Council of the
European Union

Brussels, 8 February 2017
(OR. en)

14586/1/16
REV 1 DCL 1

GENVAL 121
CYBER 134

DECLASSIFICATION

of document:	14586/1/16 REV 1 RESTREINT UE/EU RESTRICTED
dated:	31 January 2017
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 Slovenia

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

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

Council of the
European Union

Brussels, 31 January 2017
(OR. en)

14586/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 121
CYBER 134

REPORT

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 Slovenia

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 ____ 11
3.3.1 Main trends leading to cybercrime ____ 11
3.3.2 Number of registered cases of cyber criminality ____ 16
3.4 Domestic budget allocated to the prevention of and the fight against cybercrime, and support from EU funding ____ 17
3.5 Conclusions ____ 18

4 NATIONAL STRUCTURES ____ 19

4.1 Judiciary (prosecution and courts) ____ 19
4.1.1 Internal structure ____ 19
4.1.2 Capacity and obstacles to successful prosecution ____ 21
4.2 Law enforcement authorities ____ 22
4.3 Other authorities/institutions/public-private partnerships ____ 25
4.4. Cooperation and coordination at national level ____ 26
4.4.1 Legal or policy obligations ____ 26
4.4.2 Resources allocated to improve cooperation ____ 29
4.5 Conclusions ____ 29

5 Legal aspects ____ 31

5.1 Substantive criminal law pertaining to cybercrime ____ 31
5.1.1 Council of Europe Convention on Cybercrime ____ 31
5.1.2 Description of national legislation ____ 31
A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems ____ 31
B/ Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography ____ 62
C/ Online card fraud ____ 63
5.2 Procedural issues ____ 66
5.2.1 Investigative techniques ____ 66
5.2.2 Forensics and encryption ____ 71
5. 2.3 E-evidence ____ 72
5.3 Protection of human rights/fundamental freedoms ____ 75
5.4 Jurisdiction ____ 80
5.4.1 Principles applied to the investigation of cybercrime ____ 80
5.4.2 Rules in case of conflicts of jurisdiction and referral to Eurojust ____ 84
5.4.3 Perception of Slovenia with regard to legal framework to combat cybercrime ____ 84

5.5 Conclusions 85

6 Operational aspects 86

6.1 Cyber attacks 86
6.1.1 Nature of cyber attacks 86
6.1.2 Mechanism to respond to cyber attacks 87
6.2 Measures against child pornography and sexual abuse online 87
6.2.1 Software databases identifying victims and measures to avoid re-victimisation 87
6.2.2 Measures to address sex exploitation/abuse online, sexting and cyber bullying 88
6.2.3 Preventive actions against sex tourism, child pornographic performance and others 91
6.2.4 Actors and measures counteracting websites containing or disseminating child pornography 92
6.3 Online card fraud 95
6.3.l Online reporting 95
6.3.2 Role of private sector 98
6.4 Other cybercrime phenomena 98
6.5 Conclusions 101

7 International Cooperation 102

7.1 Cooperation with EU agencies 102
7.1.1 Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA 102
7.1.2 Assessment of the cooperation with Europol/EC3, Eurojust, ENISA 102
7.1.3 Operational performance of JITs and cyber patrols 104
7.2 Cooperation between the Slovenian authorities and Interpol 106
7.3 Cooperation with third states 107
7.4 Cooperation with private sector 109
7.5 Tools of international cooperation 111
7.5.1 Mutual legal assistance 111
7.5.2 Mutual recognition instruments 115
7.5.3 Surrender/extradition 116
7.6 Conclusions 121

8 Training, awareness raising and prevention 122

8.1 General and specific training 122
8.2 Awareness raising 127
8.3 Prevention 133
8.3.1 National legislation/policy and other measures 133
8.3.2 Public-private partnership (PPP) 135
8.4 Conclusions 136

9 final remarks and Recommendations 137

9.1. Suggestions from Slovenia 137
9.2 Recommendations 139
9.2.1 Recommendations to Slovenia 140
9.2.2 Recommendations to the European Union, its institutions, and other Member States 142
9.2.3 Recommendations to Eurojust/Europol/ENISA 143

Annex A: Programme for the on-site visit and persons interviewed/met 144

Annex B: Persons interviewed/met _____ **145**

Annex C: List of abbreviations/glossary of terms _____ **147**

1 EXECUTIVE SUMMARY

- The on-site visit to Slovenia was well organised and the evaluation team met highly motivated and welcoming colleagues; particularly noticeable was the preparation for and involvement in the visit by the main stakeholders - Slovenian officials from the Ministry of the Interior and the police. The team, however, regretted the lack of presentations from the prosecution service and the absence of meetings with representatives of the judiciary.
- Slovenia has developed a draft national cybercrime strategy; this document, as described to the evaluation team, prioritises adequate financial, human and material resources to effectively combat cybercrime.
- In all countries, including Slovenia, moving forward in the fight against cybercrime requires a high level of political will, budgetary efforts and enhanced coordination. As regards the latter, the evaluators got the impression that in general Slovenian practitioners knew and talked to each other. However, global institutional coordination between all competent bodies seemed to be in question.
- Slovenian authorities acknowledged that, due to the rapid development of ICT, regular modifications and amendments to the legislation and procedures should be provided.
- Following the Court of Justice decision of 8 April 2014, the Constitutional Court of Slovenia repealed the national law on 'traffic data retention'. Communication service providers are no longer obliged to keep data available to the competent authorities, which has significantly hampered detection, investigation, prosecution and legal assistance in cybercrime cases. A similar situation has been observed in a number of other Member States.
- SI-CERT provides solid expertise and an efficient contribution both to cyber security matters at national and European level and to cybercrime investigations, and merits particular attention.

- Slovenian practitioners devote a continued and remarkable energy to providing public information on, and preventing cybercrime (see in particular the excellent 'Spletno oko' hotline). However, as national authorities pointed out, the general level of awareness and understanding of this criminal phenomenon still needs to be increased throughout the country.
- As statistical systems may vary significantly from one competent entity to another (e.g. LEAs, the Prosecution Service, the courts and the private sector), it is rather difficult to get a general picture of the efficiency of the fight against cybercrime in Slovenia. This is an issue in many countries. However, considering the ratio between registered cybercrime cases and the total number of cases registered by the police services, there is a strong presumption that the detection of cybercrime requires further improvement.
- The Computer Investigation Centre set up in 2009 investigates some of the serious cases throughout the territory and provides computer forensics and professional assistance to other police services. Considering the size of the country, the existence of six regional computer investigation departments is noteworthy. At judicial level, cybercrime cases are dealt with by, on the one hand, the prosecutors acting in all prosecutorial offices and, on the other, by general courts.
- Where cooperation exists between the Slovenian police, in particular the Computer Investigation Centre, and Europol/EC3, it is active and successful. However, it is as limited as the police resources.
- Efforts are made at police force level to provide basic and/or advanced training to peers. However, in general, particular attention should be paid to the need to offer training to all competent practitioners, notably forensic experts on the one hand, and judges and prosecutors on the other.[1]

[1] The Slovenian authorities believe that with the support of the ISF (Internal Security Fund), specialist training in the area of information technologies will be carried out on the basis of a public tender in 2016 and 2017, while training courses also being planned for the period 2018 – 2020 as well. The training courses will be attended by all employees of the computer investigation units.

