, and it shall have to be substantiated by the merits of the case; the warrant shall be served on the persons referred to under paragraph 3.

(3) Legal entities or natural persons who provide telecommunications services shall notify the presiding judge of a panel, or in pre-trial proceedings a prosecutor or a police officer, of the telecommunications that were carried out.

(4) The provisions under paragraphs 1 through 3 shall apply accordingly to the content data or operation data transmitted via computer systems in real time.

The purpose of the above provisions, in particular under paragraph 4, is most of all the need to ascertain or verify the facts relevant for criminal proceedings based on the data transmitted through a computer system. These facts are the subject of telecommunications secrecy or subject to personal data protection law.

The comparison of data in information systems is governed by the provisions under Section 118 of the Code of Criminal Procedure.

Technical aspects of securing the electronic evidence consist preferably in storing and transmitting of the electronic evidence on respective portable recording media that are the part the investigation file. In practical terms, mainly the following scenarios occur:

A. If the electronic evidence is located in the computer or on any data carrier (e.g. CD, DVD carriers, mobile phones), the device is seized pursuant to relevant provisions of the Code of Criminal Procedure, and the data concerned are sent for forensic examination.

Slovak authorities experienced situations when instead of seizing the entire computer only the data from the hard disk were transferred to an external hard drive. The above procedure was applied in the event if a perpetrator committed a criminal offence at his employer's premises and the computer, in addition to the data relevant to criminal prosecution, also contained working, in particular accounting data, in which case the seizure of a thing used for committing a criminal offence would be a tough sanction, especially if the computer did not belong to the perpetrator of the crime.

If the entire computer was seized and a motion for the forfeiture of a thing was lodged, the entitled persons assisted by a computer expert were allowed to transfer from the hard drives the data deemed by these persons as personal ones, or data of a commercial nature.

B. If an electronic evidence is on the Internet, or it is owned by the provider of electronic services, the provider of electronic service is requested to preserve and provide such data pursuant to Section 90 of the Code of Criminal Procedure, and the electronic evidence is being uploaded predominantly on the external drive (in case of a large amount of data) or on DVD carriers. Such data carriers are subsequently attached to the criminal file along with the format indication and if need be with a codec.

These forensic services are provided by the Department of the Data Analysis of the Institute of Forensic Science of the Presidium of the Police Force. They perform a whole range of professional activities in the branch of digital forensics either in a laboratory or at the site of a forensically relevant event. Forensic services are carried out upon requests for forensic examination (e.g. ruling issued by a body involved in criminal proceedings, court order), in which the requesting party raises questions to be answered by a forensic expert or presents for other facts that are necessary to be given an expert opinion. When requesting an expert examination, the requesting party also attaches material things (e.g. traces seized during the search of a house or of any other premises) that are to be subject to an expert examination. Expert examination in the laboratory covers a range of procedures designed for analysis of the data contained in the submitted standard memory media as required by the requesting authority. Through the analysis of data, the facts relevant for the investigated case or the facts material for procedures to be performed at the later stages of proceedings (links between the items of evidence) from the matters unrelated to the case. The expert examination is concluded by a forensic output, as the case may be, with an attachment (mostly in an electronic form) containing selected facts. The expert opinion is handed over to the requesting authority in a printed form with an electronic attachment in an appropriate storage medium. Expert examination is carried out at the site of forensically relevant event by an forensic expert upon a request of a body involved in criminal proceedings, and it consists in a forensic copy of the data from the storage media that are material for bodies involved in criminal proceedings, or possibly in copying just selected facts upon instructions given by the latter. There is not carried out an in-depth analysis on-site. Relevant data are seized in a suitable storage medium and they are handed over to the bodies involved in criminal proceedings. The pieces of hardware are not as a rule seized on-site by a forensic expert, but by technicians.

Pieces of electronic evidence become admissible in criminal proceedings if they were obtained in a lawful manner and if simultaneously they were not obtained through unlawful duress or the threat of such duress. The rules governing the admissibility of electronic evidence are the same as the general rules governing the production of evidence.

A legitimate evidence is the evidence that was obtained in a lawful manner, i.e. in compliance with the Code of Criminal Procedure or with other separate law (e.g. on the Police Force, on the Customs Administration Authorities).

The concept of legitimacy of evidence and their sources shall be understood as the suitability of the evidence in terms of admissibility of their sources, as well as in terms of the legitimacy of the methods, means and procedures used to obtain the information constituting the content thereof.

Pursuant to the Slovak Code of Criminal Procedure, inadmissible may be considered:

- the evidence obtained through duress of the threat of such duress (Section 119 par. 4 of the Code of Criminal Procedure),
- the information obtained through making visual, audio or audio-visual recordings in a dwelling without a warrant issued by the judge for pre-trial proceedings (Section 114 par. 2 the Code of Criminal Procedure),
- the information obtained in the course of making visual, audio or audio-visual recordings, where the accused is found to be in communication with his defence counsel (Section 114 par. 4 of the Code of Criminal Proceedings),
- the evidence obtained in the course of making visual, audio or audio-visual recordings in other criminal case than specified in the authorisation if in such case the criminal proceedings is not simultaneously held in respect of an intentional criminal offence that under the Criminal Code attracts a sentence of imprisonment the upper limit whereof exceeds three years, in respect of corruption, abuse of power by a public official, legalisation of the proceeds of crime or of other intentional criminal offence in respect of which the holding of proceedings arises out of the international treaty binding on the Slovak Republic (Section 114 par. 7 of the Code of Criminal Procedure),
- the communication between the accused and his defence counsel in the course of intercepting and recording telecommunications (Section 115 par. 1 of the Code of Criminal Procedure),

- the information obtained in the course of intercepting and recording telecommunications without a warrant issued by the judge for pre-trial proceedings (Section 115 par. 2 of the Code of Criminal Procedure),
- the evidence obtained in the course of intercepting and recording telecommunications in other criminal case than specified in the authorisation if in such case the criminal proceedings is not simultaneously held in respect of a criminal offence referred to under par. 1 (Section 115 par. 7 of the Code of Criminal Procedure),
- the information obtained in comparison of data in information systems if such data are inseparably linked to other data (Section 118 par. 4 of the Code of Criminal Procedure),
- the information obtained in comparison of data in information systems in other criminal case if in such case the criminal proceedings is not simultaneously held in respect of a criminal offence referred to under par. 1 (Section 118 par. 7 of the Code of Criminal Procedure).

In case of the evidence obtained abroad, it is necessary to follow the procedures set forth under relevant international treaties in the field of legal assistance implemented by the judicial authorities while taking into account the Slovak Code of Criminal Procedure. The legal assistance in respect of computer data is frequently governed by the provisions of the Convention on Cybercrime; in relation to the states that are not parties to it, there are applied other multilateral (usually European Convention on Mutual Assistance in Criminal Matters of 29 April 1959 and the Convention on Mutual Assistance in Criminal Matters between the EU Member States) or bilateral international treaties governing the judicial cooperation in criminal matters. In the absence of a treaty the cooperation is possible using the principle of reciprocity.

Unless an international treaty provides otherwise, the validity of procedural acts performed abroad shall be governed by the provision under Section 535 of the Code of Criminal Procedure: „Service effected by a foreign authority upon a request by the Slovak authority as well as evidence taken by such authorities shall be valid if they were carried out in accordance with the law of the requested State or if they comply with the law of the Slovak Republic.“

At the national level, no problems with admissibility of the electronic evidence obtained from abroad via the legal assistance channels have so far occurred. In the reply to the questionnaire it is mentioned that the evidence obtained from abroad may also be used in evidence if the Slovak authorities decided to take over the criminal proceedings. The evidence shall not be given higher legal power than it has in the State where it was obtained.

In case of an order to take evidence or seize property on the basis of the mutual recognition instruments, the pieces of evidence are obtained in a manner as set forth under Act No 650/2005 on the Execution in the European Union of Orders Freezing Property or Evidence and on amending and supplementing Act No 300/2005 Coll., the Criminal Code, Act No 301/2005 Coll., the Code of Criminal Procedure and Act of the Slovak National Council No 372/1990 Coll. on Misdemeanours as amended.

5.3 Protection of Human Rights/Fundamental Freedoms

The Law of the highest legal force relating to the protection of human rights in digital space of the Slovak Republic is the Charter of Human Rights and Freedoms, which grants citizens the right to inviolability of the person and his privacy, preservation of human dignity, personal honour, reputation and good name, private personal and family life, protection against unauthorized collection, disclosure or other misuse of his personal data. Another document of primary authority for protection of human rights and freedoms is the Constitution of the Slovak Republic underpinning the need to promote democratic principles in the measures taken to protect the digital space of the Slovak Republic (especially Art. 19 par. 2 and 3 and Art. 26). It should also be highlighted that, according to Article 7 para 5 of the Slovak Constitution "international treaties on human rights and fundamental freedoms, international treaties whose execution does not require a law and international treaties which directly establish rights or obligations of natural persons or legal persons and which were ratified and promulgated in a manner laid down by law shall have primacy over the laws.

Statutes governing protection of the above rights and freedoms include in particular:

- Criminal Code No 300/2005 Coll. as amended:

a) Section 122 par. 2 – the criminal offence is considered as having been committed in public if it is committed with the use of a computer network, or using the means of similar effect"

b) Section 140a sets forth „Criminal offences of extremism", which are frequently committed by using a computer network:

„The criminal offences of extremism are as follows: the criminal offences of supporting and promoting of groups oriented to suppressing fundamental rights and freedoms pursuant to Sections 421 and 422, manufacturing of extremist materials pursuant to Section 422a, dissemination of extremist materials pursuant to Section 422b, possession of extremist materials pursuant to Section 422c, denial and approving of the Holocaust and crimes of political regimes pursuant to Section 422d, defamation of nation, race and confession pursuant to Section 423, incitement to national, racial and ethnic hatred pursuant to Section 424, instigation, defamation and threatening to persons for their affiliation to certain race, nation, nationality, complexion, ethnic group or family origin pursuant to Section 424a and the criminal offence committed by reason of specific motivation pursuant to Section 140 subpar. d) and f)."

c) Sections 196 and 198 – the merits of the criminal offences of „Breach of mailing secrets":

Section 196

„(1) Any person who intentionally breaches

b) the secrecy of information transferred via electronic communication service, or

c) the secrecy of private transfer of computerized data to the computer system, out of it or within it, including electromagnetic radiation from computer system transferring such computerized data,

shall be liable to a term of imprisonment of up to three years."

Section 198

„(1) Any person who, in breach of a generally binding legal regulation, manufactures, procures for himself or another, or possesses the equipment capable of intercepting the information transferred via electronic communication service, shall be liable to a term of imprisonment of up to three years."

d) Sections 201a and 201b – the merits of the criminal offence „Sexual abuse“:

Section 201a

„Any person who, through electronic communication service, suggests a child under fifteen years of age a personal meeting with the intent to commit the criminal offence of sexual abuse or the criminal offence of production of child pornography against him while not himself a child, shall be liable to a term of imprisonment to a term of six months to three years. “

Section 201b

„Any person who abuses a child under fifteen years of age with the intent of inducing sexual satisfaction through his participation in sexual activities or sexual abuse, even without such child to participate, or who enables such abuse, shall be liable to a term of imprisonment of up to two years.“.

e) Section 219 – the merits of the criminal offence of „Unlawful manufacturing and enjoyment of electronic payment means of other payment card“:

„(1) Any person who unlawfully manufactures, alters, imitates, counterfeits or gains possession of electronic payment means or electronic money or other payment card including phone card, or an object capable to fulfil such function, for the purposes of using it as genuine, or who possesses, transports, uses or provides it to another for the same purpose, shall be liable to a term of imprisonment of one to five years.

(2) Any person who unlawfully manufactures, possesses, procures for himself or otherwise gains possession or provides to another a tool, computer program or other device specifically adapted for the commission of the offence referred to in paragraph 1 shall be liable to a term of imprisonment of up to three years.“.

f) Section 221 – the merits of the criminal offence of „Fraud“:

„(1) Any person who enriches himself or other to the detriment of another person’s property through misrepresentation of another person or through taking advantage of another person’s mistake, and thus causes small damage to the property of another**10**, shall be liable to a term of imprisonment of up to two years.“

g) Section 226 – the merits of the criminal offence of „Unjust enrichment“:

„(1) Any person who enriches himself or other to the detriment of another person’s property by making unauthorised intervention into the computer hardware or software, automated machine or a similar device or equipment designed for automatic selling of goods, exchange or withdrawal of cash, or for dispensing paid-for operations, services, information or other performances with the aim of obtaining goods, services or information without payment or of collecting cash without authorisation, and who thus causes a small damage to another person' property, shall be liable to a term of imprisonment of up to two years.”

h) Section 247 – the merits of the criminal offence of „Damaging and abusing the information stored on data carrier“:

„(1) Any person who, with the intent to cause damage or other harm to another or to obtain unjust benefit for himself or other person, gains access without lawful authority to a computer system, an information carrier or the part thereof and

a) makes unauthorised use of its information,
b) unlawfully destroys, damages, deletes, alters such information or reduces its quality,
c) makes an unauthorised intervention into the computer hardware or software, or
d) obstructs the operation of computer system by inserting, transferring, damaging, deleting, reducing the quality, modifying or suppressing the computer data, or creates non-authentic data with the intention to be deemed or handled as authentic ones for legal use

shall be liable to a term of imprisonment of up to three years.

10 Small damage is less than 266 euro.

(2) The same sentence as referred to under paragraph 1 shall be imposed on the offender who, with the intention to commit the offence referred to under paragraph 1,

a) using technical means, makes an unauthorised monitoring of the closed transfer of computer data into the computer system, out of or within it, or

b) procures or makes accessible a computer programme and other equipment or computer password, access code or similar data enabling the access to the computer system in its entirety or to the part thereof.“

i) Section 249a – the merits of the criminal offence of „Falsification of cultural objects“:

„(1) Any person who unlawfully produces, imitates or modifies cultural object so as to be passed off as genuine, or who procures such object for himself or for other person or gains possession of it, shall be liable to a term of imprisonment of up to two years.

(2) The offender shall be liable to a term of imprisonment of one to five years if he commits the offence referred to under paragraph 1
a) by reason of specific motivation,
b) on a larger scale, or
c) through computer system.

j) Section 257 – the merits of the criminal offence of „Breach of regulations governing the handling of controlled goods and technologies:

(1) Any person who obtains a document, required by the authorities in charge of monitoring goods and technologies subject to separate regulations, on the basis of false or incomplete data shall be liable to a term of imprisonment of up to two years.

2) The same sentence as referred to under paragraph 1 shall be imposed on any person who destroys, damages, renders unusable or conceals documents required for keeping the records on goods and technologies controlled under separate regulations, or who fails keeping such records, or who interferes with computer hardware or software used to keep the records on such goods or technologies.

k) Section 259 – the merits of the criminal offence of „Misrepresentation of business records:

(1) Any person who presents false or grossly distorted data, or conceals mandatory data concerning important facts in a statement, report, input data entered into the computer or in other documents, which serve for

a) statistical verification, with the intention to obtain undue advantages for himself or another,

b) employee records, with the intention to obtain undue advantages for himself or another,

c) controlling accounting records,

d) controlling the use of grants, subsidies or other State budget allocation, allocations from the budgets of a public institution, the State fund, a higher territorial unit or municipality,

e) setting the value of property or security rate being transferred or assigned to other person,

f) bankruptcy, composition, restructuring or write-off of debt, or

g) entry into the Register of Companies or the Land Register, the Motor Vehicle Records or into other register pursuant to a special regulation,

shall be liable to a term of imprisonment of six months to three years.

(2) The same sentence as referred to under paragraph 1 shall be imposed on any person who, with the intention referred to in paragraph 1,

a) interferes with computer hardware or software, or

b) destroys, damages, renders unusable or fails to keep the records referred to in paragraph 1.

l) Section 272 – the merits of the criminal offence of Manufacturing and possession of instruments for counterfeiting and forgery:

(1) Any person who manufactures, procures for himself or another, or has in his possession an instrument or other object or software suitable for counterfeiting or alteration of money or its security features, securities, official documents, official seals and official seal-offs or emblems shall be liable to a term of imprisonment of up to three years.

m) Section 283 – the merits of the criminal offence of Infringement of copyright:

(1) Any person who unlawfully infringes the protected copyright to a work, performance by a performing artist, an audio recording or audio-visual recording, radio or television transmission or database shall be liable to a term of imprisonment of up to two years.

2) The offender shall be liable to a term of imprisonment of six months to three years if he commits the offence referred to under paragraph 1,

a) and causes larger damage through its commission,

b) acting in a more serious manner,

c) by reason of specific motivation, or

d) through computer system.

n) Section 368 – the merits of the criminal offence of „Production of child pornography“:

(1) Any person who exploits, elicits, offers or otherwise abuses a child for production of child pornography or child pornography performance, or enables such abuse of a child, or otherwise participates in such production, shall be liable to a term of imprisonment of four to ten years.

(2) The offender shall be liable to a term of imprisonment of seven to twelve years if he commits the offence referred to under paragraph 1

a) against a child under twelve years of age,

b) acting in a more serious manner, or

c) in public.

o) Section 369 – the merits of the criminal offence of Dissemination of child pornography

(1) Any person who disseminates, transports, procures, makes accessible or otherwise puts into distribution child pornography shall be liable to a term of imprisonment of one to five years.

(2) The offender shall be liable to a term of imprisonment of three to eight years if he commits the offence referred to under paragraph 1

a) acting in a more serious manner, or

b) in public.

p) Section 370 – the merits of the criminal offence of Possession of child pornography and participation in child pornography performance.