2 INTRODUCTION

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

The choice of cybercrime as the subject of 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, child sexual abuse/pornography online and online card fraud. It should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[3] (transposition date 18 December 2013) and Directive 2013/40/EU[4] on attacks against information systems (transposition date 4 September 2015) are particularly relevant in this context.

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

Moreover, the Council Conclusions on the EU Cybersecurity Strategy of June 2013[5] reiterate the objective of ratifying the Council of Europe Convention on Cybercrime (the Budapest Convention)[6] of 23 November 2001 as soon as possible, and emphasise in the preamble that 'the EU does not call for the creation of new international legal instruments for cyber issues'. This Convention is supplemented by a Protocol on xenophobia and racism committed through computer systems[7].

Experience from past evaluations shows that Member States will be in different positions regarding the implementation of relevant legal instruments, and the current process of evaluation 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 the fight against cybercrime, but also on the operational aspects in the Member States.

Therefore, in addition to cooperation with prosecution services, it will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from the given actors 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 victims of cybercrime.

[5] 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.

[6] CETS no 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.

[7] CETS no 189; opened for signature on 28 January 2003, entered into force on 1 March 2006.

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

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

The experts charged with undertaking the evaluation of Slovenia were Ms Patricia Nare Agostinho (Portugal), Mr Miroslav Tiza (Slovakia) and Mr Kuba Sękowski (Poland), together with Ms Claire Rocheteau from the General Secretariat of the Council. No observers from Eurojust, Europol or ENISA were present.

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 Slovenia between 11 and 13 May 2015, and on Slovenia's detailed replies to the evaluation questionnaire together with its detailed answers to subsequent follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National cyber security strategy

During the on-site visit it was indicated to the evaluation team that the current state of affairs in Slovenia presented the following main strengths and weaknesses:

- main strengths: the operational level of a cyber security system has been established; human resources with significant expertise are present at operational level, albeit underpowered; previous awareness-raising programmes (*Safe on the Internet*, SAFE.SI) have had good results; participation in joint international exercises has taken place;
- main weaknesses: the strategic level of a cyber security system is still missing; there is a lack of financial, human, material and technical resources; cooperation among key stakeholders is insufficient; the field of cyber security is not systematically regulated.

A draft 'National Cyber Security Strategy' was in public consultation from 6 to 31 March 2015. At the time of the on-site visit, the draft was to be sent for inter-ministerial coordination.

After the on-site visit the evaluation team was informed that the National Cyber Security Strategy was adopted by the Slovenian Government on 25 February 2016. The English version of the strategy is available at the following web link:

http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/pdf/Cyber_Security_Strategy_Slovenia.pdf

3.2 National priorities with regard to cybercrime

The National Cyber Security Strategy lists the following priorities:
- establishing the strategic level of the cyber security system, which includes the establishment of the National Cyber Security Authority;
- strengthening the operational level of the cyber security system;
- protection of critical infrastructure;
- encouraging the development and deployment of technology;
- participation in national and international cyber security exercises;
- implementation of awareness-raising programmes;
- education and training in the field of cyber security;
- combating cybercrime;
- international cooperation in the field of cyber security.

In terms of the prevention and combating of cybercrime, during the on-site visit the Slovenian authorities stressed the importance of law enforcement agencies, their effective organisation, international integration and professional competence. Therefore, the Strategy's main targets are to provide relevant education in the field of cybercrime and cyber security for police investigators and judicial bodies, to expand the capacities of the police in the field of digital forensics, and to continue to run public awareness-raising programmes.

Currently the national priority tasks are related to the strategic objectives and operational action plans of the EU, as the Slovenian police services have been actively participating in the EMPACT projects of CSE (child sexual exploitation), CF (card fraud) and CA (cyber attacks). All three fields are police priorities as part of the prevention, combating and investigation of cybercrime.

Chapter 5.3.5, 'Response to Cyber Threats and Misuse of Information Technologies and Systems', of the adopted Resolution on the National Security Strategy of the Republic of Slovenia mentions the fight against cybercrime, especially in the field of sexual exploitation of children on the internet.

3.3 Statistics on cybercrime

3.3.1 Main trends leading to cybercrime

According to the Slovenian authorities, greater prevalence of various electronic devices and more frequent use of various services on the internet generate new forms and ways of committing criminal offences. In recent years, more characteristics of cybercrime have been detected in Slovenia:

- organised gangs of perpetrators: while not too long ago most of these crimes were committed by individual perpetrators, perpetrators today are more frequently organised in criminal gangs where they divide roles;
- the objective of perpetrators: the objective of perpetrators is more and more frequently to acquire the details of users, which most frequently refers to usernames and passwords to access various online services (e.g. e-banking, social network profiles, e-mail, virtual money, etc.);
- purpose or motive of perpetrators: the main motive of most perpetrators of cybercrimes (especially in the fields of cyber attacks on information systems, internet fraud and abuse of payment cards via the internet) is financial benefit and unlawfully acquired profits;
- in view of the above, phishing scams targeting clients of Slovenian banks, abuse of payment cards in purchases via the internet, and infections with ransomware occur regularly.

Specific field of online child sexual exploitation

The Slovenian police have been training and equipping their staff for the investigation of cybercrime for many years. Through prevention activities (lectures, workshops at schools, awareness-raising campaigns, cooperation at conferences, seminars, etc.) the police give advice, warn of the dangers of the internet and promote safe usage of online services.

Besides typical crimes related to cybercrime, the police investigate other forms of crimes closely related to the intrusion of a child's privacy, e.g.:

- sexual assault on a person under 15 years of age (Article 173, Penal Code);
- enticement of persons under 15 years of age for sexual purposes (known as online child grooming) (Article 173a, Penal Code);
- presentation, manufacture, possession and distribution of pornographic material (Article 176, Penal Code).

These crimes infringe upon a child's sexual, physical and mental integrity and are considered a severe breach of privacy. Slovenia understands them as a reflection of various forms of violence against children.

In fact, these kinds of crimes are increasing due to an ever growing number of electronic devices providing access to the internet, and the increased usage of many internet services. New forms of crime are developing rapidly, new trends and modus operandi are emerging, and the police have had to adjust their methods and tactics, and also engage additional staff and properly train and equip them.

The reported online crimes against children are of great importance and are an investigation priority according to Slovenian legislation. Each investigation and approach depends on the circumstances of the particular case. The above-mentioned crimes against children are prosecuted *ex officio*, according to the Slovenian Penal Code (KZ-1) and the Criminal Procedure Act (ZKP). In certain legal situations the Police Tasks and Powers Act (ZNPPol), the Electronic Communications Act (ZEKom-1) and the Electronic Commerce Market Act (ZEPT) also apply.