„(1) Any person who has in his possession child pornography or who acts with the intent to get access to child pornography via electronic communication service shall be liable to a term of imprisonment of up to two years.“

q) Section 374 – the merits of the criminal offence „Unauthorised use of personal data“:

„(1) Any person who, without lawful authority, communicates, make accessible or discloses

a) personal data of another obtained in connection with the execution of public administration or with the exercise of constitutional rights of a citizen, or

b) personal data of another obtained in connection with the execution of his own profession, employment or function, and thus breaches his own obligation prescribed by a generally binding legal regulation,

shall be liable to a term of imprisonment of up to one year.“

r) Section 376 – the merits of the criminal offence of „Harm done to the rights of another“:

„Any person who unlawfully breaches the secrecy of an instrument or other written document, audio recording, visual recording or other recording, computer data or other document kept private by another, through disclosing them or making them accessible to a third person, or using them otherwise, and thus causes serious prejudice to the rights of another, shall be liable to a term of imprisonment of up to two years.“

s) Section 422b – the merits of the criminal offence of “Dissemination of the extremist materials

“(1) Any person who reproduces, transports, procures, makes accessible, puts into distribution, imports, exports, offers, sells, sends or disseminates extremist materials shall be liable to a term of imprisonment of one to five years.

(2) The offender shall be liable to a term of imprisonment of three to eight years if he commits the offence referred to in paragraph 1

a) acting in a more serious manner

b) in public

c) in the capacity of a member of an extremist group.

- Act No 166/2003 Coll. on the Protection of Privacy against Unauthorised Use of Information-Technical Means amending and supplementing certain Acts (Act on the Protection against Interception).
- Act No 650/2005 Coll. on the Execution of Orders freezing property or evidence in the European Union and on amending and supplementing Act No 300/2005Coll., the Criminal Code, Act No 301/2005 Coll., the Code of Criminal Procedure, and Act of the National Council of the Slovak Republic No 372/1990 Coll. on Misdemeanours as amended.

a) Section 3 par. 4 – Scope of the Use of Order

„(4) For the purposes of recognition and enforcement of the order for freezing of evidence, a judicial authority of the Slovak Republic shall not examine liability to punishment for an act under the national law of the Slovak Republic[11], if

a) enforcement of the order for freezing evidence is sought for an act that constitues a punishable criminal offence under the national law of the state of origin,

b) maximum sentence of imprisonment, which may be imposed for such offence under the national law of the state of origin, is at least three years, and

c) the act was classified by a judicial authority of the state of origin as

11. cybercrime, ...“.

[11] No verification of dual criminality

- Act No 154/2010 Coll. on the European Arrest Warrant

„(3) If surrender is sought in respect of an act which constitutes a criminal offence under the law of the issuing Member State, if maximum length of sentence applicable under the law of the issuing Member State is at least three years, and if the act has been qualified by the relevant judicial authority of the issuing Member State as belonging to one or more of the categories of criminal offences listed under paragraph 4, executing judicial authority shall not examine whether the act constitutes a criminal offences under their law.

(4) The categories of criminal offences pursuant to paragraph 3 shall be understood

k) cybercrime, ...".

- Act No 549/2011 Coll. on Recognition and Enforcement of Decisions that impose custodial sentences involving deprivation of liberty in the European Union and on amending and supplementing Act No 221/2006 Coll. on Custody Execution as amended.

a) Section 4 par. 2 – Scope of Application:

„(2) If recognition and enforcement of a decision is sought in respect of a criminal offence which attracts maximum length of sentence applicable under the law of the issuing Member State at least three years and if, in the certificate on issuance of the decision (hereinafter referred to as "the certificate"), it has been qualified by the relevant judicial authority of the issuing Member State as belonging to one or more of the categories of criminal offences listed under paragraph 3, the court shall not examine whether the act constitutes a criminal offences under the national law of the Slovak Republic.

(3) The categories of criminal offences pursuant to paragraph 2 shall be understood

k) cybercrime, ...".

- Act No 122/2013 Coll. on Protection of Personal Data and on amending and supplementing certain acts

a) Section 68 – regulates liability and sanctions imposed upon the controller for violation of the obligations prescribed by law.

- Act No 351/2011 Coll. on Electronic Communications as amended

a) Sections 55 through 63 regulate the protection of privacy and personal data

b) Sections 64 through 68 regulate the protection of networks and equipment

c) Section 73 regulates the sanctions for violation of obligations and prohibitions set forth under Act No 351/2011Coll.

- Act No 275/2006 Coll. on Information Systems of the Public Administration as amended

a) Section 10 – regulates the liability of persons obligated by law and sanctions imposed upon them for administrative infractions committed in breach of law .

- Act No 215/2002 Coll. on Electronic Signature and on amending and supplementing certain acts

a) Section 26 – regulates the liability of natural persons and sanctions imposed upon them for misdemeanours committed in breach of law

b) Section 26a – regulates the liability of legal entities and natural persons – entrepreneurs, and sanctions imposed upon them for administrative infractions committed in breach of law

- Act No 215/2004 Coll. on Protection of Classified Information and on amending and supplementing certain acts

Section 78 (Misdemeanours) and Section 79 (Administrative Infractions) regulate the liability of and sanctions imposed upon subjects acting in breach of law.

National priorities in this area are well reflected in the specific policy documents, such as the National Strategy for Information Security.

5.4 Jurisdiction

5.4.1 Principles applied to the investigation of cybercrime

The Slovak legal system does not provide for the provisions governing jurisdiction exclusively for the area of cybercrime. Applicability of the Criminal Code includes its applicability in time, territorial applicability, personal applicability (active/passive personality principle), universal applicability and applicability under international instruments (Sections 2 through 7b of the Code of Criminal Procedure).

Territorial Applicability

(1) This Act shall be applied to determine the criminal liability for an act committed on the territory of the Slovak Republic.

(2) The criminal offence is considered as having been committed on the territory of the Slovak Republic even if the offender

a) committed the act, at least in part, on its territory, if the actual breach of or threat to the interest protected under this Act took place or was intended to take place, in whole or in part, outside of its territory, or

b) committed the act outside the territory of the Slovak Republic, if the actual breach of or threat to the interest protected under this Act was intended to take place on its territory, or such a consequence should have taken place, at least in part, on its territory.

(3) This Act shall also be applied to determine the criminal liability for an act committed outside the territory of the Slovak Republic aboard a vessel navigating under the State flag of the Slovak Republic, or aboard an aircraft entered in the aircraft register of the Slovak Republic.

Personal Applicability

This Act shall also be applied to determine the criminal liability for an act committed outside the territory of the Slovak Republic by a Slovak national or a foreign national with permanent residency status in the Slovak Republic.

This Act shall also be applied to determine the criminal liability for a particularly serious felony if the act was committed outside the territory of the Slovak Republic against a Slovak national, and if the act gives rise to criminal liability under the legislation effective in the location of its commission, or if the location of its commission does not fall under any criminal jurisdiction.

This Act shall also be applied to determine the criminal liability for illicit manufacturing, possession of and trafficking in narcotics, drugs, poisons and precursors (Sections 171 and 172), forgery, fraudulent alteration and illicit manufacturing of money and securities (Section 270), uttering counterfeit, fraudulently altered and illicitly manufactured money and securities (Section 271), manufacturing and possession of instruments for counterfeiting and forgery (Section 272), forgery, fraudulent alteration and illicit manufacturing of duty stamps, postage stamps, stickers and postmarks (Section 274), forgery and fraudulent alteration of control technical measures for labelling goods (Section 275), establishing, masterminding and supporting a terrorist group or its member (Section 297), illicit manufacturing and possession of nuclear materials, radioactive substances, hazardous chemicals and hazardous agents and toxins (Sections 298 and 299), plotting against the Slovak Republic (Section 312), terror (Sections 313 and 314), destructive actions (Sections 315 and 316), sabotage (Section 317), espionage (Section 318), assaulting a public authority (Section 321), assaulting a public official (Section 323), counterfeiting and altering a public instrument, official seal, official seal-off, official emblem and official mark (Section 352), jeopardising the safety of confidential and restricted information (Section 353), facilitation of illegal migration (Section 355), endangering peaceful coexistence among nations (Section 417), genocide (Section 418), terrorism and certain forms of participation in terrorist actions (Section 419), acts against humanity (Section 425), using prohibited weapons and unlawful warfare (Section 426), plundering in the war area (Section 427), misuse of internationally recognised and national symbols (Section 428), war atrocities (Section 431), persecution of civilians (Section 432), lawlessness in the wartime (Section 433), even if such criminal offence was committed outside the territory of the Slovak Republic by a foreign national who does not have permanent residency status in the Slovak Republic.

This Act shall be applied to determine the criminal liability for an act committed outside the territory of the Slovak Republic by a foreign national who does not have a permanent residency status in the Slovak Republic also where

a) the act gives rise to criminal liability under the legislation effective on the territory where it was committed,
b) the offender was apprehended or arrested on the territory of the Slovak Republic, and
c) was not extradited to a foreign State for criminal prosecution purposes.

(2) The offender referred to under paragraph 1 may not be, however, imposed a more severe punishment than that allowed under the law of the State on the territory whereof the criminal offence was committed.

Applicability under International Instruments

(1) This Act shall be applied to determine the criminal liability also when set forth under an international treaty ratified and promulgated in a manner prescribed by law which is binding on the Slovak Republic.

(2) The provisions under Sections 3 through 6 shall not apply if their use is prohibited under an international treaty ratified and promulgated in a manner prescribed by law which is binding on the Slovak Republic.

If the Slovak authorities have jurisdiction over a certain act, they will evaluate the subject-matter and territorial jurisdiction (competence). Determination of the territorial jurisdiction in the area of cybercrime may be difficult in some cases.

For determining the territorial jurisdiction, it is primarily necessary to ascertain from where "an attack" was executed, i.e., from which particular computer the material was sent, e.g. in the form of an email message, and also to which computer such electronic message was delivered. In these cases, it may be important to identify IP addresses, and consequently to disclose a communicating individual. Territorial jurisdiction is thus derived from these findings.

Notwithstanding the foregoing, there may occur the cases where it is not possible to fix territorial jurisdiction based on the location of commission of a criminal offence. The Code of Criminal Procedure therefore regulates alternative criteria for determining the territorial jurisdiction under Section 17 paragraph 3 of the Code of Criminal Procedure. Jurisdiction of the prosecutor's office follows the jurisdiction of the court.

Section 17 of the Code of Criminal Procedure - Territorial Jurisdiction
(1) The proceedings shall be held by the court in whose district the crime was committed.
(2) Jurisdiction of the district court in the seat of a regional court for proceedings in respect of criminal offences referred to under Section 16 par.1 shall mean the jurisdiction of the regional court concerned.
(3) If a crime scene cannot be identified or if the criminal offence was committed in a foreign country, the proceedings shall be held by the court having jurisdiction over domicile, a workplace or place of residence of the accused; if such places cannot be identified or are located outside the territory of the Slovak Republic, the proceedings shall be held by the court that has jurisdiction over the place in which the criminal offence was detected.

5.4.2 Rules in case of conflicts of jurisdiction and referral to Eurojust

Conflict of jurisdictions occurs in many criminal matters, not only in the area of cybercrime. In this area it is significant mainly because in general several states have jurisdiction for proceedings.

As it follows on from experience of the District and Regional Prosecutor's Offices of the Slovak Republic, the conflicts of jurisdiction lead to difficulties only rarely.

From the perspective of the Prosecution Service of the Slovak Republic, positive conflicts of jurisdictions consisting in conducting parallel criminal prosecutions do not pose any problem. They enable parallel securing of evidence, which particularly in the context of the short period for data retention and technical capabilities of the perpetrators may lead to identification and punishment of perpetrators of this crime. In principle, the only obstacle for parallel proceedings in the EU space is the application of the principle *„Ne bis in idem"*.

The Prosecution Service in general makes use of the possibilities provided by international legal instruments, including the EU instruments. If need be, the consultations with the State concerned are run and, where appropriate, a criminal complaint or proceedings are transferred/accepted.

These cases may lead to the communication between the states concerned or the use of Eurojust's or EJN's channels.

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

Slovak authorities said although they have not hitherto experienced any problems associated with the cloud, it is only a question of time when they will inevitably face such a situation. The use of the cloud storage sites is becoming a common practice for both legal entities and natural persons.

As in determining the competence to issue an order to obtain respective electronic evidence, there is largely applied the principle of territoriality, a fundamental problem is to find out the physical location of the server on which the evidence is located. This is, however, very complicated and lengthy. An example of lengthiness of this procedure is the provision of anonymisation services, where it is necessary, for the purposes of criminal proceedings, to determine the IP address of the device that used the gate. An operator is in this case located on the territory of another State. The prosecutor must therefore address a foreign judicial authority and later he or she may realize from the end results of legal assistance that technical means of the system (respective mail server) have not been found on the territory of the requested State, but elsewhere, and the operator does not record logs. In this case, the request must be made and sent to other State. A fundamental problem is the fact that within the internet network there are no physical boundaries and traditional forms of judicial cooperation are not sufficiently effective when it comes to the internet network.

This problem can be partially addressed through a regional representation of transnational companies. In this way, some branches of foreign companies accept orders issued by Slovak courts and ensure data which are physically located on servers outside the territory of the Slovak Republic.

In relation to the issues of jurisdiction and cloud computing Slovak authorities consider relevant the exchange of experience within the Committee of Parties to the Convention on Cybercrime (T-CY).

Situations requiring implementation of mechanisms based of the Council Framework Decision 2009/948/JHA of 30 November 2009 have not so far happened. The legal acts in the Slovak Republic regulate procedures foreseen in the said Framework Decision in Section 530a of the Code of Criminal Procedure.

The Slovak authorities indicated a positive role of Eurojust in solving the issues outlined above.

5.4.4 Perception of the Slovak Republic with regard to legal framework to combat cybercrime

The legal regulation governing investigation and prosecution of perpetrators of cybercrime committed outside the Slovak Republic is sufficient in the sense that there are provisions governing the establishment of jurisdiction, as well as procedural rules to obtain evidence from a foreign country (in particular Part Five of the Code of Criminal Procedure, international treaties and separate laws, whereby the instruments of mutual recognition have been transposed into the legal system of the Slovak Republic). This legislation also represents a sufficient framework for the provision of legal assistance to other states.

The time is a main factor causing problems. Data retention periods in different countries are different and usually short.

Fundamental problem in the prosecution and investigation of the perpetrators of crime in national and cross-border cases is the absence of the necessary data and sufficient legislative framework at the EU level for preservation of data.

This situation caused that telecommunications service operators in the Slovak Republic retain only the information necessary for billing and claims purposes and only for a limited period of time and

to a limited extent. Some data are not kept at all. So, if it is manageable to get data from another state by means of mutual legal assistance, the obtained data cannot lead, in a number of cases, to clearing-up of the criminal offence and disclosing of its perpetrator usually for time reasons or because of non-preservation of data.

Reasons for concerns arise out of the fact that after the above decision of the Court of Justice of the European Union there have not yet been adopted clear legislative measures at the European Union level which would improve the situation described above. Given the current state, it is not possible to obtain such data even in the cases of most serious criminal offences.

5.5 Conclusions

- Transposition of the Directive 2013/40/EU on cyberattacks is being prepared. There the evaluation team recommends to take this opportunity to criminalise forms of computer sabotage such as DoS and DDoS attacks.
- In general the Slovak legislation related to cybercrime does not seem to suffer neither from major gaps nor from internal collisions; however the facilitation of undercover investigations - in accordance with fundamental rights - would be beneficial to practitioners.
- The announced empowerment of CSIRT.SK with regulatory enforcement powers for mitigating purposes should lead to strong coordination among all authorities involved, as to avoid overlapping with Police powers and ongoing criminal investigation. Slovak authorities said a bilateral agreement between CSIRT.SK and Presidium of the Police Force is under preparation that will be handling with such cases..
- The invalidation of the Directive 2006/24/CE ("Data retention") by the Court of Justice of the EU and the subsequent suspension of the Slovak national law which implemented this directive by the national Constitutional Court were repeatedly mentioned by all interviewed practitioners as a serious constraint to criminal investigation and prosecution efficacy.
- The default of reciprocity of substantive legal framework between the Slovak Republic and third states was also mentioned as an important obstacle to certain investigations, namely of defamation on social networks.

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

Global trends in computer security are also reflected in the Slovak Republic. In recent years, namely 2011 - 2013, Slovak authorities observed an increasing number of occurrences and also the detection of serious security incidents. During the reporting period, they observed an increase in the number of attempts to break into information systems together with an increase in phishing attacks.

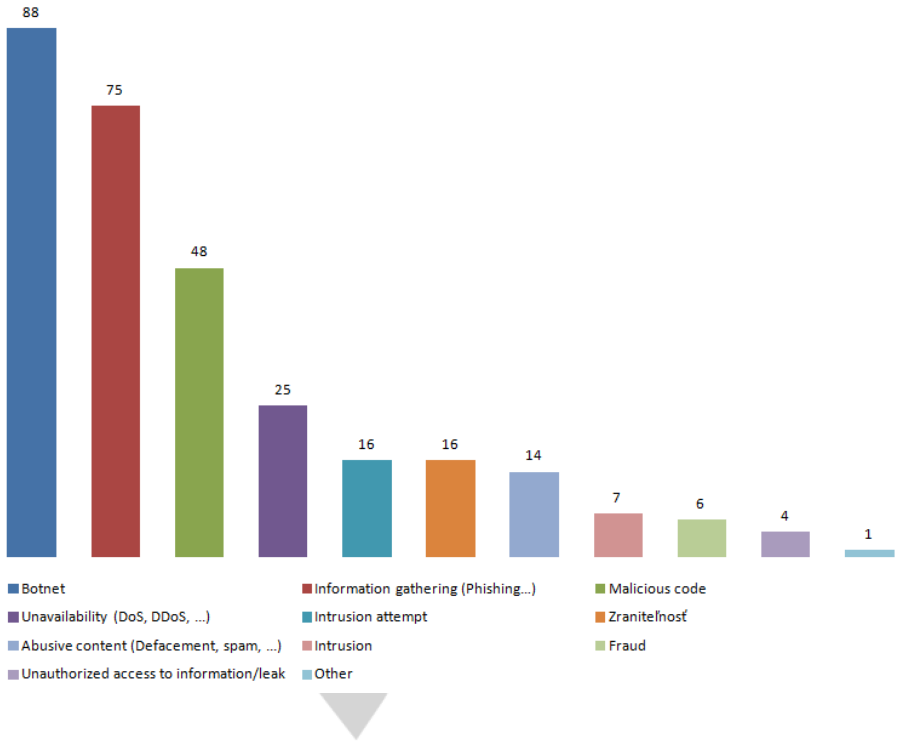
Based on the reports on possible harmful activities relating to IP addresses occurrence in the Slovak Republic (Fig. 2), it is possible to assume that malicious code in Slovakia infected at least 100,000 to 150,000 devices, representing a minimum of 6 percent of all workstations in the Slovak Republic. These devices pose a safety risk to their users, especially if they are used, for example, to work with Internet banking, buying over the Internet, but also in terms of e-Government, advanced electronic signature and the like.