On this occasion, the Slovenian authorities stressed that the national law enforcement agency disagrees with the use of the expression 'child pornography'. If pornography itself means films, images, literature, etc., portraying adults involved in explicit sexual activities or showing their genitalia, on a voluntary basis, and this kind of material is intended for the public, especially to arouse sexual excitement in the viewer (consumer), then the involvement of children in such activities cannot be considered as pornography, or termed 'child pornography' for that matter. The only possible way to discuss it is as sexual exploitation or sexual abuse of children, and consequently illegal material made by filming, picturing or recording criminal acts against the sexual integrity of children should be referred to as child sexual exploitation material (CSEM/CEM) or child sexual abuse material (CSAM/CAM). The term 'child pornography' and its many variations is mostly used by offenders in order to minimise the scope of the problem and the actual abuse. More on this topic can be found in the research on the importance of terminology in this field conducted as part of a separate project by the Slovenian Police – Criminal Police Directorate and co-authors.[8]

[8] Frangež, D., Klančnik, A. T., Ludvigsen, B. E., Veijalainen, M., Lewin, M., Konczyk, J., and Ruiz Perez, F., "The Importance of Terminology Related to Child Sexual Exploitation, Journal of Criminal Investigation and Criminology, vol. 66, no. 4, Ljubljana 2015, pp. 291-299.

Police activities in the child sexual exploitation (CSE) area focus on:

- operational resolution of CSE cases (concrete cases);
- international law enforcement cooperation (concrete cases, strategic issues, implementation of action plans);
- active cooperation in EU projects in order to deploy new workflows;
- suggestions for amendments to the relevant legislation based on new trends and modus operandi of offenders to increase child protection;
- educating and training internal professional audience (police officers, investigators),

as a relevant partner in inter-institutional cooperation at national level.

The main trends and modus operandi of offenders are, according to the Slovenian authorities:

Sexting: the act of sending sexually explicit messages, primarily between mobile phones, especially when self-made images are sent to the receiver. If the images contain a person below 18 years of age in a sexually explicit pose (naked, focus on genitalia, sexual act, etc.), then it is illegal to possess these kinds of images or to disseminate them to any third party.

Revenge porn: sexually explicit media that are publicly shared online without the consent of the pictured individual. Images are usually uploaded by ex-partners, ex-boyfriends or ex-girlfriends with the intention of shaming or embarrassing the pictured individual. The victims are mostly young women (18+). However, to the understanding of the evaluation team revenge porn is not a criminal offence under Slovenian law.

Online (child) grooming: this occurs when offenders form relationships with children and pretend to be their friend. According to their modus operandi, they commit this activity first by searching for and finding information about a potential victim. They then try to gauge the likelihood of the child reporting them, and to gather as much information as possible about the child's family, his/her experiences growing up, peer problems, hobbies, idols, and other things that children or young people are interested in, especially social networks. In their communication with the child they will often pretend to be younger or a different gender, give a false physical description, or send images of other people. When offenders realise it is 'safe enough', they will try to isolate their victim and may use flattery, promises of gifts, or even threats and intimidation to achieve some control over the victim. For these offenders is easy to find a child victim online, e.g. through chatrooms focused on young people's interests or via social networking websites.

Sexual extortion: a form of sexual exploitation that involves non-physical forms of coercion to extort sexual favours from the victim. Sexual extortion refers to a broad category of sexual exploitation in which abuse of power is the means of coercion, as well as to threats to release sexual images or sensitive personal information to the public (e.g. on the internet).

Live streaming of abuse for payment: refers to live distant child abuse (LDCA)[9];this is an act in which an internet user pays for access to specific websites to watch, via an electronic device, child sexual abuse committed by a child sexual offender in real time in a different location. Payments are made often via virtual financial instruments or mechanisms.

Other forms also include the production of CAM using a web-cam, naked 'selfies' or self-generated images of nakedness or sexual acts made by children/youths (victims), and cyber bullying among children.

[9] European Financial Coalition (2015). Strategic assessment analysing threats and trends of online child sexual exploitation, commercial live web streaming, p. 22. Europol, European Cybercrime Centre (EC3), 24.2.2015. Link: https://www.europol.europa.eu/sites/default/files/publications/efc_strategic_assessment_2014.pdf

3.3.2 Number of registered cases of cyber criminality

Judicial statistics are separate from those of the State Prosecutor's Offices and from those of the police. The private sector manages its own statistics (e.g. Spletno oko).

The police receive reports of criminal offences (*notitia criminis*) or establish the criminal offence through their own activities.

If there is reason to suspect that a criminal offence has been committed which gives rise to an *ex officio* prosecution, a file is opened in the police information system and information is entered. During the investigation and collection of evidence, all proceedings are documented and any information is entered in the file. A criminal complaint is filed by the police to the competent State Prosecutor's Office when they assess that they have collected sufficient evidence that a certain person is justifiably suspected of committing a criminal offence. After filing a criminal complaint with the competent State Prosecutor, the police close the file.

When the competent State Prosecutor's Office receives a criminal complaint filed by the police, the Office records it in its information system. This system has a different methodology for capturing data, which is why the information cannot be compared to police information.

Following the examination of the criminal complaint, the State Prosecutor's Office either dismisses the complaint or files it with the competent court, where it is entered in the court information system.

In terms of cybercrime, the police statistics reflect the number of complaints filed under the authority of the competent State Prosecutor's Office. In practice, most complaints are filed by the police. The number of registered cases of cybercrime was 1569 in 2013 and 1018 in 2014. Since the police in the Republic of Slovenia deals with approximately 90 000 crimes per year, the share of registered cybercrime appears to be 1.43%.

3.4 Domestic budget allocated to the prevention of and the fight against cybercrime, and support from EU funding

In the field of cyber security threat prevention, Slovenia runs two awareness-raising programmes:
- *Safe on the Internet*, which is also involved in the Cyber Security Month campaign, is operated by the National CERT and financed by the Ministry of Education, Science and Sport;
- 'SAFE.SI', which is operated by a consortium of organisations and financed by the European Commission (DG Connect) and the Ministry of Education, Science and Sport.

After the on-site visit the evaluation team was informed that these programmes are currently co-financed by the Ministry of Public Administration and not by the Ministry of Education, Science and Sport.

According to the budgetary funds allocated and their needs, the Slovenian police allocate certain funds annually to combat cybercrime. There is no budgetary item intended only for cybercrime. The Slovenian police have so far acquired funds to combat cybercrime from the co-financing project run by the European Anti-Fraud Office OLAF from the Hercules II programme. Based on the project, the purchase of computer equipment and training in digital forensics were co-financed.

3.5 Conclusions

- Slovenia's National Cybercrime Strategy was adopted on 25 February 2016. The goal of the Strategy is to improve inter alia the country's cyber security assurance system and the safety in the cyberspace.
- Different statistical systems are used within the police, the prosecution services, the judiciary and the private sector. There is no clear correlation between the data, which leads to some discrepancies in statistical figures relating to cybercrime. There is an issue regarding the different definitions of cybercrime used by each of these entities.
- Moreover, cybercrime figures entered in the various systems are very low, which may be due to the lack of a common clear definition of cybercrime, and may also raise the question of the efficiency of cybercrime detection in Slovenia.
- There are no budgetary funds specifically dedicated to combatting cybercrime in Slovenia, except for the police and when it comes to EU funding.

4 NATIONAL STRUCTURES

Criminal proceedings in the Republic of Slovenia are mixed proceedings characterised by two main stages, i.e. preliminary proceedings and main proceedings. Preliminary proceedings are divided into pre-trial proceedings and criminal proceedings.