CSIRT.SK also noted an increased amount of phishing messages in the area of public administration, some of which are also part of targeted attacks on these institutions. Such fraudulent e-mails tend to be aimed at obtaining credentials. Malware or link to malicious code is often annexed to such e-mails. The main objective of malicious code is usually harmful activity aimed at creating a backdoor for the attacker in order to get the access to the network, system, data leakage or to control the device, to link it to botnet networks and the like. In such cases, the methods of social engineering, i.e. phishing and malicious e-mail messages are used to infect devices. The infection then occurs by running the malicious code contained in the annex or by accessing the website (drive-by download) via interposed link.

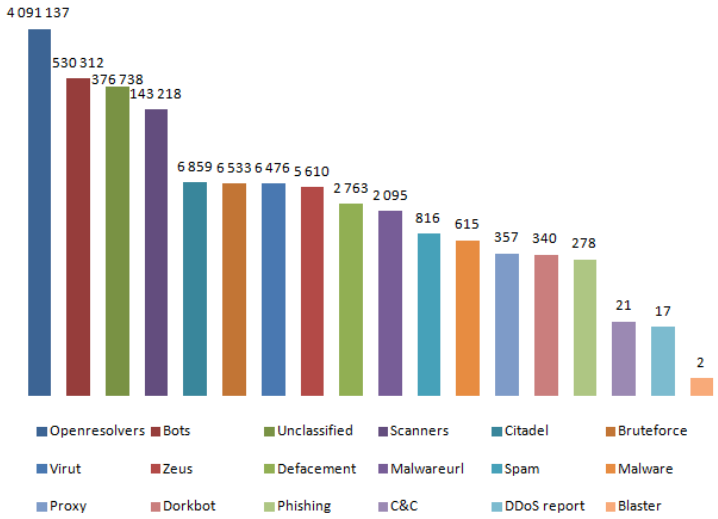
Phishing sites that require entering logins to various information systems did not focus only on state administration and public administration. These were often phishing sites designed to elicit logins to web banking services such as Internet banking, PayPal, Facebook or different Google services, which are used by majority of the Slovak population. Most reported sites were hosted in the Slovak Republic. In cooperation with operators of the Web servers, such fraudulent phishing websites were continuously removed.

Increasingly common type of attack on the infrastructure of the organization is DDoS attack. In this type, attackers try to limit the availability of electronic services on the targeted device through depletion of resources, line congestion or disabling the equipment or service. The most common type of DDoS attacks were DDoS TCP-SYN flood and DDoS UDP flood over NTP whose participants were also IP addresses belonging to the address space of the Slovak Republic.

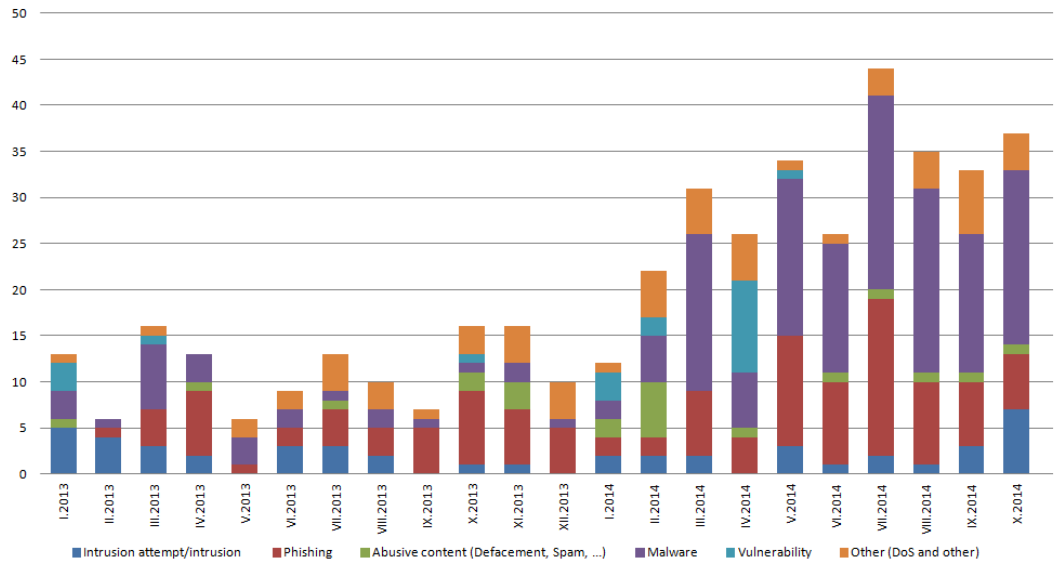
Picture 1: Types and number of serious computer security incidents for the period of 1.1.-30.10.2014 (source CSTIRT.SK)



Picture 2 - Types and number of reported computer security incidents in the IP address space of the Slovak Republic for the period of 1.1.- 30.10.2014 (source CSTIRT.SK)



Picture 3 – Development of serious computer security incidents for the period of 1.1.2013 - 30.10.2014 (source CSTIRT.SK)



6.1.2 Mechanism to respond to cyber attacks

In connection with transposition of the Directive of European Parliament and Council 2009/140 / EC, in particular its Articles 13a and 13b, requirements relating to the integrity and security of networks and services associated with the obligation to report security incidents to undertakings providing public networks or public services were transposed into the Act no. 351/2011 Coll. on Electronic communications.

As stated in the Telecommunications Office of the Slovak Republic Measures (no. O-30/2012), Section 1, Paragraph 3 — security incident is "any event in any way impairing the security of networks or services or integrity of the networks concerned."

As stated in the Telecommunications Office of the Slovak Republic Measures (no. O-30/2012), Section 4 — Security incident is reported to the Regulatory Office for Electronic Communications and Postal Services (the "Authority") immediately after discovering the security incident. Report shall be made electronically, using encryption or other alternative form – according to the Authority's requirements.

Measure O-30/2012 on the safety and integrity has been developed taking into account the recommendations of ENISA. Details of reporting the leakage of personal data are laid down in European Commission Regulation no. 611/2013 (http.teleoff.gov.sk/data/files/34911.pdf).

In the event of cyber attacks, which could have malfunctioned running state, the future direction of the organization and countermeasures addressing the National Security Council, which would give a mandate to the competent bodies to prepare and implement appropriate countermeasures.

Tasks for operators of critical infrastructure and for certain groups of information systems operators – aiming to protect them from security threats – are defined in several legally binding regulations.

Critical infrastructure in the Slovak Republic is described by the Act No. 45/2011 Coll. This act defines eight sectors of the national critical infrastructure and identifies criteria for determination of critical infrastructure operators composed mainly from private sector subjects. The role of operators in the protection of critical infrastructure consists of different security measures implementation defined by the Act No. 45/2011 Coll. on Critical Infrastructure (Section 9 Responsibility of the operator and Section 10 Security plan). Those measures are especially dealing with implementation of the modern technology to protect the infrastructure, adoption of the security plan and organisation of regular security crisis exercises.

As to the obstacles faced by law enforcement authorities when responding to cyber attacks, Slovak authorities underlined once again that computer data retention periods vary in different member states and within the individual providers. In particular, this problem is visible after the decision of the Court of Justice of the EU and in relation to third countries. Harmonised length of this period and data request procedures would be appropriate for the effective investigation of cybercrime, so they are provided to the competent investigating authority in the shortest possible time. Due to the need to comply with the established formal procedures for obtaining evidence currently established limits for storing computer data perceived as insufficient (if any).

Detection of cyber criminals requires technical, as well as legal knowledge. The level of the knowledge of the offenders in the field of IT technology is usually higher than the knowledge of the police officers, prosecutors and judges. This expertise can be improved by targeted professional training activities (theoretical and practical) aimed at Police Force, prosecution and the courts. It should also take place on the international level (i.e. in the form of practical workshops at Europol, Eurojust, within EJTN etc.).

It is reasonable to consider the specialisation on this particular type of crime in at the level of the Police Officers, investigators and prosecutors. This approach could lead to more targeted support in terms of technical equipment, as well as the education system. One possibility is the creation of contact points at the national regional level. On the other hand it is clear that the computers moved into our daily life to such an extent that it is impossible to address this type of crime solely to the specialists. Therefore it is necessary to provide the training for all prosecutors and judges working in the criminal field – legal training, as well as technical. It is important to gain practical experience as well as access to case law. These issues require further consideration.

Regarding the criminal investigation, the main obstacles that law enforcement agencies have to overcome when collecting evidence related to cyber-attacks (especially hacker attacks) are lacking equipment for the Police Force, insufficient number of experts analysing particular situation and highly qualified professionals working in specialized police work in this area. This can lead to errors in the investigation (e.g. incorrect procedure in the crime scene, such as inadequate inspection and documentation of the scene). More problems are caused by incorrectly posed questions addressed to the forensic expert or the fact, that an forensic expert with another field of expertise than computer forensic science is invited to the investigation.

The amount of data is increasingly growing and storage media of still greater capacity, holding more and more data, are being presented for the examination. These must be analysed by an expert, which takes more and more time and puts higher technical demands on forensic computer technology performing the expert examination.

It should also be noted that the dynamic development of computer attacks by more skilled and constantly improving computer offenders is not easy to keep up with in a long-term, especially with the new - modified and more sophisticated attacks by the perpetrators. Insufficient IT systems knowledge of operators, their managers and security specialists seems to cause difficulties in this area.

In the future, Slovak authorities expect long-term persistence of such a trend.

6.2 Actions against child pornography and sexual abuse online

Directive 2011/93/EU has been transposed into the Slovak Criminal Code. Act No 300/2005 Coll. Came into effect on 1 August 2013, whereby both, the Criminal Code as amended, and certain other acts have been amended and supplemented. No implementation problems have come to the Slovak authorities knowledge.

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

Slovak practitioners make use of the database ICSE (designed for identification of the victims of child pornography) maintained by Interpol. Until now eight police officers from the Police Force have been trained to search the above database.

A judicial warrant is required for CAM deletion pursuant to the Code of Criminal Procedure of the Slovak Republic. It takes a certain period of time to render such warrant, and that is the reason why the communication channel INHOPE under the project STOPLINE.SK implemented by a non-profit organisation called "e-Slovensko" is widely used to avoid re-victimisation (*see below*).

Article 21 of Directive 2011/93/EU requires Member States to establish measures against advertising abuse opportunities and child sex tourism. Slovak Police officers use operational information carry out searches for such cross-border perpetrators and they actively participate in transnational actions. The latest such operation took place on 11 – 12 September 2014 within the framework of operational activity 5.4 OAP – Cybercrime 2014, sub-priority – Sexual Exploitation of Children, set forth under the EMPACT priorities.

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

This is covered by the above-mentioned project Zodpovedne.sk.

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

In the above context, the legislation has been amended through transposition of the provisions of EU Directive 2011/93/EU into the Criminal Code of the Slovak Republic, whereby such acts have been criminalised. It consists namely of the amendment to the criminal offence of possession of child pornography pursuant to Section 370 of the Criminal Code extending the aforementioned qualified facts of the case so as to impose criminal sanctions upon persons who intentionally participate in real time web-based performance. Moreover, Criminal Department of the General Prosecutor's Office of the Slovak Republic examined, practical experience gained by the prosecutors involved in criminal prosecution of the perpetrators who allegedly committed criminal offences of manufacturing, dissemination and possession of child pornography materials. Based on the results of this evaluation the Criminal Department intends to take specific investigation measures to prevent children from real time web-based performances.

Another equally important measure implemented over a long-term period consists in preventive and awareness raising activities carried out at the premises of primary and secondary schools, as the school environment groups are most at risk of becoming victims of the threat posed by this crime. Given the size of the above group at risk, the prevention and awareness raising activities are being organised in cooperation with the NGO e-Slovensko within the project titled ZODPOVEDNE.sk (Assumed Responsibility). These activities are also supported by handing out of promotional items developed by e-Slovensko in cooperation with the Ministry of the Interior of the Slovak Republic.

Specific measures also include the aforementioned project titled *ovce.sk (sheep),* the underlying idea whereof is to employ prevention to make children more aware of the given issues and thereby reduce the risk of becoming a victim of this crime.

A single hotline (nonstop telephone assistance call No 116 111, Live Chat with an operator or via email: potrebujem@pomoc.sk */ I need help*) has been made available as a part of the project Zodpovedne.sk funded by the European Commission within the framework of community programme „Safer Internet Plus, Active Presentations Given at Schools to Students, Teachers and Parents".

For the purposes of developing information tools, the Ministry of the Interior joined the project Zodpovedne.sk that is designed to ensure the safe and responsible use of internet, mobile phones and other new technologies. It is supported by the European Union under the community programme Safer Internet Plus. The project aims to raise public awareness about the safe use of internet and mobile phones, risks posed at virtual space and about the possibilities of getting advice and assistance. The projects partners are e-Slovensko, civic association, the Ministry of the Interior of the Slovak Republic, Slovak National Committee for UNICEF, Slovak Telekom and SK-National Informatics Centre Slovakia. More information about the European Communities project can be found on www.SaferInternet.org.

Main objectives of the project are as follows:

- establishing and operation of the national awareness raising center Zodpovedne.sk,
- raising awareness, spreading information about the safe use of internet, mobile communications and new technologies, prevention of crime,
- establishing and operation of the helpline Pomoc.sk,
- participation in the international networks, best practice exchange with other national centres and the Safer IT organisations,
- establishing and operation of the national centre for reporting illegal content on internet Stopline.sk., UNICEF and MoI SR
- available in Slovak and English languages,
- subproject ovce.sk for the youngest users of internet.

6.2.4 Actors and measures countering websites containing or disseminating child pornography

Act on Electronic Communications does not stipulate the obligation to filter, block access or remove content from internet. Enterprises, however, on their own initiative, block selected ports or services that may pose technical risk to their networks. The Regulatory Authority for Electronic Communications and Postal Services does not keep any records of such procedures followed by the enterprises. As of 1 October 2014, there has come into force the new General Authorisation for the Provision of Electronic Communication Networks or Electronic Communication Services (http://www.teleoff.gov.sk/data/files/41722.pdf)), which under Article IV. point 2 par. 5 and Annex No 2 imposes upon the enterprises the obligation to disclose the information concerning the blocking of ports and services. When blocking content, operators display alert messages reporting the cases of violation of the operating rules.

An administrator of the National Domain SK-NIC is authorized to suspend the provision of technical services at the domain on the basis of a final and enforceable decision rendered by the administrative authority, in particular if there is a threat to national and international cyber security, namely if through the domain in question or through services available via such domain the malicious content is disseminated (especially computer viruses, malware), or if sham content of service is provided (mainly phishing), or if hardware available through the domain is a control centre of the interconnected hardware network disseminating malicious content (mainly botnet), and suchlike.

The measures such filtering, blocking of access and removal of content may be taken in individual cases pursuant to Section 90 par. 1 subpar. c) and d) of the Code of Criminal Procedure on the grounds of a judicial order[12].

The Regulatory Authority for Electronic Communications and Postal Services neither uses any tool to filter websites nor requires the businesses to do so. For the purposes of blocking, there is employed reporting via STOPLINE.SK operated in an international network INHOPE. The Ministry of the Interior of the Slovak Republic participates in funding the INHOPE network membership fee, allocating funds to the civic association e-Slovensko that is implementing this project.

[12] *Section 90 Preservation and Surrender of Computer Data*

(1) If the clarification of facts relevant for criminal proceedings requires the preservation of stored computer data, including operational data saved through the computer system, the presiding judge of a panel or, prior to the commencement of criminal prosecution or in pre-trial proceedings, a prosecutor, may issue an order substantiated also by the facts of the case against the person who is in the possession of or control over such data, or to the provider of such services, requesting them to

a) preserve and maintain integrity of such data,

b) enable making and keeping copies of such data,

c) prevent access to such data,

d) remove such data from the computer system,

e) surrender such data for the purposes of criminal proceedings.

(2) The order referred to in paragraph 1 subpar. a) or c) shall have to specify the period during which the data shall be kept safe, the length whereof may not exceed 90 days; a new order shall have to be issued for any extension of that period.

(3) If the stored computer data, including operational data saved through the computer system, are no longer needed for the purpose of criminal proceedings, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings respectively, shall forthwith issue an order vacating the previous order to keep the data safe.

(4) The order referred to in paragraphs 1 through 3 shall be served on the person who is in the possession of or control over such data, or on the provider of such services, who may also be imposed the obligation to keep the measures set out in the order confidential.

(5) The person who is in the possession of or control over computer data shall surrender such data, or the provider of services shall surrender the information related therewith that is in its possession or under its control to the authority that issued the order pursuant to paragraph 1.