The police are the authority responsible for the detection, prevention and investigation of criminal offences. The State Prosecutor's Offices guide the work of the police in pre-trial proceedings and are responsible for the prosecution of perpetrators of criminal offences.

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

The Office of the State Prosecutor General of the Republic of Slovenia is the highest-ranking prosecutor's office in the country, within which operate supreme and higher state prosecutors and also some state prosecutors of lower ranks assigned to the Office of the State Prosecutor General to perform demanding professional tasks.

The Office of the State Prosecutor General is organised into four departments: the criminal law department, the civil and administrative affairs department, the training and expert supervision department, and the expert information centre.

11 District State Prosecutor's Offices (*Celje, Koper, Kranj, Krško, Ljubljana, Maribor, Murska Sobota, Nova Gorica, Novo mesto, Ptuj, Slovenj Gradec*) perform tasks of the first instance authority. Their area of operation is linked to the eleven counties of the district courts. Some district prosecutor's offices have **external departments** (*Ljutomer, Velenje, Postojna, Sežana, Piran, Domžale, Trbovlje, Kočevje*).

A Specialised Prosecutor's Office of the Republic of Slovenia is responsible for the prosecution of offenders in the fields of traditional organised and economic crime, terrorism, corruption, and other crimes where detection and prosecution require special organisation and competence across the entire national territory.

A department for investigating and prosecuting officials with special powers (special section) acts as an independent internal organisational unit in a specialised Prosecutor's Office of the Republic of Slovenia. The special section has exclusive territorial and subject-matter jurisdiction to deal with criminal offences committed by an official.

Within the general function of filing and representing criminal charges, a state prosecutor is to perform all the procedural acts of an authorised prosecutor, provide guidance to the police and other competent authorities, apply the deferred prosecution and settlement procedure and perform other tasks in accordance with the act regulating criminal procedures. **In short, cybercrime offences are dealt with by the prosecutors acting in all prosecutorial institutions, not only in the Specialised State Prosecutor's Office.**

Cybercrime offences are dealt with by general courts. The evaluation team was not able to interview judges during the visit but it was clearly stated by other stakeholders that judges generally lack awareness of and basic knowledge of how to deal with cybercrime.

4.1.2 Capacity and obstacles to successful prosecution

Capacity. With the adoption of the National Cyber Security Strategy, the Government of the Republic of Slovenia would like to improve its cyber security system. The current draft of the strategy plans the establishment of a National Cyber Security Authority and Government CERT (SIGOV-CERT), which will both upgrade the capacity for cybercrime investigation. The newly established National Cyber Security Authority will coordinate all the resources in this field (existing and new CERTs, the police, some Ministries) to ensure a safe cyber space. One of the important tasks in the context of the cyber security strategy is the provision of training for the police and judicial authorities working in the field of cybercrime. In the past five years, the police have monitored the increasing problem of cybercrime and upgraded their capacity through organisational measures, additional staffing and material-technical resources.

Obstacles. The performance of cybercrime investigation was affected by a decision of the Constitutional Court of the Republic of Slovenia in 2014. In the constitutional review procedure instigated on the request of the Information Commissioner, the Constitutional Court decided on 26 September 2013 to suspend the constitutional review procedure regarding Articles 162 to 169 of the Electronic Communications Act, pending a decision by the Court of Justice of the European Union in the cases of *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (hereinafter referred to as 'C-293/12' and 'C-594/12'). In the aforementioned cases, the Court of Justice of the European Union declared the Data Retention Directive to be invalid *ab initio* in its judgment of 8 April 2014.

Thus it assessed that, by adopting this Directive, the legislator of the European Union exceeded the boundaries required by the principle of proportionality, taking into account Articles 7 and 8 and the first paragraph of Article 52 of the Charter of Fundamental Rights of the European Union. Subsequently, the Constitutional Court of the Republic of Slovenia issued Decision No U-I-65/13 of 3 July 2014, which fully repealed the provisions of Articles 162 to 169 of the ZEKom-1 stipulating mandatory and long-term retention of traffic data (14 and 8 months respectively). In addition to repealing the aforementioned Articles, the constitutional decision ordered the operators to destroy all the data kept on the basis of the repealed legislation immediately after the publication of the decision in the Official Gazette of the Republic of Slovenia.

Due to the aforementioned constitutional decision, the police could no longer acquire traffic data on the basis of the repealed provisions of the ZEKom-1, but only on the basis of Article 149b of the ZKP. On the basis of the aforementioned provisions, operators only submit traffic data kept in their bases for so-called commercial purposes (e.g. to calculate a service pending its payment) for a period of three months or, in the case of non-payment, no longer than the expiry of the limitation period.

4.2 Law enforcement authorities

The Slovenian police

In Slovenia police perform their tasks and exercise their powers according to the provisions of the Police Tasks and Powers Act (*Zakon o nalogah in pooblastilih policije, cited as the ZNPPol*), in order to ensure basic police duties, which include the provision of security for individual people and the community, respect of human rights and fundamental freedoms and enhancement of the rule of law (Article 1(2)).

The tasks of the police deriving from their basic duties are as follows:

- to protect people's lives, personal safety and property;
- to prevent, detect and investigate criminal and minor offences, to detect and apprehend perpetrators of criminal and minor offences and other wanted or missing persons and to hand them over to the competent authorities, and to collect evidence and investigate circumstances that are important for the identification of material gain from the proceeds of criminal and minor offences;
- to maintain public order;
- to supervise and direct traffic on public roads and on unclassified roads currently in use for traffic;
- to conduct state border controls;
- to perform tasks in connection with the movement and residence of aliens;
- to protect particular persons, premises, buildings and the environs of such buildings and, unless otherwise provided by law, to protect particular jobs and classified information of public authorities;
- to perform tasks in the event of natural and other disasters;
- to carry out other tasks set out in the ZNPPol and other regulations according to the law.

Computer Investigation Centre and Departments

The police encompasses the organisational unit of the Computer Investigation Centre, which operates within the Criminal Police Directorate at the General Police Directorate, and regional computer investigation departments which operate in six out of eight Criminal Police Directorates in Koper, Ljubljana, Celje, Maribor, Kranj and Novo Mesto.

In the Republic of Slovenia, the police are competent to discover, prevent and investigate criminal offences related to cybercrime and have been operating in this field since 1999.

In 2009, the Computer Investigation Centre was established at the Criminal Police Directorate within the General Police Directorate. It has departments in individual police directorates which employ over sixty criminal police officers with a knowledge of IT and computer sciences. The work of the Computer Investigation Centre and the departments within the criminal police directorates cover three areas:

- investigation of cybercrimes (abuse of personal data, violation of material copyright, attacks on information systems, breaking into business information systems, acquisition of instruments to commit a criminal offence);
- protection and investigation of confiscated electronic devices and data (computer forensics);
- professional assistance in other fields of crime (regarding the criminal offences of recording sexual abuse of children, internet fraud, racial intolerance on the internet, tax evasion, corruption, abuse of e-banking, etc.).

Combating cybercrime requires a major financial and human resources input from law enforcement authorities. Therefore, ways must be sought to improve the exchange of specific knowledge, methodologies and work systems for the law enforcement authorities in the field of cybercrime and computer forensics. Cooperation between the private and public sector is very important. Combating cybercrime is very complex, which means that law enforcement authorities cannot successfully fight such crime without the cooperation of international institutions, the private sector and the general public.

The main obstacles are the data retention and slow operation of the institute of international legal aid.

4.3 Other authorities/institutions/public-private partnerships

In addition to the police and the State Prosecutor's Office, the following organisations also deal with preventing and combating cybercrime:

- the national organisation SI-CERT, which is part of the *Arnes* Public Institute and provides great support in cybercrime investigation through the expertise of its employees and its links with similar international organisations, which facilitate international connections and data exchange.
- the European Cybercrime Centre, which began operating within Europol in January 2013 and which provides better operational support to combat cross-border crimes in the EU, specialised strategic assessments and endangerment assessments, more focused training, and research and development to promote the development of special tools to combat cybercrime.
- the 'Safer Internet Centre SAFE-SI' project, which combines three components:
    - raising awareness of safer use of the internet and new technologies;
    - helpline for young people and their parents who experience internet-related issues;
    - ***Spletno oko,*** a point of contact for the anonymous reporting of illegal online content (recordings of sexual abuse of children and hate speech).

The activities of the SAFE-SI are aimed at four target groups: children, young people, parents and professionals (teachers, social workers, child care workers).

The objective of the project is to attain in Slovenia a high level of awareness of the aforementioned topics among the target populations by regularly providing verified information and advice regarding safe use of new technologies.

In addition to national and international investigation organisations, there are also private information security companies in the Republic of Slovenia which carry out analyses and provide cyber-related risk management.

Public-private partnership in the prevention of and fight against cybercrime is present in Slovenia as cooperation within different conferences on topical issues relating to cybercrime. Cooperation takes place in individual cases in the form of information exchanges (e.g. on current attacks on information systems), the public information system, operative meetings, joint preventive measures and similar. The Slovenian authorities stated that such partnerships and cooperation should be reinforced. At the same time, they acknowledged that there is no dedicated funding allocated to the police for enhancing cooperation with the private sector.

4.4. Cooperation and coordination at national level

4.4.1 Legal or policy obligations

Currently, the Republic of Slovenia does not have a multidisciplinary mechanism to respond to a serious cyber attack.

The National Cyber Security Strategy, as already noted above, envisages the establishment of a national body in charge of cyber security which will establish a strategic level for the provision of cyber security: this body is expected to deal comprehensively with issues from all areas of cyber security. Coordination of activities at lower levels of the system will also be implemented through the national body. It will also represent a point of contact for international cooperation in this field.

According to the first paragraph of Article 81 of ZEKom-1, operators must, immediately upon detection, notify the Agency for Communication Networks and Services of any breach of security or integrity that has had a significant impact on the operation of public communications networks or the provision of public communications services. Once a year, the Agency then informs ENISA of the cyber security incidents reported by operators during the year. The Agency also notifies ENISA when cyber security incidents of larger proportions occur. Additionally, according to Article 159 of ZEKom-1, in cases of violation of personal data, the public communications service provider must immediately inform the Agency.

Cooperation between law enforcement authorities and the private sector is only regulated under the provisions of various laws which govern and refer to the data and procedures related to cybercrime (mainly the Electronic Communication Act and the Law on Electronic Commerce and Electronic Signature). In cases where the private sector or its customers are the injured party, cooperation with law enforcement authorities is mostly good, since they take care of the preservation of evidence, its interpretation and its delivery to the law enforcement authorities. The cooperation of the private sector is also relatively good in cases when, for instance, their information system only stores the date or evidence related to the criminal offence. Such cooperation with the private sector should be strengthened and improved in Slovenia and is defined as one of the main goals in the national strategy for cyber security.

Financial institutions (banks, processing centres...) collect and store data on transactions, video surveillance, etc. according to their rules. If it is established that abuse or criminal offences related to the abuse of non-cash means of payment occurred, they report it to the police. The police acquire all available information from the private sector during the pre-trial procedure; the private sector, in addition to providing this information, assists the police in clarifying all the circumstances related to the criminal offences. The success of the investigations depends on the mutual cooperation between the police, the banks and the other financial institutions which execute payment transactions in the territory of the Republic of Slovenia, as well as the processing centres and other entities which provide services for the latter.

The police and the Bank Association of Slovenia ('ZBS') therefore adopted a Protocol. The Protocol includes the general principles of mutual cooperation and provides a basis for its improvement, and emphasises the determination of the measures taken by the banks and the police in cases of abuse of non-cash means of payment. The Protocol also includes the prompt mutual notification of the methods used to commit the offences, and any new developments and preventive measures in this field.

Articles 145 and 146 of the Criminal Procedure Act are used for the reporting and prosecution of the criminal offences.

In practice, the Slovenian criminal police cooperate with the ZBS and in this connection a police representative has already given several lectures as part of training courses organised by the ZBS. The police and the ZBS also organise panel discussions, which are attended by representatives of all the banks and processing centres, who are also contact persons in cases of abuse of non-cash means of payment. These panel discussions allow participants to exchange good and not-so-good practices and experiences.

The police and the ZBS have concluded a Protocol to ensure effective cooperation between the police and the private sector in cases of abuse of non-cash means of payment. The Protocol puts emphasis on cooperation and measures taken by banks and the police in cases of abuse of non-cash means of payment. The Protocol also covers the exchange of up-to-date information about new payment tools, services, other new developments and possible preventive measures.

The details of contact persons who cooperate and exchange information in cases of abuse of non-cash means of payment are indicated in the Protocol. The obligations of the police and of banks as regards the detection and handling of such criminal offences are also defined in the Protocol.

4.4.2 Resources allocated to improve cooperation

As part of the EU FACETRACE project, which aims to improve the facial recognition of perpetrators of criminal acts, the Slovenian criminal police have acquired funds, software and hardware which also serve for investigating criminal acts related to the abuse of non-cash means of payment.

When investigating payment card abuse (including cases of physical payment card abuse), the police use various investigative and technical methods, such as inspecting the location of criminal acts, securing devices used to copy information from the magnetic strips on payment cards (skimming), looking for papillary and biological traces on devices, carrying out technical inspections of devices and securing data from devices. The Slovenian police focus on investigating devices, as conclusions and data acquired from such devices can significantly contribute to clarifying a criminal act. By using the currently available software and hardware, the police are capable of acquiring data from seized skimming devices which is important for investigations of this kind. However, since the technology used in skimming devices is constantly evolving, it would without a doubt be sensible to upgrade the equipment used by forensic investigators.

4.5 Conclusions

- In Slovenia, cybercrime is dealt with by generalist prosecutors and criminal courts; there are no judicial authorities specialised in this area. At police level, there is a Computer Investigation Centre which operates nationally (with competence to carry out investigations throughout the national territory), and six computer investigation departments operating at regional level.