Blocking of access / taking down web pages or the service through which personal data, child pornography or other illegal content are disclosed in violation of law is set forth under legal regulations as follows:

I. Act No 301/2005 Coll., the Code of Criminal Procedure,

Pursuant to Section 90 par. 1 (Preservation and Surrender of Computer Data, see footnote 12.)

Pursuant to Section 82 par. 1 subpar. b) (Reasonable Obligations and Restrictions):

„(1) If a judge for pre-trial proceedings or the court issued, pursuant to Section 80 or 81, a decision not to arrest the accused or release him or her from custody with the aim of strengthening the purpose otherwise effected by custody, the body deciding on a custody ruling may simultaneously place one or more reasonable restrictions or obligations on the accused, in particular,

b) ban on activity whereby the crime was committed".

II. Act No 71/1967 Coll. on Administrative Proceedings (Administrative Code), as amended:

Pursuant to Section 43 par. 1 (Preliminary Measures):

„(1) The administrative authority may order, prior to the termination of the proceedings and to the extent necessary to ensure the purpose of the proceedings is met:
a) that the parties perform an action or abstain from an action or suffer an action performed by others".

III. Act No 171/1993 Coll. on the Police Force as amended:

Pursuant to Section 25a par. 1 (Authority to Prohibit Access, Provision and Disclosure of Personal Data of Designated Persons):

„(1) A police officer protecting designated persons shall be authorised to prohibit access, provision and disclosure of personal data11b) of designated persons and persons close to them from information systems of operators and intermediaries11ba) who process 11bb) personal data pursuant to a separate regulation. 11bc)“

IV. Act No 351/2011 Coll. on Electronic Communications as amended:

Pursuant to Section 41 par. 4 of the quoted Act:

„(4) The undertaking that provides a public network or public network services shall be obliged, upon a written request of an authority acting in criminal proceedings and at its expense, for the reasons of preventing fraud or misuse, to block the access to numbers or services provided by means of specific numbers, and withhold interconnection or other services revenues. The request shall contain the specification of the period of the blocking duration. The undertaking shall not assume the responsibility for any damages incurred by the execution of such request.“

The undertaking that fails to fulfil the obligation under Section 41 shall be imposed a penalty up to € 300,000 /Section 73 par. 1 subpar. c) of the above Act/,

Pursuant to Section 43 (Rights and Obligations of Undertaking and User) of the quoted Act:

(1) The undertaking shall have the right to:

d) temporarily interrupt or restrict the provision of public services on the grounds of misuse of the service, and this so long until such misuse has been eliminated or technical measures to prevent such misuse have been implemented.

V. Act No 308/2000 Coll. on Broadcasting and Retransmission and on Amendments of Act No 195/2000 Coll. on Telecommunications regulates the prohibitions and obligations imposed upon the subjects providing services pursuant to this Act.

Pursuant to Section 19 par. 1 (Protection of Human Dignity and Humanity) of the quoted Act:

„(1) Audiovisual media on-demand service, programme service and all parts thereof must not

a) through their processing and content, interfere with human dignity and with the fundamental rights and freedoms of others,
b) promote violence and in an open or hidden form instigate hatred on the basis of gender, race, colour of skin, language, faith and religion, political or other thoughts, national or social origin, affiliation to the national or ethnic group,
c) promote war or describe cruel or other inhuman behaviour in a way which means inappropriate trivialization, excuse or approve of it,
d) depict without justification scenes of actual violence where an actual account of dying is emphasized in an inappropriate form, or depict persons subjected to physical or psychical suffering in a way which can be considered an unjustified attack on human dignity; this shall apply even when it affects persons who have agreed with such depiction,
e) in an open or hidden form promote alcoholism, smoking, use of narcotic substances, poisons and precursors or trivialize the effects of using the above substances,
f) depict minors who are subjected to physical or psychical suffering in an inappropriate form,
g) depict child pornography or pornography containing deviant sexual practices.“

Pursuant to Section 20 par. 1 and 2 (Protection of Minors) of the quoted Act:

„(1) A broadcaster shall be obliged to ensure not to broadcast the programmes or other elements of the programme service that can impair the physical, mental or moral development of minors, especially those containing pornography or coarse unjustified violence.“

Pursuant to Section 67 par. 12 (Fines):

„(12) The Council shall impose a fine from 500 to 60,000 Euro upon a broadcaster accessible through internet, if it

a) broadcasts the programme and other elements of programme service, the content whereof is contrary to obligations pursuant to Section 19 or 20 par. 1,
b) failed to suspend the programme or a part thereof or failed to comply with the conditions under which the broadcasting of the programme or a part thereof is suspended as set forth by the Council [Section 16 par. 2 subpar. a)].

In addition, the order to block access / remove malicious content of websites falls within the competence of the prosecutor prior to the commencement of criminal prosecution or in pre-trial proceeding, or of the presiding judge of a panel in proceedings before the court (Section 90 par. 1 subpar. c, d/the Code of Criminal Proceedings). The same measure must also be taken by the provider of service in compliance with the legal regulation as follows.

The internet may be used to also make public, disseminate and offer, inter alia, audiovisual works, the content whereof may be of the most diverse nature. In order to prevent unlawful internet activities, the conditions of public distribution of audiovisual works are set out under Act No 343/2007 Coll. on Conditions of Registration, Public Distribution and Preservation of Audiovisual Works, Multimedia Works and Sound Recordings of Artistic Performances including Amendments and Supplements to certain other Law (Audiovisual Law). Its provisions (Section 12 et seq.) regulate protection of minors against distribution of works of pornographic nature. It is safeguarded through the unified labelling system – a system for classification of audiovisual works, sound recordings of artistic performances, multimedia works, programmes provided via audiovisual on-demand service and programmes or other components of programme service according to their age suitability in terms of barred access, unsuitability or suitability for a group of minors up to 7, 12, 15 or 18 years of age. Details of the unified labelling system and the method of its application shall be determined, as stipulated in the Act (Section 12 par. 2), in a generally binding legal regulation (Decree of the Ministry of Culture of the Slovak Republic of 3 December 2007 No 589/2007 Coll., laying down details of a single labelling system for audiovisual works, audio recordings of artistic performances, multimedia works, programmes and other components of programme services and on the method of its application).

Pursuant to this Act (Section 19 par. 2 and 4) the provider of audiovisual media on-demand service shall be obliged to ensure that audiovisual media on-demand service and all components thereof which might endanger physical, psychical or moral development of minors, especially those containing pornography or coarse unjustified violence, are accessible only in such a manner that the minors are not normally enabled to hear or see such audiovisual media on-demand and all the components thereof. Based on the unified classification of programmes according to the age suitability, the broadcaster of television programme service and the provider of audiovisual media on-demand service are obliged, for the purposes of the protection of minors, to introduce and apply the unified system of labelling set forth under a separate regulation. This separate regulation is the above Audiovisual Law and its executive bylaw on the unified system of labelling. If the provider ascertains that its contractual parties breach the conditions, as almost all the providers put ban on operation of pornography sites, it may put ban on operation of the pornography site.

As regards a private sector, it bears no responsibility. The actions (blocking of access/removal of content/taking down websites) are performed based on the court warrant.

Existing practice proves the sufficiency of sending alerts reporting the illegal content on websites of the servers located in the Slovak Republic, specifying that the user of their service breaches the operating rules which contain a clause on prohibition of illegal activities while using services. The operator published the information notifying that the website was blocked on the grounds of violation of the operating rules.

In respect of reporting illegal content by citizens, they can use directly a reporting form located on the website STOPLINE.SK described in paragraph below.

Requests for blocking of content in cases when the server is located outside the Slovak Republic are made via a reporting form on the website STOPLINE.SK functioning in the international network INHOPE. Since the line is operated 24/7, there is no need for specific procedure to be followed in urgent cases. In case of need to block access / remove content of websites, CSIRT.SK cooperates with administrators who act towards eliminating unwanted activities on the basis of good will.

6.3 Online card fraud

6.3.1 Online reporting

In most cases, an online payment card fraud is reported by the banking sector. Cases reported by citizens were recorded only on rare occasions. In general, the online payment card fraud are reported, it happens rarely, that such notification is not made, for instance due to the possible damage caused to the business portfolio of the affected bank, especially if the information is published by media.

6.3.2 Role of the private sector

Cooperation between banking sector and Police Force of the Slovak Republic is at a high level. As it was mentioned before Slovak Banking Association (SBA) commission for security of payment cards was established. It deals with the identification of payment card frauds, looking for the solutions how to prevent from such frauds and which forms of precautionary measures shall be adopted. Members of the commission are representatives from commercial banks located in the Slovak Republic and representatives from chosen subjects operating in the sector of authorisation, issuing and handling payment cards (e.g. company Wincor – Nixdorf, First Data, etc.). There is also one member representing the Police Force of the Slovak Republic.

Information exchange between members of the SBA commission for security of payment cards results in early identification of cases and helps to prevent financial losses. Evaluation of monitoring of payment card transactions can indicate those cases where electronic data were attacked or merchants and clients have been infected (Malware, harmful code, etc.). Indication of new forms of misusing means of payment can also be a part of this information exchange. Based on the obtained information, banking sector and Police Force of the Slovak Republic adopt specific precautionary measures. Forms and tools of prevention are also evaluated and applied on the basis of operational meetings of mentioned commission. There are notices and warnings issued through media, press conferences and media campaigns. Regarding the protection from abuse of payment cards data on magnetic stripe, the most ATM machines in the Slovak Republic apply communication with payment card via chip which is a part of all new issued payment cards. Comparable situation is in the case of POS terminals.

All e-commerce merchants comply and use 3D secure rules in order to improve and secure authorisation of online payments. All banks provide online risk-monitoring service which is used to control and verify online payment cards transactions. This monitoring system going in 24/7 regime and its objective is the identification and preventing from payment card frauds.

6.4 Conclusions

- Although the SK authorities are aligned with most private sector forensic tools due to the backlog accumulated by the Institute of Forensic Science of the Presidium of the Police Force, they appear to regularly make use of private computer experts. However, this is not uncommon with law enforcement.

- For CSE investigations the Slovak authorities make good use of Interpol's victim ID Database (ICSE).

- The Ministry of the Interior of the Slovak Republic (Presidium of the Police Force) has created several channels of communication with third parties to receive information on possible cybercrime events.

- StopLine.sk, the Slovakian helpline for reporting child abuse produces good results. It was noted that Slovakia has no national sex offenders register, although this is not uncommon.

- Card Fraud appeared to be one area in which the Slovak authorities displayed some measure of success, benefiting from good relations with the many commercial banks and the private sector, good information sharing and a good case clearance rate.

- The CCU does not work with Academia, other than the Police College. However it provided examples of working with private industry (internet security companies) for malware investigations.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

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

No formal requirements are in place. General rules and procedures of cooperation will be applied. In the case of Eurojust, cooperation is regulated by the Act No. 383/2011 Coll. on representation of the Slovak Republic in Eurojust. Currently a draft Order of the general prosecutor of the Slovak Republic regulating exchange of information and cooperation between prosecutors and national member representing the Slovak Republic in Eurojust, as well as a draft Order of the general prosecutor of the Slovak Republic regulating activities of the European Judicial Network in the prosecution of the Slovak Republic, were elaborated.

CSIRT.SK is not directly involved in detecting cybercrime either. The cooperation with institutions such as Europol/EC3 and ENISA is focused mainly on the prevention of cybercrime, capacity building and awareness rising. No special procedures and formal requirements are needed for these purposes.

The Ministry of Interior of the Slovak Republic uses the communication channels of the SIENA network, as well as the Europol national unit. The legal basis for this way of exchanging information is regulated in the ACTS ADOPTED UNDER THE CHAPTER VI OF THE EU COUNCIL DECISION of 6 April 2009 establishing the European Police Office (Europol) (2009/371/ JHA).

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

Police Force of the Slovak Republic cooperates with Europol/EC3 in the fight against online child abuse and cyber-attacks. They also collaborate in cases posed by Eurojust. Although the Prosecutor's Office has dealt with only limited number of cybercrime cases calling for cooperation with Eurojust, the experience is seen as positive.

In a numerous cases the consultations took place and Eurojust facilitated the execution of legal aid in another Member State. As an example, there is a case, in which the Slovak Prosecutor's Office provided cooperation to the competent judicial authority of another Member State. The MLA request was initially directed to the surveillance and recording of the complete service of data transmission server with an IP address and its subsequent confiscation, including searches of other premises. It was a malware disguised as an invoice, where there were more than 10,000 incidents reported in the requesting Member State, as well as banking Trojan URL zone. Given the confusing content of the request, partly due to the quality of the translation, Eurojust was asked to obtain additional information that enabled the modification and subsequent execution of the request.

Another cooperating partner is CSIRT.SK, for cases of cyber incidents. CSIRT.SK collaborates with partner organization CERT-EU – an intervention team dealing with cyber security in the European institutions. Cooperation takes place in the incidents where a source or a target of an attack has the IP address within the space of Slovak Republic.

Based on the previous experience, especially with the exchange of knowledge and operational information, the Slovak Republic assessed contribution in tackling cybercrime very positively.

The contribution of ENISA lies in an active participation in the activities of the agency aimed at preventing cybercrime, capacity building and awareness of information security — as seen by the Ministry of Finance of the Slovak Republic. Therefore these activities are perceived positively, as well as the activities of Europol/EC3 – building cooperation between law enforcement teams such as CSIRT/CERT – at national and international level.

In general, Slovak authorities would appreciate if police authorities – including Europol – had more privileges to access the cybercrime data in the early stages (before the prosecution or pre-trial); in order to effectively secure computer data until the time when request for MLA is sent. In this respect, it would be appropriate to strengthen the legal framework and the scope of powers of these bodies. Mechanism for ensuring the positioning and operational data, which generally serve as auxiliary data in the investigation and in obtaining the evidence, should be substantially simplified. Consequently, for the purposes of judicial authorities, interference of Eurojust could come into consideration.

7.1.3 Operational performance of JITs and cyber patrols

The Slovak Republic uses JIT, however it did not participate in JITs related to cybercrime.
Currently there is no legal framework on the cyber patrols in the Slovak Republic.

7.2 Cooperation between the Slovak authorities and Interpol

Cooperation with Interpol in cybercrime is seen as very positive. Interpol works as an excellent facilitator of communication and knowledge (mainly used for sending and receiving knowledge about the criminal activity of Slovak nationals in the territory of third-countries) as well as the authority that fulfils the tasks.

7.3 Cooperation with third states

The Slovak Republic as one of the member countries of the Organization for Security and Cooperation in Europe - OSCE is committed to implement and maintain confidence-building measures in the field of cyber security (Confidence Building Measures) undertaken within that organization in 2013. By implementing these measures, the Slovak Republic aims to develop cooperation between the Member States in order to achieve the early information sharing and effective response in the elimination of illegal use of information and communication technologies.

The National Central Bureau of Interpol International Police Co-operation Bureau of the Police Force of the Ministry of Interior is used for communication in the prevention and investigation of cybercrime.

Participating States are encouraged to have in place modern and effective national legislation to facilitate on a voluntary basis bilateral co-operation and effective, time-sensitive information exchange between competent authorities, including law enforcement agencies, of the participating States in order to counter terrorist or criminal use of ICTs. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.

Slovak authorities see the Europol/EC3/Eurojust as bodies that may contribute to the effectiveness of cooperation with the third countries.

7.4 Cooperation with the private sector

Legal basis for preventing and combating cybercrime is not binding with respect to the private sector. The private sector can only contribute by reporting and through educational activities. In the context of child pornography and child abuse, this area is very well covered already in the projects STOPLINE.SK and ZODPOVEDNE.SK. In this regard, we can evaluate cooperation as very effective.

In relation to online fraud with payment cards and identification of Slovak servers' abuse, hosting provider was willing to provide all the information and electronic data documenting illicit activities. The data was provided to the police departments carrying out the investigation of the software attacks targeting the clients of Slovak banks.

The Electronic Communications Act does not pose special responsibility or liability for blocking / removing content from the Internet.

The applications for blocking the access/removing the content or websites in the framework of the Act on Electronic Communications are not tackled in any way, because this act does not impose such an obligation.

In case that the concept “internet providers” used in the question means enterprise within the meaning of the Act on Electronic Communications (enterprise providing access to the internet but not content), those have a wide range of specific obligations and responsibilities, which are described in the whole act and other measures and decisions issued by the Authority.

Section 41 of the Act on Electronic Communications gives law enforcement bodies the possibility to block the use of phone number, service provided through number or payment for done call. This relates only to the telephone service but not to the internet.

Direct communication with providers is used to disable access / removal of content or websites and for informing them on cases of breaches of the framework agreement on the use of Internet services by users / website operators. This process is possible within a set of published rules used to the level of the national registrar of the national domain ".sk".

At this level, the following measures may be used:

Refrain from the use (operation) of a second level domain,
Refrain from the transfer of the domain to a third party other than the applicant (the applicant's representative)
Transfer the domain to a designated person,
Refrain from publishing certain information through the domain,
Remove web page for the particular domain,
Ban to abolish a domain,
Suspension of a domain,
Refrain from establishing back-up or other similar rights to third-level domain,
Refrain from providing any domain to use for the benefit of third persons.

If judicial authority from one state needs to execute the procedural acts in another state, in principle, it has to apply the instruments of the mutual legal assistance. A possibility of direct cooperation with local branches of companies at the Slovak territory has not been used, however, there is one case, where the prosecution service cooperated successfully with Microsoft Slovakia, limited liability company. Data related to the e-mail accounts held on domains live.com and a Hotmail.com administrated by the American company Microsoft corporation, seated at One Microsoft Way, Redmond, USA, have been provided on the basis of an order of a prosecutor under Section 90 of the Code of Criminal Procedure branch, Microsoft Slovakia, limited liability company, seated at Prievozská 40, Bratislava. The Slovak branch provided data to 3 accounts on domains live.com and Hotmail.com in following range:

Data provided by the user during the creation of e-mail account by means of an online form, date and time of the creation of the e-mail account and IP address, from which the account has been created, statement from the account, including times of the access and IP addresses – History.

The Slovak branch provided requested data in a prompt manner, which enabled the fast evaluation of the IP addresses and determination of the next steps in the investigation. Microsoft Slovakia, however, is unable to provide the content of communication.

Coercive measures were not used. The information obtained will be used for the evaluation of the possibilities of cooperation.

7.5 Tools of international cooperation

7.5.1 Mutual Legal Assistance

The use of instruments of legal assistance is a basic procedure for securing evidence from abroad for the purposes of prosecution in the Slovak Republic. Requests for legal assistance are sent to the EU Member States as well as to the third countries, particularly to the United States. As it is important to ensure the evidence in such a way that it can be used in court, according to the Slovak law it is necessary to provide the evidence within the frame of judicial cooperation.

In addition to the Convention on Cybercrime, the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 with two Additional Protocols, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union established by the Council in accordance with Article 34 of the Treaty on European Union (Brussels, 29 May 2000), the Protocol, and other conventions of the Council of Europe, the UN, the instruments based on the mutual recognition, as well as cooperation based on reciprocity are applied.

For the process under the Convention on Cybercrime application for legal aid is often preceded by a request for expeditious preservation of computer data.

In the legal assistance Slovak authorities said they face several difficulties:

1. Short period of retention or insufficient range of stored data

2. In contrast to the short period of time referred to in paragraph 1, there are long delays in the processing of applications for legal assistance - information (mainly on service and location) sent after more than half a year, have no real use, as they usually require the provision of further evidence of electronic communications in Slovakia.

3. The *de minimis* principle (no processing requests where the damage does not exceed a certain amount or where other conditions are not met).

4. The application of the Convention on Cybercrime and costs (current issue with the Swiss Confederation, which sought reimbursement for finding information about IP addresses), objective burden of US authorities, where most critical servers and companies (Yahoo, Google, Facebook) are located.

7.5.2 Mutual recognition instruments

None of the EU mutual recognition instruments mentioned in the questionnaire have been used in relation to cybercrime.

7.5.3 Surrender/Extradition

In principle all listed criminal offences can be considered extraditable offences in Slovakia. At the same time, all the criminal offences listed in the questionnaire may lead to surrender procedures under the Act. No. 154/2010 Coll. On European arrest warrant.

Regardless of the nature of the crime, the general mechanism applies. The competent issuing/executing authorities are listed in the notification of the Slovak Republic for a Council Framework Decision 2002/584/JHA.

In general, there is any Court of the Slovak Republic empowered issue and send a European arrest warrant (Schengen Information System is also used). The European arrest warrants are transmitted to the competent Regional Prosecutor´s Office. Decision on execution of EAW is made either by the prosecutor of the Regional Prosecutor's office (if the person consents to surrender), or regional courts. The Supreme Courts decide on appeals against decisions of Regional Courts. SIRENE NCB (Interpol NCB) is used for sending the EAW and alerts. EAW can be also send in direct contact.

In the extradition proceedings requests are sent and accepted by the Ministry of Justice of the Slovak Republic. The National Interpol Bureau may be used for the purposes of sending a request. Regional courts decide on admissibility of extradition, except for the simplified extradition proceedings. The Supreme Court decides on appeals against Regional Courts decision. The Minister of Justice makes decisions on granting the extradition.

The preliminary investigation in the case of the European arrest warrant and extradition proceedings are carried out by the prosecutors of the regional prosecutor offices.

The extradition primarily falls into the competence of the Ministry of Justice – in sending, as well as receiving requests for extradition. Transmission of European Arrest Warrants falls within the competence of the Slovak courts. As regards receiving European arrest warrants, which are sent to the Regional Prosecutors' offices, the numbers are available in the standardised questionnaire prepared at the European Union level. Taking into account the uniform nature of the questionnaire for the whole EU, the information on the type of crime is not recorded.

The general legal framework is used, whether under the European arrest warrant or requests for extradition (in relation to third countries). Following the request for provisional arrest – if it is necessary to act quickly – it is possible to put a person into provisional detention. In urgent cases, personal freedom is restricted in a very short time (in hours). Data on the average length of the implementation of the European Arrest Warrant are available at European Union level in a standardized questionnaire.

In general, the extradition is based on the international treaties, including Convention on Cybercrime, or on the principle of reciprocity.

7.6 Conclusions

- Slovakia is a member of the Council of Europe and T-CY Committee.

- The contact point for Slovakia in relation to requests for preservation of computer data pursuant to Article 29 of the Budapest Convention is the NCB Interpol, which is a unit within the International Police Cooperation Bureau of the Police Force. In urgent cases, NCB Interpol can contact the police officers of the Cybercrime Unit for advice.

- There are regular contacts between the General Prosecutor's Office, the Cybercrime Unit (CCU) of the Presidium of the Police Force and the National Bureau of Interpol.

- The authorities met, in particular from the Police, are well aware of Europol/EC3.

- Eurojust seems to be well known and appreciated among the prosecutors met during the visit, who demonstrated to know very well the members of the national desk at Eurojust. During the visit it was also considered that Eurojust could have a role in assisting practitioners by collecting best practices and case law from other jurisdictions and disseminate this information to practitioners in all Member States.

8 TRAINING, AWARENESS-RAISING AND PREVENTION

8.1 Specific training

Were already mentioned above the activities carried out by the Computer Crime Department of the Criminal Police Bureau of the Presidium of the Police Force. Should also be mentioned the Department of the Data Analysis which provides general and specialised LEAs and the judiciary with trainings and lectures on everything that is coved by the Forensic Science Institute. The Department of the Data Analysis does not provide any regular or systematic professional training. However, the Forensic Science Institute systematically educate its expert employees. In order to permanently improve its expert work, the Institute creates suitable conditions for high-quality and competent exercise of professional practice and growth of each its expert. All experts have to pass a training period which follows after they have completed their university studies in the field of criminalistics, forensic science, police and law theory and practice. Finally, they need to learn quality standards as well. During the training period, experts gain essential theoretical and practical knowledge, experiences and correct habits in order to investigate and research forensic materials. They learn to interpret discovered outcomes. They shall learn how to search for and secure (fix) forensic materials in every forensic field, but particularly in the field where he/she specialises himself/herself. The training period for a qualified expert in criminalistics lasts for three years in the Forensic Science Institute. It consists from trainings, seminars, expert courses, conferences and from practical exercises realised under a supervision of an already qualified expert. When a trainee successfully completes the whole system of professional training, he/she gets a certificate on their forensic science qualification which authorises them to perform expert professions, to interpret and defend their research outcomes. Nevertheless, all experts must obey the principle of life-long learning. They must keep their professional competence up-to-date and constantly improve their work, take part in trainings, seminars, professional courses and conferences. Out of their own volition, they must independently, systematically and constantly search for and study the newest knowledge in forensic science disciplines and criminalistics and apply them into their practice. Each expert must prove his/her competence regularly, i.e. once in every five years, as is stated in Paragraph 27 (6) of the Act No. 73/1998 Coll. on the Police Force, Slovak Information Service, The Prison Warden Corps and the Railway police, as amended.

Police Academy, Department of Computer Science and Management in particular, provides theoretical knowledge on the subject to all students of the first year of the Bachelor's degree, to the following extent:

Compulsory subjects: IT Science I. - one compulsory lecture on Cybercrime, which contains the definition and allocation of cyber crime, the legislative framework and some types of cybercrime described.

IT Science II. for all students in the 3rd year of the Bachelor's degree where part of the course is devoted to the issue of safe behaviour on the Internet, with an emphasis on social networks.

Choice subjects: Practical IT Science - for students in the first year of the Bachelor's degree - lectures on current threats in cybercrime area.

This topic is also covered in of other courses provided by the Department of Criminology, in particular: Criminology II - for students of the second year of the Master's degree study program.

The judiciary receives professional trainings from the Judicial Academy of the Slovak Republic, as stated in Act No. 548/2003 Coll. on the Judicial Academy, as amended. Moreover prosecutors and judges may register via Judicial Academy of the Slovak Republic for international seminars abroad and participate there (e.g. in cooperation with the EJTN).

In 2014, the Judicial Academy organised an event called “Computer Crime” which took place on 16-17 September 2014 in Omšenie. Its participants were 6 judges, 23 prosecutors, 6 higher judicial officers and 4 assistants of the Supreme Court judges; 39 participants in total.

Beside this event, there were also seminars that covered the computer crime topic as their secondary topic, for example:

- „Organized Crime“, 17 - 18 March 2014 in Omšenie, which was attended by 18 judges, 23 prosecutors, 4 assistants of the Supreme Court judges and 3 higher judicial officers; 48 participants in total.

- "Custody, remand of persons and seizure of property in criminal proceedings", 27 - 28 February 2013 in Omšenie, which was attended by 32 prosecutors, 2 higher judicial officers, 15 judges; 49 participants in total.
- "Information-technical means and means of operational-searching activities", 20-21 February 2012 in Omšenie, was attended by 34 judges, 13 prosecutors; 47 participants in total.

The Judicial Academy organises also regional seminars that improve computer skills among judiciary.

- "Effective use of computer, internet and legal search engines" – in 2014, the Academy realised six one-day events.
- "Effective use of computer, internet and legal search engines" – in 2013, the Academy realised seven one-day events.
- "Effective use of computer, internet and legal search engines" – in 2012, the Academy realised twelve one-day events.

The Computer Crime topic has become a part of seminars that deal with international judicial cooperation in criminal matters. As an example a regional workshop organised by the Judicial Academy in cooperation with EJTN could be mentioned. It took place on 26th – 27th September 2012 in Omšenie. Participants attended a lecture named „Gathering and using evidence in EU cross-border cases". The lecture covered also international cooperation against computer crime.

Judicial Academy and the EJTN organized on 24 – 26 November 2014 in Omšenie the seminar with the topic "International judicial cooperation in criminal matters in practice – EAW and MLA simulations, which included the issues of obtaining of evidence related to telecommunications (i.e. telephone and internet communications) in the course of solving the practical cases. The participants of the seminar were judges and prosecutors from the Slovak Republic, the Kingdom of the Netherlands and the Kingdom of Spain, as well as both vice-Presidents of Eurojust.

The General Prosecution of the Slovak Republic provides its prosecutors with internal training activities on computer crime. Examples of such are:

A seminar created by the Criminal Department called "Computer crime and protection of intellectual property" which took place on 2nd – 4th May 2010 in an education and rehabilitation centre for Slovak prosecutors in Stará Lestná. Among lecturers, there was an advocate from a Legal Department of Slovgram, a deputy from a Legislative and Legal Department of the Industrial Property Office and an anti-piracy manager from the Microsoft Company, Ltd, Bratislava.

A seminar for prosecutors – specialized on crimes committed by minors and for crimes against children. The seminar took place on 7th – 8th March 2011 in an education and rehabilitation centre for prosecutors in Krpáčovo. The seminar was focused on production, spreading and possession of child pornography connected to computer crime. Its lecturer was an anti-piracy manager from the Microsoft Company, Ltd, Bratislava.

Regional seminars with the topic "Effective use of computer, internet and legal search engines" are contained in the approved Training plan for 2014. The seminar on the topic "Cybercrime" is planned too. Several aspects of cybercrime will be a part of other training activities of the Judicial Academy.

As mentioned previously, the Department of Computer Crime of the Criminal Police Bureau of the Presidium of the Police Force provides, in cooperation with the Police Force Academy and Police higher schools, lectures on cybercrime related topics. Their lecturers pass their professional knowledge on, explain practical examples and show how to solve problems which they have to face on daily basis. Information is exchanged also among police officers who take part in FP Copy, FP Terminal /Europol/EC3 and various CEPOL activities. But they do not only gain new knowledge, they establish new contacts and therefore improve the cooperation as such as well.

The Forensic Science Institute has implemented its own system of professional trainings. Since the main aim of the Institute is to perform expert activities, it considers CEPOL/EUROPOL courses as rather supplementary, and its experts attend these courses cca once per year because the courses are not all focused on expert activities.

Prosecutors may participate in trainings organised by the Judicial Academy. The International Department of the General Prosecutor´s Office deals with the issues of cybercrime within its own activities (it holds regular work sessions of the Director of the International Department with deputy regional prosecutors and prosecutors mainly dealing with legal relations with abroad.). During one of the meetings between the director of the International Department and regional deputy directors that took place on 5th – 7th May 2014, there was held a lecture named "Practical Information on Convention on Cyber Crime (notification No. 137/2008 Coll.) and related questions." The lecture content was later forwarded to prosecutor offices at regional and district level. This is a standard and continuous way of training and education. Besides this, prosecutors are also trained how to solve practical problems that may appear in their everyday work – it reflects current practical knowledge.

The International Department of the General Prosecution cooperates with relevant Police Force units. Such an example is that prosecutors from the International Department took part at a Europol Roadshow – awareness seminar in Bratislava – "Slovakia and Europol together against crime" which took place on the 20th of November 2013. One of its topics was also "Computer Crime" which was cover by one lecture.

In November 2014, Eurojust held a strategic seminar on computer crime in Hague. Based on the agreement between the General Prosecutor´s Office and the Ministry of Justice, the representative of the Ministry of Justice participated in the seminar.

The International Department of the General Prosecutor´s Office follows activities performed by the Committee of Parties to the Convention on Cybercrime and also other legislative activities happening in connection to this topic at the EU level. Afterwards, it forwards information to prosecutors on lower levels. Currently the topic of mutual legal assistance in cybercrime cases is under consideration of the Committee of Experts of the Council of Europe on the Operation of the European Conventions on Co-operation in Criminal Matters (PC-OC). General Prosecutor´s Office takes part in activities of the said Committee.

8.2 Awareness-raising

The Slovak Ministry of Finance has prepared an educative series for state employees, based on the Draft of Education System in Information Security of the Slovak Republic which was adopted by the Slovak Government resolution No. 391/2009. The pilot series began in 2013 and continued in 2014. Professional workers of CSIRT.SK (Computer Security Incident Response Team) participate in trainings organised by the Police Force Academy in Bratislava. The trainings are aimed to increase the professional knowledge of investigators.

The Slovak Ministry of Interior cooperates with a bank sector to inform Slovak citizens about possible threats and emerging forms of online frauds with payment cards. It also forwards information gained from other Member States during Europol working groups meetings (FP Terminal). Banks operating inside Slovakia act independently and individually. From time to time, they consult their activities with the Police Force. Slovak citizens are informed only within the dimensions of Slovakia or directly by commercial banks.

The Slovak Ministry of Education, Science, Research and Sports participates in the Council of Europe campaign „**No Hate Speech Movement**". The campaign has a European dimension. Among its participants, there are many non-governmental and state organisations working with children and youth. These organisations coordinate their activities under the National Committee of the No Hate Speech Movement. The whole campaign is realised under the auspices of the Section of National Care for Sport and Youth – the ministerial Department for Youth. The campaign aims to increase the knowledge of youth and their involvement in fight against hate speech on the internet. It informs them further about the effects caused by this phenomenon.

The campaign is carried out online through various tools created by the Council of Europe – online courses for young people, guides for elementary and high schools, and through its active promotion via social networks. The campaign is supported in OFFLINE form, too, through various attractive activities during summer festivals and such events as Pohoda, Bažant na Mlynoch and Hug Day, also during sport events (UEFA European Under-17 Championship in May 2013) and via various competitions: the best video, drawing or story about a given topic, which can be found on the campaign web page and Facebook. The campaign topic became a theme for the Human Rights Olympic Games for elementary and high schools in 2014. The campaign was promoted through promotional and educative materials, courses and trainings for bloggers and presenters of internet platforms, including vast number of young people. The campaign has been promoted also in media: in The Radio and Television Slovakia in a program for youth "Five minutes after twelve", in TA3 "Talks over the midnight", and through radio channels – Radio FM, etc. We aim to place a special emphasis mainly on a non-formal education when we work with youth. The Slovak Youth Institute (IUVENTA) realises national projects called KomPrax and PRAKTIK through accredited trainings for young leaders, youth leaders and for those who work with youth and multipliers. The trainings were organised by the Youth Council in Žilina region with financial support from the Ministry of Education.

The civic association eSlovensko, a member of the National Committee, organized a project NEHEJTUJ.sk – a methodical material for teachers at elementary schools.

The campaign included also some international activities with partners from Serbia (festival in Vrnjacka Banja, Regional Bus project). The campaign activist participated also in international events, last time in a Gabala (Qabala) Forum in Azerbaijan.

The campaign aims to prepare a research studying intolerance on the internet, whose results will be published during the final evaluation conference in June 2015.

The Methodology and Pedagogy Centre (MPC) is a separate budget organisation established by the Ministry of Education under the Act of the Slovak National Council No. 596/2003 Coll. on State Administration in Education and School-self-government, as amended. The centre focuses on methodical activities and continuous education for educators, expert and non-pedagogic employees of schools and school facilities in Slovakia. In order to improve the media literacy of teachers and professional employees, the centrum realises a project called **Activating methods in education**. The project should result in an analysis on interactive didactic tools that should improve the media education and critical thinking in relation to traditional and new media.

The MPC cooperates with the International Centrum for Media Literacy at the Faculty of Mass Media Communication **of the University of Ss. Cyril and Methodius in Trnava (visit** www.medialnavychova.sk). Together, they have signed a Memorandum on cooperation in 2012 along with other non-profit organisations, particularly with the eSlovensko.