- The performance of cybercrime investigation was affected by a decision of the Constitutional Court of the Republic of Slovenia in 2014, which, in addition to repealing the legal basis for data retention, also ordered operators to destroy all the data kept on the basis of the repealed legislation. As a result, the police can only access traffic data kept by an operator for its own business purposes.
- The National Cyber Security Strategy provides for the establishment of central coordination of the national cyber security assurance system at the strategic level to ensure cyber security in the country at lower levels. This body will represent a single point of contact for international cooperation and its functions will be determined by the Government of the Republic of Slovenia. At the operational level of cyber security assurance, SI-CERT will operate with its capabilities at the national level, the Ministry of Defence in the field of defence and protection against natural and other disasters, the police in ensuring cyber security in the context of public safety and the fight against cyber crime, SOVA in counter intelligence, and the emergent SIGOV-CERT in public administration.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on Cybercrime

Slovenia is a party to the Council of Europe Convention on Cybercrime, which was signed on 24 July 2002 and ratified on 8 September 2004, and which entered into force on 1 January 2005. The Convention was published in the Official Gazette of the Republic of Slovenia – International Treaties, No 17/2004, as an Act ratifying the Convention on Cybercrime and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

5.1.2 Description of national legislation

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

At the time of the on-site visit Directive 2013/40/EU on attacks against information systems (transposition date 4 September 2015) has not yet been implemented into Slovenian legislation. At most, certain sections of the Directive are in the process of being implemented through Slovenia's participation in the Cyber Attack group of the EMPACT project (Operational Action 5.1 in Article 13 of Directive 2013/40/EU).

After the on-site visit the evaluation team was informed that the directive has been implemented into the Slovenian legislation. Implementation was officially notified on 12 August 2016.

Acts unique to information systems, in particular those related to cyber attacks (illegal access to information systems, illegal system interference, illegal data interference, illegal interception of computer data, misuse of devices):

The title and relevant provision Minimum/maximum penalties	Penal Code (Official Gazette RS, no. 50/12 – Officially consolidated version)
• Illegal access to information system (Article 221/1), (Article 237/1) • Illegal system interference (Article 221/2), (Article 237/1) • Illegal data interference (Article 221/2), (Article 237/1) • Illegal interception of computer data (Article 221/1), (Article 237/1)	Attack on Information Systems Article 221 (*1) Whoever without authorisation enters or breaks into an information system, or illegally intercepts data during a non-public transmission into or from the information system, shall be sentenced to* ***imprisonment for not more than one year****.* *(2) Whoever makes an illegal use of data in an information system, or changes, copies, transmits, destroys, or illegally imports data in an information system, or obstructs data transmission or information system operation, shall be sentenced to* ***imprisonment for not more than two years****.* *(3) Any attempt to commit such an offence referred to in the preceding paragraph shall be punishable.* *(4) If the damages incurred by the committing of the offence under paragraph 2 of this Article are considerable, the perpetrator shall be sentenced to* ***imprisonment for not less than three months and not more than five years****.* Information system abuse Article 237 (*1) Whoever, in the performance of commercial operations, illegally enters or breaks into an information system, or*

	illegally uses it by applying, altering, copying, transmitting or destroying, or inserts into the information system any data, or obstructs data transmission or information system operation, or illegally intercepts data during a non-public transmission into or from the information system in order to either procure unlawful proceeds for himself or a third person or cause damage to the property of another, shall be ***sentenced to up to three years in prison***. *(2) If the offence under the above paragraph has resulted in a large property benefit or a large loss of property and if the perpetrator intended to cause such loss of property or to gain such property benefit, he shall be sentenced to* ***imprisonment for not more than five years.*** Meaning of Terms of the Penal Code Article 99 …. (*11) Pursuant to this Code, economic activity or commercial operation shall include:* *1) implementation, governance, decision-making, representation, management and supervision within the framework of the activity referred to in paragraph 10 of this Article;* *2) management of immovable and movable property, funds, income, claims, capital assets, other forms of financial assets, and other assets of legal entities governed by public or private law, the use of these assets and control over them.*

• Misuse of devices – production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools (Article 306/3)	Penal Code (Official Gazette RS, no. 50/12 – Officially consolidated version) Manufacture and Acquisition of Weapons and Instruments Intended for the Commission of Criminal Offence Article 306 (*1) Whoever manufactures or acquires or keeps weapons, explosive materials or instruments for their manufacture, or poisons which he knows to be intended for the commission of a criminal offence, or whoever provides another person with access to the same, shall be sentenced to* ***imprisonment for not more than three years****.* *(2) Whoever manufactures or offers to another, a false key, lock-pick or any other instrument of burglary, if he knows it to be intended for the commission of a criminal offence, shall be* ***sentenced to imprisonment for not more than one year****.* *(3) The* ***punishment under the above paragraph*** *shall be imposed on whoever possesses, manufactures, sales, puts to use, imports, exports, or makes available in any other manner, with the intention of committing a criminal offence, instruments intended for the breaking or illegal entry into the information system.*

The definition used	As unauthorized entry into the information system would be considered if the offender with a method of social engineering acquires username and password of another person and directly logs into a server, or if he enters into the system through the use of technical data or tools that are intended for the management and maintenance of the system without authority to enter into a substantive part of the system or authority to access the data. It is clear from the general provisions of the Penal Code that this offence can only be intentional. It can not be done by random connection to an unprotected wireless network (Wi-Fi), which is unwanted because it happened only because of the automatic logon. For unauthorised break into the information system the perpetrator would use different tools, such as malicious software or different approaches to exploit the weaknesses of the information system to break and into built-in settings or obstacles of the server.
Intent/recklessness	Offences provided in Articles 221, 237 and 306 of the Penal Code have to be committed intentionally. According to the Article 27 of the Penal Code the perpetrator shall be punished for the criminal offence committed through negligence only if the law so determines.

Aggravating/mitigating factors	Penal Code provides in its general provisions, Article 49 general rules on sentencing: General Rules on Sentencing Article 49 *(1) The perpetrator shall be sentenced for a criminal offence within the limits of the statutory terms provided for such an offence and with respect to the gravity of his offence and his guilt.* *(2) In fixing the sentence, the court shall consider all circumstances, which have an influence on the grading of the sentence (mitigating and aggravating circumstances), in particular: the degree of the perpetrator's guilt; the motives, for which the offence was committed; the intensity of the danger or injury caused to the property protected by law; the circumstances, in which the offence was committed; the perpetrator's past behaviour; his personal and pecuniary circumstances; his conduct after the committing of the offence and especially, whether he recovered the damages caused by the committing of the criminal offence; and other circumstances referring to the personality of the perpetrator and to the expected effect of the punishment on the future life of the perpetrator in the social environment.* *(3) In fixing the sentence of a perpetrator who committed a criminal offence after he had already been convicted or had served his sentence, or after the implementation of his sentence had been barred by time, or after his sentence has been remitted (recidivism), the court shall pay particular attention to whether the earlier offence is of the same type as the new one, whether both offences were committed for the same motive and to the time, which has lapsed since the*

	former conviction or since the serving, withdrawing, remitting or barring of the sentence. Aggravating factors: Penal Code in Article 41 provides a general provision for offences committed within criminal organisation. Liability of Members and Leaders of Criminal Organisation Article 41 *(1) A member (hereinafter: the member) of a criminal organisation with at least three persons shall be punished with a severer sentence prescribed for a criminal offence committed within a criminal organisation if he commits the criminal offence to implement the criminal organisation's plan in association with at least one member as an accessory or accomplice.* *(2) In the case referred to in paragraph 1 of this Article, the leader of the criminal organisation, who led the implementation of the criminal plan or had at his disposal illegally gained property benefits at the time of committing the criminal offence based on the criminal plan, notwithstanding whether he participated at its implementation directly as the perpetrator or accessory pursuant to Articles 20 or 37 and 38 of this Penal Code, shall be punished the same as the perpetrator.* Penal Code in Article 294 also provides liability for participation in a criminal organisation as a separate criminal offence. Article 294 provides for a mitigating factor in the paragraph 3.