Educational Activities

MPC undertakes trainings within the accredited educational programmes. Under the national project entitled "Professional and Career Development of Teaching Staff", as to **10 September 2014,** MPC managed to have **accredited 543 educational programmes** (hereinafter referred to as "AEP") (over the period of **2010 - 2014**). Below are the numbers of participants and graduates of AEP giving focus to the topics in question over the period of 2010-2014. The figures concerning the participants who passed, as to 31 August 2014, the programmes having dedicated priority themes under continuing education and training system are referred to in the progress chart of the national project the Professional and Career Development of Teaching Staff.

The issues of **promotion and development of digital competences of teachers and of information and communication technology** (ICT) are incorporated in **78 AEP** across their topics. Working with digital technology is integrated into several school subjects (general education subjects and subjects of educational treatment), and its objective is to facilitate learning through ICT via integration of the digital technology into the teaching and learning of languages – English, Hungarian, German and Slovak. In the years 2010-2014, **25,313 participants** were delivered the above topics, the number of graduates thereof was **21,477.** In 2014, there were **7,486** participants and **7,035** graduates. Promotion of media literacy is the main topic in **4 AEP**, we registered **441** trainees and **320** graduates by 2014. **11 AEP** give focus to the prevention of socio-pathological phenomena. In the years 2010-2014, there were **481** participants and **362** graduates of these programmes in the MPC.

Works devoted to those topics were published during the implementation of two national projects. The end results include 4 textbooks explaining risks and threats posed by the internet. 16 textbooks were published within the national project entitled the Education of Teaching Staff of Kindergartens, a part of lifelong learning aimed at digital and information technologies.

Within the national project Professional and Career Development of Teaching Staff, MPC published **3 textbooks** on the topic concerned**:**

- Bobot, V., Jakubeková, M. **School Information Security**. ISBN 978-80-8052-486-9, 64pp.
- Oľšavská, M. **Selected Elementary Information on the Prevention of Socio-pathological Phenomena, Part One**. ISBN 978-80-8052-684-9, 52pp.
- Oľšavská, M. **Selected Elementary Information on the Prevention of Socio-pathological Phenomena, Part Two** ISBN 978-80-8052-685-6, 38pp.

Within the national project Education of Teaching Staff of Kindergartens, a part of lifelong learning, there was published **one educational material** covering the issues of safety of children on the internet:

- Kalaš, I. et alia **Digital Technologies in Kindergartens 6**. ISBN 978-80-8052-584-2, 2013, 41pp.

MPC published on 13 December 2013 a specialized issue of the professional and methodological journal Pedagogické rozhľady No 4-5/2013 (New Issues in Pedagogy, *translator's note*) which gave focus to media education and related media literacy. The topics of cybercrime and exploitation of children on the internet are covered in 2 professional articles:

- Hollá, K. **Media Education as Prevention of Risky Online Risky Behaviour.** Pedagogické rozhľady. Professional and methodological journal for schools and educational facilities 4-5/2013. Bi-monthly Journal. Volume 22, p. 19.

The Project Slovak Safer Internet Centre is a Community project giving as a priority focus to safe and responsible use of the internet and mobile phones. An umbrella organisation of the project in Slovakia in terms of its organising and managing is a civic association eSlovensko. The European Commission provided 50% of the funds and the remaining 50% is covered by the partners involved in the project.

In 2013-2014, the Ministry of Education, Science, Research and Sport of the Slovak Republic along with the Slovak Committee for UNICEF was **one of the partners of the project Slovak Safer Internet Centre, and it co-funded it**.

The project entitled Slovak Safer Internet Centre started in 2011 – 2012, and it has continued as Slovak Safer Internet Centre II in 2013 - 2014. The main **objectives of the project** were as follows:

- **Establishing and running the national awareness raising centre - Zodpovedne.sk**, in which every year thousands of children, teaching staff and parents are delivered instructions and lectures on responsible use of the internet, mobile communication, new technologies and on the crime prevention,
- **Establishing and running the free helpline Pomoc.sk** serving the purpose of addressing the problems of children on the internet,
- **Establishing and running the national centre for reporting illegal content on the internet Stopline.sk**,
- **Creation of children's animated series OVCE.sk**, which in its 24 parts deals with various areas posing threats in virtual world, ethics in mobile communication, social inequality and suchlike. The tales are also available in minority languages as well as in sign language for deaf children and with an audio commentary for blind children.

During the project, the cooperation has also been established with the following organisations falling within the competence of the Ministry of Education, Science, Research and Sport of the Slovak Republic:

- National Institute for Education - when incorporating the topics of safe and responsible use of new technologies into the subject of Informatics,
- Methodology and Pedagogy Centre - in the area on continuing education and training of teaching and non-teaching staff as well as youth service workers,
- Research Institute for Child Psychology and Pathopsychology - in the area of research aimed at behaviour of minors and juveniles on the internet,
- IUVENTA - when working with youth service workers and volunteers.

The project was granted several awards in 2013 and 2014 (a prize at The World Summit Award in the category of e-Inclusion & Empowerment, Panta Rhei Award in the category of "Top Bestseller for Kids" for the book OVCE.sk, KOMENIUM PRIX prize), and it is a positive example of successful cooperation of a non-profit sector with the state administration.

8.3 Prevention

8.3.1 National legislation/policy and other measures

The State prevents and fights online frauds with payment cards in cooperation with a bank sector. Preventive measures are adopted primarily through media and campaigns that aim to protect bank clients in Slovakia. Commercial banks issuing payment cards apply specific technological measures (e.g. on the level of transaction authorisations). Criminal police officers are acquainted with these crimes during professional trainings but they may also study how these crimes can be committed during a higher police education.

Pornography and its spreading (i.e. its production, purchase or any other acquisition, its subsequent sale, purchase, hiring or any other form of its entering into circulation, public or private spreading) through sound, picture or any other carriers is considered harmful and undesirable because it may endanger morality. Individual cases with pornographic materials showing disrespectful behaviour towards humans, violence or sexual intercourses with animals or any other sexually pathological practices are particularly reprehensible – they are punishable under the act No. 300/2005 Coll. – the Criminal Code, as amended –Section 371 and the following.

Similar activities are not only morally unacceptable by the whole society or risky for healthy development of underage people but they even establish a criminal liability and its subsequent enforcement through a punishment.

According to Section 372 (1) (a) (b) of the Criminal Code, a person is punishable by law if he/she offers, cedes or sells any pornographic material to a person below 18 years of age or if he/she leaves such material at any place that is accessible by non-adults. Therefore, this section establishes a **crime of Corrupting Morals** where the offender acts against a particular social group – against persons who are younger than 18 years of age. The crime presupposes a specific group of potential victims (objects) who are considered as highly sensitive and vulnerable from psychological view but also from a broader society-wide perspective. The objective aspect of the crime lies in a perpetrator´s action committed against persons who have not reached 18 years yet, and the action must be performed in one of the ways stated in Section 371 (1) (a) or (b) of the Criminal Code. It is important to stress out that it is sufficient to complete the crime if a perpetrator commits any of the actions listed in Section 372 (1) of the Criminal Code against one under aged person[13].

An act of offering is defined as any presentation of a pornographic material with the real intension to provide it to an underage person. Most frequently, the perpetrator´s offer may be realised through a purchase contract, but he/she may also lend it or forward it as a gift, etc. Of course, an internet environment offers the perpetrator an easy option to make the pornography material publicly accessible, with a possibility to download it. So, if anyone places a content on the Internet, he/she makes it accessible to public.

A place accessible to underage persons is any place which is usually visited by them. Similarly, in case of the Internet (there is no objective doubt that it is accessible also for persons who are younger – even much younger – than 18 years of age), a pornographic material is displayed or made accessible via web pages. Web pages with such content should be made inaccessible to under aged persons. There is no protection that is legally regulated on a technical level, but generally it includes:

[13] The person under the 18 years old.

(i) **A registration principle**, which means that when a person wishes to access a web page containing a pornographic material, he/she must fill in an on-line registration form with their name, address and other contact details. Thanks to the data, the web page operator shall verify the visitor´s age without any problems.

(ii) **A technical safety measure** may be described as any process, product or component entered into a process, product or device which aims to prevent, reduce or stop any unauthorised access.

(iii) **Subscription system and paid access** mean that if a person wishes to enter a web page with a pornographic content, he/she is obliged to register and pay in order to gain access to the web page content based on a fixed price list.

Of course, safety measures can overlap or complement each other. Even a web provider who offers a (virtual) place for file sharing must not forget to secure the content against unlimited or an easy access for underage persons. If a provider would neglect this duty or would not fulfil it effectively enough (which, in the end, shall be decided by a court), the provider could potentially become at least an accomplice committing the crime of Corrupting Morals in the form of assistance. It is necessary to clearly declare that a web page content is not suitable for non-adults.

The conclusions on the protection of children in the digital world of the Council of the European Union (2011/C 372/04) stresses out, that in order to enable maximal usage of opportunities offered by audio-visual media and internet, it is necessary to create a safe media environment for under aged persons. This shall be built on principles of human dignity, safety and respect for private life. The education sector considers **media literacy and awareness-rising** as important tools which can significantly improve media competence of children, parents and teachers so they can develop their critical approach towards audio-visual and online materials. Still, we need to improve our efforts as the digital environment is changing far too rapidly. In this document, it is further declared, that the current level of protection and media literacy is generally not sufficient and some measures lack continuity.

At the same time, the Council of the European Union calls upon the Member States to respect the freedom of expression on one hand, but also to continue their efforts to protect children on the other hand. MS should support major campaigns aimed to raise awareness of children, parents, teachers and other persons who work with children in order to maintain consistency between teaching of online safety and media literacy at schools and in other institutions that provide education and care for children.

On 24th October 2014, the Slovak Government adopted **"Conception of computerization and digitalization of the education sector until 2020"** (the original title in Slovak: "Koncepcia informatizácie a digitalizácie rezortu školstva s výhľadom do roku 2020"). The conception introduces a basic idea for further development of education, science, research and sport with regard to global trends of digitalization and development in Slovakia. Its main aim is to define needs and activities in the computerization and digitalization process of the education sector in coming years, making educative institutions improve their quality, while the ministry shall provide them with an adequate help. Through computerization and digitalization, the ministry aims to adjust the education to the market and practical needs. The conception shall further develop into action plans which will define exact tasks, responsible institutions and deadlines, so the ministry will be able to control regularly how the concept is being followed and fulfilled. In April 2015, the government is going to pass an action plan focused on rising pupils´ and educators´ digital competence, where one of the most important pillars shall be an education streamlining safe usage of ICT tools.

There is also a **Conception of media literacy in context of a life-long education** (the original title in Slovak: "Koncepcia mediálnej výchovy v kontexte celoživotného vzdelávania") which was adopted by the Slovak Government on 16th December 2009 by resolution No. 923. This conception focuses on the media literacy importance, with an emphasis placed on online dangers and internet safety.

Information education and cyber safety on elementary schools

Pupils learn cyber/informatics safety mainly in a subject called **Information Education and Informatics.**

In order to reach goals set for education and training on elementary schools, there were created fixed standards (for performance as well as for the curriculum). Each specified performance has its own learning concept which is structuralised into separate thematic units. A teacher can modify the learning concept of a thematic unit according to his/her current needs. When a child completes an educational degree, he/she should master the whole educative standard of The National Education Program.

On the 1st stage of elementary school – ISCED 1, pupils learn information safety in a subject called Information Education. **Its aim is to provide pupils on the 1st stage of primary education** with a computer acquaintance and learn them perform everyday tasks.

In order to maintain continuity between various subjects, pupils train mathematics, Slovak and foreign languages through various computer applications. They gain new knowledge with support from educative programs in biology and geography and they further develop their creativity and aesthetic feeling through various graphic editors.

Meanwhile, the emphasis is not placed on the fact that children would have to master an application but that they understand the many options they can use on daily basis. As most suitable appear to be programs specially developed for pupils. Through them, children can familiarise themselves with the most commonly used computer functions (applications intended for adult users are not suitable because of their excessive complexity). In a thematic circle **Communication through ICT, pupils learn following terms**:

- e-mail, e-mail program, e-mail address, directory
- www, web browser, web page, link, site search,
- safety, code of conduct in internet environment.

On the 2nd stage of elementary school, pupils should master the basic terms and techniques that can be used in work with data and algorithm creation or in computational process. Similarly to mathematics, informatics in combination with ITC creates a basis for other subjects. In a subject called Informatics, it is necessary to focus the study on basic universal terms that go beyond current technologies. Available technologies should provide Informatics lessons with a lot of space for motivation and practical projects.

The educational and training process on the 2nd stage of elementary school lets pupils:

- familiarise with following terms: datum and information, various types of data, data collection, data saving, data display, data processing and data presenting,
- understand terms as algorithm and program (formal registration of automated data processing),
- familiarise with systems for data processing and their composition (computer, additional devices, media, communication) and logical structure (e.g. operating system),
- develop their abilities to turn a problem into an algorithm, develop their programmer skills, learn to work in common environment of application programs, learn to effectively search for information burned on CDs or saved in a network, and learn to communicate via network,
- gain skills necessary for research (ability to create a simple research project, formulate a problem), develop their formal and logical thinking, learn various methods of problem solving,
- develop their cooperative and communication skills (pupils learn to cooperate within a group and solve problems together, openly speak and discuss a problem and refer about it),
- develop their personality, creativity, logical thinking, responsibility, moral quality, will power, stamina, self-criticism, and self-control,
- learn to respect intellectual property and authorship of information products, systems and applications (to make children understand that information, data and programs are products of intellectual work, that they are objects of property rights and have a certain value), accept social, ethical and legal aspects of informatics.

On the 2nd stage of elementary school – ISCED 2, pupils have more options to develop their individual learning methods during Informatics classes. A thematic unit called **Software and hardware – work in computer network and on the internet** teaches children to orientate in various networks, use safety tools for sharing (copying, transferring), downloading and sending files. Another thematic unit **Software and hardware – fight against viruses and spying** covers these topics: spreading of computer viruses and spam, safe and ethical behaviour on the internet and social networks, hackers´ activities. Pupils can debate about risks that exist on the internet, about computer crimes, trustworthiness and credibility of information placed on a web, they learn to avoid dubious applications. In a thematic unit called **Information society – legality of software usage**, pupils can discuss principles of copyrights and how to obey them, legal consequences when someone uses a product illegally, or a topic covering criminal and illegal contents. In a thematic unit **Communication and cooperation**, pupils learn to judge information accuracy, and to compare pros and cons of communication via chat and e-mail.

Standard Curriculum

- Information technologies in knowledge society.
- Technology and its dangers, viruses, antivirus programs.
- Safety principles.
- Validity, information accuracy and dangerous content.
- Program licences, legal use, freeware, shareware.
- Legal use of pictures and texts from the internet.

Standard performance

A pupil:

- is able to use ICT in knowledge society (in areas of banking, health care, transport, art, etc.),
- understands how computer viruses are spread, how they can be discovered and removed. Knows internet safety and computer protection,
- knows computer crime dangers and its consequences,
- is able to judge reliability of a gained information,
- knows what a copyright is, and knows legal and an illegal software, and the difference in usage and spreading of programs with various licence levels.

Textbooks (exercise books) for the subject are approved by The Ministry of Education, Science, Research and Sports under the name Information education (1st stage of elementary school) and Creative informatics (2nd stage of elementary school).

The Creative Informatics textbooks cover a following content in relation to given topics:

Informatics around us – Computer and safety vs. dangers: dangers and risks, privacy and personal data protection, viruses, programs and licences, principles of safe conduct.

1st exercise book with internet – basic rules for safe internet usage,

2nd exercise book with internet – Internet traps: malware, spam, hoax, phishing and pharming, personal data misuse and identity theft, online bullying.

Currently, **the Department of the Regional Education System of the Ministry of Education, Science, Research and Sport** prepares changes in the curriculum for elementary schools in The National Education Program. It also plans to innovate education standards which will come into force from the 1st September 2015.

Cyber security on high schools

Informatics at high schools introduces students with basic terms, procedures and computer tools, it helps them build cybernetic culture, i.e. it teaches students to use more effectively tools, technologies and products provided by the information civilisation and respect legal and ethical principles. Students should master these during Informatics classes but also during other subjects where IT can be used and also through organisation and school management.

The educational-training process makes students:

- ☐ shift problems into algorithms to find their solutions, develop their programming skills;
- ☐ learn to work in an environment of common application programs (independently from a platform), learn to effectively search for information stored in a memory media or in a network, learn to communicate via network;
- ☐ develop their cooperation and communication skills (learn to cooperate in a group when solving a problem, create a plan for their work, specify problems and distribute them in a group, explain a problem to another student, solve partial problems, collect results, put them together into a final solution, refer the solution publicly together with the whole group);
- ☐ gather abilities necessary for research work (perform a simple research project, name a problem, find information from adequate source, find solution and causational links, verbalise their opinion orally and in a written way, discuss a problem, make conclusions);
- ☐ develop their personality, creativity, logical thinking, responsibility, morality and will power, stamina, self-criticism and endeavour self-control;
- ☐ respect intellectual property and copyright on IT products, systems and applications (to make them understand that data, information and programs are products of intellectual work, that they fell under authorship and have a certain value); make them understand social, ethical and legal aspects of informatics.

A textbook Informatics for students focuses on a safe communication – it teaches students to be cautious with their sensitive information so it would not get into wrong hands. One of the solutions is to encrypt their messages with a symmetric or an asymmetric encryption.

Students will familiarise with a protocol HTTPS for common communication, with a digital identification document – a server certificate, with a certification authority which enables them to verify the real identity of a certificated owner, and also with a hash function for verification of original data published on the internet.

In order to maintain the internet safety, we have created an **educational curriculum** that is applied on all degrees of regional schools (from a pre-school to a high-school level) and there is also an **obligatory summary topic "Media education"** whose aim is to familiarize children with media in a way that suits their mental level, "so they will be able to orientate themselves in the media environment and use various types of media in a safe way".

On the governmental level, this problem has been addressed also in the **Conception of Cyber Security of the Slovak Republic**, which is currently still underway. One of its priorities is to raise awareness and educate people about cyber security. The Slovak Government has established an interdepartmental working group which should elaborate the Conception of cyber security in the Slovak Republic. The group met for the first time on 6th August 2014. Its members come from the Ministry of Finance, the Presidium of the Police Force, the Ministry of Economy, the Ministry of Defence, the Ministry of Transport, Construction and Regional Development, the Ministry of Foreign and European Affairs, the Ministry of Health, The Ministry of Education, Science, Research and Sport, the National Security Authority, the Slovak Information Service, the Office of Security Council, the General Prosecution´s Office, the National Agency for Network and Electronic Services.

The coordinator of the information security of information systems of the public administration, the Slovak Ministry of Finance started **series of trainings for state employees**. A pilot series took place at the end of 2013 and next series followed in 2014. Educative materials were intended for project participants but also for open professional public. The materials should raise awareness and improve competences in information security area and therefore help in creation of safe environment in Slovakia (for more information visit http://informatizacia.sk/vzdelavanie-v-oblasti-ib/17005s).

Non-profit sector intensively informs the public about dangers on the internet, threats for mobile phones and other new technologies. One of the most active is an organisation called **eSlovensko**, which has prepared lots of materials including teaching guides. All materials can be used by teachers on elementary (www.ovce.sk) and high schools (www.nehejtuj.sk).

Research and survey

In 2014, the Slovak Centre of Scientific and Technical Information (a Department of Prevention and Research Among Children) made an **opinion survey** which had been requested by the Slovak Ministry of Education, Science, Research and Sport – it inquired **prevention coordinators and children** about bullying problems in elementary and high schools. The survey contained also questions about **cyberbullying, its manifestation and forms**.

The Research Institute for Child Psychology and Pathopsychology realised a research called **Slovak children and dangers of virtual space** (in Slovak *"Slovenské deti a riziká virtuálneho priestoru"*).

The Slovak Ministry of Education, Science, Research and Sport financially supported a project called **Research on Efficiency of Algorithms for Intelligent Recognition of Spam, Suggestions for Theoretical Models of New Algorithms and Their Efficiency Assessment** (under the Act No. 185/2009 Coll.).[14]

[14] For more information on the project, visit: https://www.vedatechnika.sk/SK/stimuly/Documents/Stimuly%202013/slovanet_prezentacia_2013_okt.pdf

KEGA – the Cultural and Educational Grant Agency of the Ministry of Education, Science, Research and Sport supported a research **042UK-4/2015** called **How to understand consumer behaviour among children and youth**, which was carried out by **The Comenius University in Bratislava**. This project analysed children´s behaviour with regard to marketing and media communication targeted for Slovak children and youth. Its compiled profiles grouped according to age cohorts will become grounds for creating further educative materials for schools and families. Such analysis became a world standard for protection of children and youth against aggressive persuasive methods. On the other hand, Slovak professional and general public relies only upon piecemeal and sporadic information and intuitive behaviour as there is no science-based systematic and comprehensive interdisciplinary analysis.

This project aims to provide the mentioned missing link. It is well-known that children are highly sensitive and non-protected percipients who are exposed to manipulative techniques used in marketing communication. This leads to increased commercialism and life dissatisfaction. Education in consumer behaviour should lead children and youth to acquire a consumer competence, i.e. critical judging of marketing and media communications that aims to affect their buying and consumer behaviour. It is very important to improve their consumer socialization, i.e. to make them obtain appropriate attitudes, habits, due knowledge and skills related to consumer and buying behaviour.

KEGA supported also a research **026UK-4/2015** called **Moral attitudes of children and adults in family and school: applied research and methodical material for teachers, education advisers and prevention coordinators**.

The University of Žilina carries out a KEGA project 505-070ŽU-4/2010 called **Media education and life-long learning of educators**. The research has a following annotation stating that the research project on moral attitudes of parents, children and teachers shall result in a practical guide – a methodical material for teachers, education advisers and prevention coordinators who work at elementary schools, where the problem of incorrect social and moral development shows as the most urgent. The suggested methodical workshop and the guide will be published in a printed form. Both will be derived from the most recent information gained from the research. They will also initiate a new preparation of elementary school teachers.

The non-profit organisation **eSlovensko** is currently realising a project called Zodpovedne.sk (in English: *Responsibly.sk*). The project is focused on a safe and responsible behaviour in usage of the internet, mobile phones and other new technologies. It is supported by the EU under a community program Slovak Safer Internet. It is targeted particularly at children and youth. So far, the project resulted in such publications as Children in the web, Ovce.sk.

a) **Ovce.sk** is a unique fairy-tale series about a safe internet. It has been available in Slovakia for three years. It shows children how to avoid the many dangers lurking in the internet and mobile communication. It can be found on www.ovce.sk (or with English subtitles at http://uk.sheeplive.eu/). It belongs among the most viewed webpages promoting safe internet using. Its three parts are devoted to such sensitive topics as cyber sexual harassment, sexting, disclosure of profile photos and responsible internet using. The parts bear names Fotoalbum, Harassment (*Obťažovanie*) and Responsibly (*Zodpovedne*). They are accompanied by audio commentary for visually impaired or even by a sign language for hearing-impaired. They have become very popular abroad – so far, they have been translated into 22 languages, including all EU languages and Chinese.

b) **Children in the web – How to protect ourselves and our children on the internet** is a new publication created by eSlovensko. On its 92 pages, it brings a basic overview of internet dangers. It explains how to recognise possible dangers and what they may look like. The publication is intended for parents but also for teachers and other people who work with children and youth and who want to study this issue deeper.

One positive example of self-regulatory activities related to protection of young children in Slovakia is "**The National Code for Mobile Operators on Safe Use of Mobile Services**" which was signed by all three mobile operators in Slovakia. It respects principles applied by the EU for protecting minors. The Code is published on www.orange.sk.

8.3.2 Public Private Partnership (PPP)

Ministry of Interior of the Slovak Republic uses Public Private Partnerships in prevention and fight against cybercrime. In this context can be noted that the Ministry of Interior has entered into joint projects of civil association Zodpovedne.sk. Description of the projects mentioned in point 1.2. In the case of the online payment card fraud, Ministry of Interior cooperates with private sector engaged in the detection and preventive measures, more precisely – in the development of applications detecting presence and operation of malicious code (malware, trojan or. other forms of malicious code). The cooperation is based on the exchange of information and cases detected their analysis and results, which are then used in the application of preventive measures. The cooperation is based on personal relationships, and there is no legal or contractual basis. But this is a cooperation based on experience with clarifying the threats and various forms of illegal activity.

8.4 Conclusions

- The Cybercrime unit conducts a 5 day training course on cybercrime for 25 officers, every three months. This course is for Regional and District police and provides basic training on cyber investigations including open source intelligence training and how to remain anonymous online.

- The Slovak authorities host a Judicial Academy within which prosecutors and judges can share best practices and experience.

- There is a certain scope to improve in the field of training of police officers who are in charge of investigation of this specific crime. The current situation is deemed insufficient when taking account of new cybercrime trends, despite the fact the situation has been improved in the past.

- Particularly in the field of prevention of child abuse online, Slovakia appears to be very active. Media literacy in the context of life-long education is fostered, and pupils starting from first stage of primary education are taught information safety. Cyber security is also addressed in high schools.
- The non-profit organisation E-Slovensko is an example to be followed, including for the training material developed for the youngster, with movies and books designed to explain the danger of "sexting", " disclosure of pictures" and "child grooming" to children in a very easy way to understand. The organisation is also very active in reporting to police when incidents appear to be related directly to Slovakia, or to INHOPE when incidents are more clearly linked to third States. They are also very active with the private sector, e.g. cooperation with Facebook is very good (for instance, in cases of cyberbulling via Facebook page they contact the Headquarters in Ireland and the page is removed quickly).

- E-Slovensko also facilitated a study to assess whether social molesters are always paedophiles or not. The study was presented during the visit and it was commented by the Team that its outcome should be disseminated to law enforcement and the judiciary as soon as possible. The outcome of this study is particularly relevant for adjudicating and sentencing purpose, as it was observed that in a number of cases a court did not sentence an accused because he/she was not determined to be a paedophile by the expert called to evaluate the suspect. The study shows that even if not a paedophile, in a high number of cases the accused is nevertheless a child sexual molester.

9 FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions and considerations from Slovakia

In recent period, the situation has improved also due to setting up of a specialised department within the Police Force and thanks to progressive capacity building of intervention teams as CSIRT / CERT, but this positive development has to be maintained in order to address topical threats. However, in the opinion of the law enforcement agencies, the capacities for preventing and combating cybercrime are currently very limited. Regarding capacity building in relation to carrying out expert examinations at the forensic institute established by the State, i.e. at the Institute of Forensic Science of the Police Force, the situation in the examination of computer technology is not entirely satisfactory. The Institute has 3 regional branches of digital forensics in the cities of Bratislava, Slovenská Ľupča and Košice. The Digital Forensics Department in Bratislava examines, in addition to computer technology, also mobile devices, their parts and SIM cards. The maximum time limits for the cases to be concluded are currently about 12 months as a standard. The Digital Forensics Department in Bratislava, however, suffers from high staff turnover.

For this reason, the private sector is employed very successfully to prevent cybercrime. Another problem is posed by the lack of flexibility in adopting effective legislation on cybercrime in order to address emerging threats.

It appears to be problematic to provide examples of good practice in combating cybercrime as this type of crime is developing very fast and the solutions found are very often outdated due to the availability of new technologies. Computer experts put forward technical solutions which may be subsequently reflected in the legislation what is, however, a time-consuming process at the end whereof such solutions are already overcome by technical progress. Given the fact that cybercrime is highly sophisticated type of crime, it is not possible to follow certain predetermined templates, but flexible and timely reaction is required conditional upon the special features of each particular case.

As an example of good practice, in the context of cooperation under the Convention on Cybercrime, namely when applying Article 29 (Expedited preservation of stored computer data), there was drawn up a standardized form, which is used mainly in cooperation with the USA and which greatly contributed to the facilitation of cooperation. Letters of request are sent by e-mail to the Interpol NCB and to the International Department of the General Prosecutor's Office of the Slovak Republic to an official e-mail address as scanned documents with attached signatures and the official stamp of the Prosecutor's Offices. At the International Department of the General Prosecutor's Office of the Slovak Republic, the records of the said requests (including incoming requests) are kept so as to bring an update of the situation in this field and, as the case may be, to identify problematic cases in advance and, if necessary, to consult them directly with the relevant authorities.

Some District Prosecutor's Offices do not have scanners, therefore they must sent a request to be scanned at the Police Force unit or at the superior Prosecutor's Office. In this regard, it would be appropriate to supplement the technical installations (it has been planned under the project OPIS).

One of the necessary conditions is the coordination of procedures and sharing the pieces of knowledge between the Police Force and the Prosecution Service, as well as the communication with telecommunications services providers, which occur at different levels.

It is necessary to undertake prevention and awareness raising activities for families and at schools, e.g. in relation to pornography, internet fraud, phishing, etc. The emphasis should be put on targeted searches of police authorities and on the analysis of classified crimes.

More attention should be focused on the effectiveness of the criminal law system when it comes to forfeiture of the proceeds or instruments of crime.

At the national level, it would be advisable to keep records on major cybercrime cases. In the field of international cooperation, it would be appropriate to create, at a level of the EU, a register containing both the successful and failed cases of legal assistance which could provide a guidance on how to resolve similar situations in the future. Such tool only makes sense provided that it is continuously updated and understandable (language barrier).

Within the framework of cybercrime prevention, Slovak authorities find it desirable to keep the general public informed, through all available media, about the forms of cybercrime (in particular, scams on the Internet used to fraudulently obtain advance money), and to encourage user to take precautions while using the internet. Raising awareness is necessary to be started already with school-age children.

Added value for combating cybercrime lies undoubtedly also in training activities for the staff of the Police Force, Prosecution Service and courts designed to improve their knowledge of information technology. An alternative for improving the situation consists in considering the possibility to have the staff specialised in cybercrime in the Police Force (in particular, highly qualified professionals) and in the Prosecution Service, and in improving the technical equipment of departments. However, a consideration should be given to the fact that today cybercrime affects all criminal activities. Therefore the specialization cannot be considered as the only option. The international exchange of knowledge among the Police, Prosecution Service and courts is also necessary.

Improved results could also be achieved through speeding up and simplifying of the process of securing computer data already at the level of international police cooperation prior to sending letters rogatory in order to avoid failure in their obtaining, as well as through streamlining the processes of obtaining evidence in the context of legal assistance done between the judicial authorities.

Slovak authorities would like to repeatedly emphasise that, after the decision of the Court of Justice of the European Communities and the Constitutional Court of the Slovak Republic, realistic capabilities for the investigation of cybercrime have become extremely limited, and it is necessary to urgently find a solution to this problem at the EU level.

In legislative terms, we could see the benefits of the transposition of the Directive on cyber attacks. Other legislative proposals could address the obligation to report the incidents related to online fraud with payment cards. Further option is also the legal regulation on handling electronic data by operators and their provision to the Police Force and Prosecution Service.

The Criminal Department of the General Prosecutor's Office of the Slovak Republic prepared "the Evaluation of practical experience of prosecutors in the prosecution of perpetrators who allegedly having committed the criminal offences of production, dissemination and possession of child pornography", which also includes the issues related to sharing information on circulation and possession of child pornography provided by foreign entities. The lessons learnt indicated that the biggest problems are experienced when clarifying the contactless child pornography (i.e. dissemination via internet and its possession), in particular, when it comes to obtaining the information about its downloading from foreign servers. Because of the Slovak law of evidence, it is "a battle against time." Unless the data gained in the course of various international operations are processed without delay, they are rendered useless and the criminal prosecution is ineffective. It could be again highlighted that the identification of the perpetrators of cybercrime in international cyberspace is extremely hindered.

The International Department of the General Prosecutor's Office of the Slovak Republic elaborated a document entitled "Evaluation of the effectiveness of requests for preservation of stored computer data sent/received from abroad in the period 2009 – 2012 focused on the implementation of the Convention on Cybercrime dated 23 November 2001 by Slovak law enforcement agencies".

In connection with the sham contracting in the truck transport made to a large extent over the internet in cyberspace (orders, shipment confirmation, sending of documents, communication), in 2014, there was convened a working meeting of representatives of the General Prosecutor's Office of the Slovak Republic and the Supreme Public Prosecutor's Office of the Czech Republic. Bilateral meetings are considered to be a highly suitable method of seeking common solutions in the field of international cooperation.

The Cooperation of the International Department of the General Prosecutor's Office with the Interpol Bureau and with the Cybercrime Unit of the Police Presidium is to be highlighted. Recently a procedure was agreed on the basis of a real case (no translation, insufficient information on location of servers, scope of data to be seized etc.), which is considered as time saving procedure. If a foreign request for preservation of data is delivered to Interpol – Interpol forwards a request to International Department of the GPO and to the Cybercrime Unit at the same time. In case of missing translation, Interpol asks for it immediately. Cybercrime Unit checks, whether the information provided in the request for preservation is sufficient from the technical point of view and whether it is urgent (taken into account the existence of data). If needed, Cybercrime Unit provides further technical guidance. In the meantime, the International Department of the GPO considers legal issues. The analyses of the Cybercrime Unit are sent to the International Department of the GPO for consideration as well. For communication the specific e-mail channel was established. The information may assist in the evaluation of complexity of the information available and necessary for data preservation. International Department of the GPO sends a foreign request to subordinated competent prosecutor´s office (it has also a possibility to deal with the request alone) together with any necessary legal or technical information already identified. The letter addressed to the subordinated prosecutor´s office contains contact details of the Cybercrime Unit (the local prosecutor´s may need to consult technical issues). The legal issues may be consulted with superior prosecutor´s offices.

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 Slovakia was able to satisfactorily review the system in this country.

Slovakia should conduct a follow-up on the recommendations given 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 fit to make a number of suggestions for the attention of the Slovak authorities. Furthermore, based on the various good practices, related recommendations to the EU, its institutions and agencies, Eurojust, Europol and ENISA, are also put forward.