	Criminal Organisation Article 294 *(1) Whoever participates in a criminal organisation which has the purpose of committing criminal offences, for which a punishment by imprisonment of more than three years, or a life sentence may be imposed, shall be punished by imprisonment of three months up to five years.* *(2) Whoever establishes or leads an organisation as referred to in the preceding paragraph, shall be punished by imprisonment of six months up to eight years.* *(3) A perpetrator of a criminal offence from the preceding paragraphs who prevents further commission of these offences or discloses information which has a bearing on the investigation and proving of criminal offences that have already been committed, may have his punishment for these offences mitigated, in accordance with Article 51 of this Penal Code.*
Multiple crimes/recidivism	Penal Code provides in its general provisions, Article 49 general rules on sentencing: General Rules on Sentencing Article 49 *(1) The perpetrator shall be sentenced for a criminal offence within the limits of the statutory terms provided for such an offence and with respect to the gravity of his offence and his guilt.* *(2) In fixing the sentence, the court shall consider all circumstances, which have an influence on the grading of the sentence (mitigating and aggravating circumstances), in particular: the degree of the perpetrator's guilt; the motives, for which the offence was committed; the intensity of the*

	danger or injury caused to the property protected by law; the circumstances, in which the offence was committed; the perpetrator's past behaviour; his personal and pecuniary circumstances; his conduct after the committing of the offence and especially, whether he recovered the damages caused by the committing of the criminal offence; and other circumstances referring to the personality of the perpetrator and to the expected effect of the punishment on the future life of the perpetrator in the social environment. *(3) In fixing the sentence of a perpetrator who committed a criminal offence after he had already been convicted or had served his sentence, or after the implementation of his sentence had been barred by time, or after his sentence has been remitted (recidivism), the court shall pay particular attention to whether the earlier offence is of the same type as the new one, whether both offences were committed for the same motive and to the time, which has lapsed since the former conviction or since the serving, withdrawing, remitting or barring of the sentence.*
Incitement, aiding and abetting, and attempt	The provisions on incitement, aiding and abetting and attempt are provided in general provisions of the Penal Code: <u>Attempt</u> Attempt Article 34 *(1) Any person, who intentionally initiated a criminal offence but did not complete it, shall be punished for the criminal attempt, provided that such an attempt involved a criminal offence, for which the sentence of three years' imprisonment or a heavier sentence may be imposed under the statute; attempts involving any other criminal offences shall be punishable only when so expressly stipulated by the*

	statute. *(2) Against the perpetrator, who attempted to commit a criminal offence, the sentence shall be applied within the limits prescribed for such an offence or it may be reduced.* <u>Incitement, aiding and abetting</u> Participant Article 36a *The provisions of this Code that are applicable to the perpetrator shall also apply to a participant who solicits or supports a criminal offence, unless otherwise provided by the law.* Criminal Solicitation Article 37 (*1) Any person who intentionally solicits another person to commit a criminal offence shall be punished as if he himself had committed it.* *(2) Any person who intentionally solicits another person to commit a criminal offence, for which the sentence of three years' imprisonment or a heavier sentence may be imposed under the statute, shall be punished for the criminal attempt even if the committing of such an offence had never been attempted.* Criminal Support Article 38 (*1) Any person who intentionally supports another person in*

	the committing of a criminal offence shall be punished as if he himself had committed it, or his sentence shall be reduced, as the case may be. *(2) Support in the committing of a criminal offence shall be deemed to be constituted, in the main, by the following: counselling or instructing the perpetrator, on how to carry out the criminal offence; providing the perpetrator with instruments of criminal offence or removing the obstacles for the committing of criminal offence; a priori promises to conceal the perpetrator's criminal offence or any traces thereof; instruments of the criminal offence or objects gained through the committing of criminal offence.* Punishability of Those Soliciting or Supporting a Criminal Attempt Article 39 *If the perpetration of a criminal offence falls short of the intended consequence, those soliciting (hereinafter, the instigator) or supporting (hereinafter, the aide) the criminal attempt shall be punished according to the prescriptions that apply to the criminal attempt.* Limits of Punishability of Accomplices Article 40 (*1) The perpetrator, the instigator and the aide shall be punished for criminal offences within the limits of their intent.* *(2) If the instigator or the aide voluntarily prevented the intended criminal offence from being accomplished, his*

	sentence may be withdrawn. *(3) Personal relations, attributes and circumstances, on the basis of which the guilt or Punishability are excluded by law or sentence remitted, reduced or extended, shall be taken into consideration only with respect to the accomplice (hereinafter, the accomplice), by whom such relations, attributes and circumstances were determined.*

Content-related acts, in particular those related to child sexual abuse online and child pornography (Computer-related production, distribution or possession of child pornography and Computer-related solicitation or "grooming" of children):

The title and relevant provision Minimum/maximum penalties	Penal Code (Official Gazette RS, no. 50/12 – Officially consolidated version) Sexual Assault on a Person below Fifteen Years of Age Article 173 (*(1) Whoever has sexual intercourse or performs any lewd act with a person of the same or opposite sex under the age of fifteen years shall be sentenced to* ***imprisonment for not less than three and not more than eight years***. *(2) Whoever commits the offence under the preceding paragraph against the defenceless person under the age of fifteen or by threatening him/her with imminent attack on life or limb or, by acting in this way, commits the aforementioned offence against another person, shall be sentenced to* ***imprisonment for not less than five and not more than fifteen years***. *(3) A teacher, educator, guardian, adoptive parent, parent, priest, doctor or any other person who through the abuse of his position has sexual intercourse or performs any lewd act with a person under the age of fifteen and whom he is entrusted to teach, educate, give medical treatment, protect or care for shall be sentenced to* ***imprisonment for not less than three and not more than ten years***. *(4) Whoever, under circumstances under paragraphs 1, 2 or 3 of this Article, violates the sexual integrity of the person under the age of fifteen years shall be sentenced to* ***imprisonment for not more than five years***. *(5) The act referred to in paragraph 1 of this Article shall not be illegal if it is committed with a person of comparable*
• Computer – related solicitation or "grooming" of children (Article 173a, Article 173) • Computer-related production, distribution or possession of child pornography (Article 176)	

	age and if it corresponds to the mental and physical maturity of this person. Solicitation of persons under fifteen years of age for sexual purposes Article 173a *(1) Whoever proposes, by using information and communication technologies, a meeting to a person under fifteen years of age for the purpose of committing a criminal offence referred to in paragraph 1 of Article 173 or producing pictures or audio-visual or other items of a pornographic or other sexual nature, and where this proposal has been followed by material acts leading to such a meeting, shall be* ***sentenced to up to one year in prison****.* *(2) The act referred to in the preceding paragraph shall not be illegal if it is committed for the purposes of committing the act referred to in paragraph 1 of Article 173 and under conditions referred to in paragraph 5 of Article 173 of this Code.* Presentation, Manufacture, Possession and Distribution of Pornographic Material Article 176 *(1) Whoever sells, presents or publicly exhibits documents, pictures or audio-visual or other items of a pornographic nature to a person under fifteen years of age, enables them to gain access to these in any other way or presents them a pornographic or other sexual performance shall be given a* ***fine or a prison sentence of up to two years****.* *(2) Whoever, by force, threat, deception, exceeding or abusing powers, recruitment or solicitation, or for purpose of exploitation, instructs, obtains or encourages a minor to*