9.2.1 Recommendations to Slovakia

The Slovak Republic should:

1. Next to the fields of cyberdefence and cybersecurity, endeavour the alignment with the European Agenda on Security in the area of prevention and repression of cybercrime (cf.3.2, 3.5);

2. Ensure accuracy of statistical data on cybercrime, including by progressing towards interoperability of the various relevant databases as a priority, with a view to quickly achieving cases comparison, criminal identification, cases quantification etc.; a first important step in this process should be to set-up the necessary structural modifications of those databases, for instance adding special fields signalling the event as cybercrime (cf.3.3,3.5);

3. Consider establishing a national network of focal points prosecutors especially trained in cybercrime matters within all regions of Slovakia and general prosecutors offices; such a network may offer an alternative to the creation of a specialised branch of the Prosecution Service while gathering feedback on operational cases and helping to coordinate prosecutorial actions and define an efficient nationwide prosecution policy in this matter (cf. 4.1, 4.5);

4. Consider to set up a similar formal network within the Police Force at regions level and, if possible, lately at district level (as "contact points" these policemen should benefit from continuous specific training in cybercrime) ; such a network could also help maintaining a communication channel from public and private sector to the police (cf. 4.2, 4.5, 6.2, 6.3, 6.4);

5. Continue and increase training; in this aim make more use of CEPOL's Officer Exchange Program and ECTEG courses with a view to facilitating knowledge flatten and spread, in less time, with less expenses and for more criminal investigation officers, thus producing a "body of knowledge" and operational capability which will therefore enhance magistrates and other fellows assistance with more confidence and overall quality; not only police, but also prosecutors and judges should benefit from such training; it is of great importance that officers and magistrates dealing with cybercrime cases are the ones attending special courses in this area (cf. 8.1, 8.4);

6. Seek to invest in its online surveillance capability ; consideration should be given to the use of new technical possibilities in tackling computer crime on-line as well as to legal regulation related to such new possibilities (cf. 6, 8.4);

7. Consider developing a user-friendly handbook of best practices for police officers as first responders and other police officers (Reference can be made for example to ENISA's "Good practice material for first responders") (cf. 8.1, 8.2, 9.1);

8. Enhance coordination of the actions of various stakeholders involved at national level in the fight against cybercrime (cf. 4.4, 4.5);

9. Make better use of the data it has available to it; the CSIRT would appear to hold a wealth of intelligence related to cyber/computer crime which for some reasons does not lead to investigations; Slovakia could furthermore make more efficient use of the analysis and services provided by Europol/EC3. By increasing exchanges the national law enforcement authorities would not only enrich their own investigations but also those of the whole EU wide law enforcement community. Last but not least, it may also allow them to better assess the scale and scope of cybercrime affecting the Slovak Republic (cf. 3.5, 6.1, 6.4, 7.1);

10. Conclude, and run as quickly as possible the draft agreement currently being negotiated between the Ministry of Interior (dealing with cybercrime) and the Ministry of Finance (running CSIRT.SK); inform GENVAL, in the follow up to the visit, whether this agreement has been signed, and if so, if it has contributed to an improvement in the recording of cybercrime cases (cf. 4.4.2, 4.5);

11. Improve the existing on-line reporting mechanism for non-child abuse related crimes (facilitating reporting by citizens about and strengthening the fight against cyber/computer crime and online fraud) in the project stopline.sk (cf. 6.2.3, 6.4);

12. Continue to enrich the national substantive and procedural legislation applicable to cybercrime matters and to adapt it to the particularities of the virtual world (e.g. DoS and DDoS attacks, virtual currencies…); moreover create urgently a legal framework to address undercover investigations in cybercrime (cf. 5.2.3, 5.5, 6.1.1);

13. Continue to actively supporting, also financially, projects from the private sector contributing to the prevention of, awareness of and fight against cybercrime, such as those run by the civic association E-Slovensko (cf. 6.2, 8.2,8.3, 8.4), (*see also Rec.15 below*) ;

14. Consider facilitating the dissemination and raising awareness of the scientific study on child sex molester to all competent national authorities ; more generally consider to improve relations with academies in relation to cybercrime (cf. 8.4);

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

The European Commission should:

15. Continue supporting, in particular financially, the various projects focusing on the dissemination of information about the safe and responsible use of the Internet and mobile phones, about the threats present in cyberspace in particular to the youth, and possibilities for getting advice and assistance, such as the excellent and multi-awarded projects developed and maintained by the civic association E-Slovensko (e.g. stopline.sk, zodpovedne.sk, pomoc.sk etc.) (cf. 6.2, 8.2, 8.3, 8.4);

The Member States and the European Union institutions should respectively:

16. Explore any possibility of creation of common statistical denominators in the field of cybercrime, including harmonised methodology, methods for data collection and evaluation at European Union level (cf. 3.3, 3.5);

17. Consider organising, and support the organisation of, operationally-oriented trainings on the whole life-cycle cybercrime case, where speakers and participants involved are practitioners from police, prosecutorial and judicial authorities and from private sector (cf. 8.1, 8.4);

18. Explore any possibilities legally available to address the issue of the retention and use of relevant data for the purpose of fighting against cybercrime in accordance with human fundamental rights; better engage in a dialogue with the private sector, the academic world and with third States authorities to this end (4.1.2, 5.4.2, 5.4.4, 5.5, 6.1.2);

The Member States should:

19. Consider including in their on-site visit program the possibility to engage with the judiciary and in particular judges and courts, and to appoint prosecutors and judges among the national experts to take part in the 7th Round of mutual evaluation visits; present real cybercrime cases to their evaluation team possibly from the police's, prosecution's and judiciary perspectives;

20. Consider engaging in, and maintaining, a constant dialogue with the private sector and discuss methodologies to ensure that the gathering of E-evidence takes place in a way to allow its admissibility in Court, including the principles of confidentiality, availability, integrity and non-repudiation of evidence (cf. 5.2.3, 5.5, 8.1, 8.4);

21. Consider establishing a national network of members of the Judiciary with specific knowledge (or specialisation) in cybercrime matters, including with a view to exchanging knowledge and experience between the members of the network and facilitating the spreading of best practices (cf. 7.1, 7.5, 7.6, 9.1);

22. Take inspiration from the Slovak best practice to engage direct communication with competent authorities of another State, especially third States to the EU (e.g. USA), to clarify beforehand possible issues ; a form for requests of expedited production order agreed upon by executing authorities in a given state is also to be considered as a best practice (cf. 4.1, 9.1);

9.2.3 Recommendations to Eurojust/Europol/ENISA

Eurojust should:

23. Continue and develop training activities/seminars in the field of cybercrime (cf. 7.1, 7.6, 9.1);

24. Consider facilitating contacts among magistrates with a special knowledge in cybercrime with a view to fostering exchange of views and practices (cf. 7.1, 7.6, 9.1);

25. Collect and disseminate case studies and best practices at national level identifiable from national and Eurojust's casework, in particular when judicial cooperation in criminal matters is at stake (cf. 7.1, 7.6, 9.1);

Europol/EC3 should:

26. Consider proposing to Member States a standard approach on structural elements for criminal intelligence databases in cybercrime (cf.3.3, 3.5) ;

27. Facilitate the adoption of a common taxonomy on cybercrime (cf.3.3, 3.5).

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

7th Round of Mutual Evaluations – Slovakia – 17-20 FEBRUARY 2015

Tuesday 17 February 2015

9:00 - 9:20 : Welcome speech by Mr. Milan Lučanský (1st Vice-president of the Police Force)

10:00 - 10:15 : Welcome Speech by Mr. Juraj Palúš (Director General of the legislation Section) Introduction of the Judiciary system in Slovakia
10:15 - 10:35 : Legislative adjustment of Cybercrime in Slovak Republic - transposition of Directive 2013/40/EU of 12 August 2013 on attacks against information systems

10:50 - 11:10 : Judicial cooperation in criminal matters/legal contact with foreign countries
11:10 - 12:00 : Questions & answers

14:00 - 14:15 : Status and scope of Prosecution in Slovak Republic
14:15 - 14:30 : Cybercrime and international cooperation in criminal matters

14:45 - 16:30 : Discussion with district, regional, general prosecutors and with the prosecutor from the Office of the Special Prosecutor

Wednesday 18 February 2015

9:00 - 9:15 : The Cybercrime Unit - Position and tasks in the structure of the Police Force
9:15 - 9:30 : Cybercrime - the field of cyber attacks in the Slovak Republic

9:45 - 10:05 : The Role of the Police Force of the Slovak Republic in the fight against on-line child sexual exploitation
10:05 - 10:20 : On-line Card Fraud - what we can do?
10:20 - 10:30 : The activities of the National Central Bureau of Interpol in relation to cybercrime
10:30 - 10:40 : Europol National Unit within international information exchange of cybercrime
10:40 - 12:00: Questions & answers

13:45 - 14:00 : The structure of Regional Directorates of the Police Force
14:00 - 14:45 : The current difficulties in clarifying and investigating of sexual child abuse crime with using information technology by Mr. Marek Koman (Head of the Investigation Unit of the District Directorate of the Police Force in Bratislava II.)

15:00 - 15:45 : The current difficulties in clarifying and investigating of sexual child abuse crime with using information technology by Mr. Marek Koman (Head of the Investigation Unit of the District Directorate of the Police Force in Bratislava II.)
15:45 - 16:30 : Questions & answers

Thursday 19 February 2015

9:00 - 9:10 : Welcome speech by Mr. Vazil Hudák (State Secretary of the Ministry of Finance of the Slovak Republic)
9:10 - 10:35 Role and responsibilities of the Ministry of Finance in the area of cyber security by Petra Hochmannová (Head of government CSIRT.SK - DataCentrum)

10:50 - 11:05 : Role of the National Security Authority in Cyber Defence by Mr. Mário Italy (Director of Information security and electronic signate Department)
11:10 - 11:20 : Activities of the Slovak Intelligence Service in the fights against the cyber attacks (employee of the SIS)

13:00 - 14:00 : gSlovak leader in Safer internet tools/activities for minors and combatting online child sexual abuse material (part 1) by Mr. Miroslav Drobný (President of the E-Slovensko)

14:15 - 15:15 : Slovak leader in Safer internet tools/activities for minors and combatting online child sexual abuse material (part 2) by Mr. Jan Hajek (Project manager of the E-Slovensko)
15:15 - 15:45 : Questions & answers
15:45 - 16:05 : Security and Integrity of networks and services and Personal data breach notification

Friday 20 February 2015

9:15 - 10.30 : Questions and answers - Evaluation of the mission.

10.30 - 11.00 : Closing ceremony

ANNEX B: PERSONS INTERVIEWED/MET

Meetings 17 FEBRUARY 2015

Venue: Ministry of Interior, Presidium of the Police Force, Bratislava

Person interviewed/met	Organisation represented
Milan Lučanský	Presidium of the Police Force (1st Vice President of the Police Force)
Anna Jarabá	Presidium of the Police Force (Assistant to the 1st VP) and GENVAL delegate for Slovakia
Róbert Bohunický	Presidium of the Police Force, Criminal Police Bureau (Senior police officer of the Operational Department)
Stanislav Španko	Presidium of the Police Force, Criminal Police Bureau (Head of the Cybercrime Unit)
Daniela Talapková	Presidium of the Police Force (officer of the sekretariat of the 1st VP)
Branislav Boháčik	International Department of the General Prosecutor´s Office (Prosecutor)
Ján Lehotský	Ministry of Justice (Chief State Adviser)
Martin Jurčík	Ministry of Finance, DataCentrum (employee of gevernment CSIRT.SK)

Venue: Ministry of Justice, Bratislava

Person interviewed/met	Organisation represented
Juraj Palúš	Ministry of Justice (General Director of legislation section)
Ján Lehotský	Ministry of Justice (Chief State Adviser)
Stanislava Juríčeková	Ministry of Justice (General State Adviser of the Judicial Cooperation Department)
Richard Sviežený	Ministry of Justice (Director of the legislation department)
Branislav Boháčik	International Department of the General

	Prosecutor´s Office (Prosecutor)
Anna Jarabá	Presidium of the Police Force (Assistant to the 1st VP) and GENVAL delegate for Slovakia
Stanislav Španko	Presidium of the Police Force, Criminal Police Bureau (Head of the Cybercrime Unit)
Róbert Bohunický	Presidium of the Police Force, Criminal Police Bureau (Senior police officer of the Operational Department)
Daniela Talapková	Presidium of the Police Force (officer of the sekretariat of the 1st VP)
Martin Jurčík	Ministry of Finance, DataCentrum (employee of gevernment CSIRT.SK)

Venue: Prosecutor General's Office, Bratislava

Person interviewed/met	**Organisation represented**
Peter Šufliarský	Deputy of the General Prosecutor for the Criminal matters
Alica Kováčová	International Department of the General Prosecutor´s Office (Head of Department)
Branislav Boháčik	International Department of the General Prosecutor´s Office (Prosecutor)
Tibor Šumichrast	Criminal Department of the General Prosecutor´s Office (Prosecutor)
Oliver Janiček	Regional Prosecution´s Office Bratislava (Deputy Regional Prosecutor for Criminal Matter)
Juraj Novocký	Special Prosecutor's Office (Prosecutor)
Svetozár Chabada	District Prosecutor´s Office Bratislava II. (Deputy District Prosecutor)
Matúš Harkabus	Regional Prosecutor´s Office Žilina (Prosecutor)
Anna Jarabá	Presidium of the Police Force (Assistant to the 1st VP) and GENVAL delegate for Slovakia
Ján Lehotský	Ministry of Justice (Chief State Adviser)

Person interviewed/met	Organisation represented
Stanislav Španko	Presidium of the Police Force, Criminal Police Bureau (Head of the Cybercrime Unit)
Róbert Bohunický	Presidium of the Police Force, Criminal Police Bureau (Senior police officer of the Operational Department)
Daniela Talapková	Presidium of the Police Force (officer of the sekretariat of the 1st VP)
Petra Hochmannová	Ministry of Finance, DataCentrum (Head of gevernment CSIRT.SK)

Meetings 18 February 2015

Venue: Presidium and Regional Directorate of the Police force, Bratislava

Person interviewed/met	Organisation represented
Stanislav Španko	Presidium of the Police Force, Criminal Police Bureau (Head of the Cybercrime Unit)
Radoslav Lefčík	Presidium of the Police Force, Criminal Police Bureau (Senior Police Officer at the Cybercrime Unit)
Ivan Bacigál	Presidium of the Police Force, Criminal Police Bureau (Senior Police Officer at the Cybercrime Unit)
Róbert Bohunický	Presidium of the Police Force, Criminal Police Bureau (Senior police officer of the Operational Department)
Monika Gorylová	Presidium of the Police Force, National Central Bureau INTERPOL (Senior police officer)
Róbert Uhrecký	Presidium of the Police Force, Europol National Unit (Head of Unit)
Anna Jarabá	Presidium of the Police Force (Assistant to the 1st VP) and GENVAL delegate for Slovakia
Melánia Dornáková	Regional Directorate of the Police Force in Bratislava (Head of the Criminal Police Department)

Person interviewed/met	Organisation represented
Marek Koman	District Directoriate of the Police Force Bratislava II. (Head of the Investigation Unit)
Daniela Talapková	Presidium of the Police Force (officer of the sekretariat of the 1st VP)
Branislav Boháčik	International Department of the General Prosecutor´s Office (Prosecutor)
Ján Lehotský	Ministry of Justice (Chief State Adviser)
Martin Jurčík	Ministry of Finance, DataCentrum (employee of gevernment CSIRT.SK)

Meetings 19 February 2015

Venue: Ministry of Finance, Bratislava

Person interviewed/met	Organisation represented
Štefan Adamec	Ministry of Finance (Advisor of the State Secretary)
Petra Hochmannová	Ministry of Finance, DataCentrum (Head of gevernment CSIRT.SK)
Martin Jurčík	Ministry of Finance, DataCentrum (employee of gevernment CSIRT.SK)
Zuzana Halásová	National Security Authority (employee of Information security and electronic signature Department)
Miroslav Brvnišťan	National Security Authority (Head of Acreditation Division)
Anna Jarabá	Presidium of the Police Force (Assistant to the 1st VP) and GENVAL delegate for Slovakia
Daniela Talapková	Presidium of the Police Force (officer of the sekretariat of the 1st VP)
Branislav Boháčik	International Department of the General Prosecutor´s Office (Prosecutor)

Person interviewed/met	Organisation represented
Ján Lehotský	Ministry of Justice (Chief State Adviser)
Stanislav Španko	Presidium of the Police Force, Criminal Police Bureau (Head of the Cybercrime Unit)
Miroslav Drobný	e-Slovensko (President)
Jan Hájek	e-Slovensko (Project manager)

Meetings 20 February 2015

Venue: Ministry of Interior, Presidium of the Police Force, Bratislava

Person interviewed/met	Organisation represented
Anna Jarabá	Presidium of the Police Force (Assistant to the 1st VP) and GENVAL delegate for Slovakia
Daniela Talapková	Presidium of the Police Force (officer of the sekretariat of the 1st VP)
Branislav Boháčik	International Department of the General Prosecutor´s Office (Prosecutor)
Oliver Janiček	Regional Prosecution´s Office Bratislava (Deputy Regional Prosecutor for Criminal Matter)
Ján Lehotský	Ministry of Justice (Chief State Adviser)
Stanislav Španko	Presidium of the Police Force, Criminal Police Bureau (Head of the Cybercrime Unit)
Zuzana Halásová	National Security Authority (employee of Information security and electronic signature Department)
Miroslav Brvnišťan	National Security Authority (Head of Acreditation Division)
Martin Jurčík	Ministry of Finance, DataCentrum (employee of government CSIRT.SK)

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	SLOVAK OR ACRONYM IN ORIGINAL LANGUAGE	SLOVAK OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CAM	-	-	Child Abusive Material
CCU	*CCU*	-	The Cybercrime Unit of the Criminal Police Bureau at the Presidium of the Police Force of the Slovak Republic
CERT	-	-	Computer Emergency Response Team
CSE	-	-	Child Sexual Exploitation
CSIRT.SK	*CSIRT.SK*	-	The Slovak national and governmental CERT
DAIS			Directive 2013/40/EU on Attacks against Information Systems
EC3	-		European Cybercrime Center at Europol
EJTN	-	-	European Judicial Training Network
EMPACT	-	-	European Multidisciplinary Platform against Criminal Threats
ENISA	-	-	European Network and Information Security Agency
EUROJUST	-	-	The European Union's Judicial Cooperation Unit
EUROPOL			The European Police Office
GENVAL	*GENVAL*	*Groupe de travail "Questions Générales y compris l'Evaluation"*	Working Party "General Questions including Evaluation"

IP	-	-	Internet Protocol
JIT	-	-	Joint Investigation Team
LEA	-	-	Law Enforcement Authorities
MLA	-	-	Mutual Legal Assistance
NBAC	*NBAC*	-	National Security Analysis Centre of the Slovak Republic
SBA	*SBA*	-	Slovak Banking Association
SIS	*SIS*	-	Slovak Information Service (Intelligence)
T-CY	-	-	the Committee of Parties to the Council of Europe Convention on Cybercrime
VOIP	-	-	Voice Over IP