	produce pictures, audio-visuals or other items of a pornographic or other sexual nature, or uses them in a pornographic or other sexual performance or is knowingly present at such performance, shall be sentenced to ***between six months and eight years in prison****.* *(3) The* ***same punishment as referred to in the preceding paragraph*** *shall be imposed on whoever, for himself or any third person, produces, distributes, sells, imports, exports pornographic or other sexual material depicting minors or their realistic images, or supplies it in any other way, or possesses such material, or obtains access to such material by means of information and communication technologies, or discloses the identity of a minor in such material.* *(4) If an offence from paragraphs 2 or 3 of this Article was committed within a criminal organisation for the committing of such criminal offences, the perpetrator shall be given a* ***prison sentence of between one and eight years****.* *(5) Pornographic or other sexual material from paragraphs 2, 3 or 4 of this Article shall be seized or its use appropriately disabled.*
Intent/recklessness	Offences provided in Articles 173, 173a and 176 of the Penal Code have to be committed intentionally. According to the Article 27 of the Penal Code the perpetrator shall be punished for the criminal offence committed through negligence only if the law so determines.
Aggravating/mitigating factors	Penal Code provides in its general provisions, Article 49 general rules on sentencing: General Rules on Sentencing Article 49 *(1) The perpetrator shall be sentenced for a criminal*

	offence within the limits of the statutory terms provided for such an offence and with respect to the gravity of his offence and his guilt. *(2) In fixing the sentence, the court shall consider all circumstances, which have an influence on the grading of the sentence (mitigating and aggravating circumstances), in particular: the degree of the perpetrator's guilt; the motives, for which the offence was committed; the intensity of the danger or injury caused to the property protected by law; the circumstances, in which the offence was committed; the perpetrator's past behaviour; his personal and pecuniary circumstances; his conduct after the committing of the offence and especially, whether he recovered the damages caused by the committing of the criminal offence; and other circumstances referring to the personality of the perpetrator and to the expected effect of the punishment on the future life of the perpetrator in the social environment.* *(3) In fixing the sentence of a perpetrator who committed a criminal offence after he had already been convicted or had served his sentence, or after the implementation of his sentence had been barred by time, or after his sentence has been remitted (recidivism), the court shall pay particular attention to whether the earlier offence is of the same type as the new one, whether both offences were committed for the same motive and to the time, which has lapsed since the former conviction or since the serving, withdrawing, remitting or barring of the sentence.* Aggravating factors: Penal Code in Article 41 provides a general provision for offences committed within criminal organisation. Liability of Members and Leaders of Criminal Organisation

	Article 41 (*1) A member (hereinafter: the member) of a criminal organisation with at least three persons shall be punished with a severer sentence prescribed for a criminal offence committed within a criminal organisation if he commits the criminal offence to implement the criminal organisation's plan in association with at least one member as an accessory or accomplice.* *(2) In the case referred to in paragraph 1 of this Article, the leader of the criminal organisation, who led the implementation of the criminal plan or had at his disposal illegally gained property benefits at the time of committing the criminal offence based on the criminal plan, notwithstanding whether he participated at its implementation directly as the perpetrator or accessory pursuant to Articles 20 or 37 and 38 of this Penal Code, shall be punished the same as the perpetrator.* Penal Code in Article 294 also provides liability for participation in a criminal organisation as a separate criminal offence. Article 294 provides for a mitigating factor in the paragraph 3. Criminal Organisation Article 294 *(1) Whoever participates in a criminal organisation which has the purpose of committing criminal offences, for which a punishment by imprisonment of more than three years, or a life sentence may be imposed, shall be punished by imprisonment of three months up to five years.*

	(2) Whoever establishes or leads an organisation as referred to in the preceding paragraph, shall be punished by imprisonment of six months up to eight years. *(3) A perpetrator of a criminal offence from the preceding paragraphs who prevents further commission of these offences or discloses information which has a bearing on the investigation and proving of criminal offences that have already been committed, may have his punishment for these offences mitigated, in accordance with Article 51 of this Penal Code.*
Multiple crimes/recidivism	Penal Code provides in its general provisions, Article 49 general rules on sentencing: General Rules on Sentencing Article 49 (*1) The perpetrator shall be sentenced for a criminal offence within the limits of the statutory terms provided for such an offence and with respect to the gravity of his offence and his guilt.* *(2) In fixing the sentence, the court shall consider all circumstances, which have an influence on the grading of the sentence (mitigating and aggravating circumstances), in particular: the degree of the perpetrator's guilt; the motives, for which the offence was committed; the intensity of the danger or injury caused to the property protected by law; the circumstances, in which the offence was committed; the perpetrator's past behaviour; his personal and pecuniary circumstances; his conduct after the committing of the offence and especially, whether he recovered the damages caused by the committing of the criminal offence; and other circumstances referring to the personality of the perpetrator and to the expected effect of the punishment on the future*

	life of the perpetrator in the social environment. *(3) In fixing the sentence of a perpetrator who committed a criminal offence after he had already been convicted or had served his sentence, or after the implementation of his sentence had been barred by time, or after his sentence has been remitted (recidivism), the court shall pay particular attention to whether the earlier offence is of the same type as the new one, whether both offences were committed for the same motive and to the time, which has lapsed since the former conviction or since the serving, withdrawing, remitting or barring of the sentence.*
Incitement, aiding and abetting, and attempt	The provisions on incitement, aiding and abetting and attempt are provided in general provisions of the Penal Code: <u>Attempt</u> Attempt Article 34 (*1) Any person, who intentionally initiated a criminal offence but did not complete it, shall be punished for the criminal attempt, provided that such an attempt involved a criminal offence, for which the sentence of three years' imprisonment or a heavier sentence may be imposed under the statute; attempts involving any other criminal offences shall be punishable only when so expressly stipulated by the statute.* *(2) Against the perpetrator, who attempted to commit a criminal offence, the sentence shall be applied within the limits prescribed for such an offence or it may be reduced.* <u>Incitement, aiding and abetting</u>

	Participant Article 36a *The provisions of this Code that are applicable to the perpetrator shall also apply to a participant who solicits or supports a criminal offence, unless otherwise provided by the law.* Criminal Solicitation Article 37 (*1) Any person who intentionally solicits another person to commit a criminal offence shall be punished as if he himself had committed it.* *(2) Any person who intentionally solicits another person to commit a criminal offence, for which the sentence of three years' imprisonment or a heavier sentence may be imposed under the statute, shall be punished for the criminal attempt even if the committing of such an offence had never been attempted*. Criminal Support Article 38 *(1) Any person who intentionally supports another person in the committing of a criminal offence shall be punished as if he himself had committed it, or his sentence shall be reduced, as the case may be.* *(2) Support in the committing of a criminal offence shall be deemed to be constituted, in the main, by the following: counselling or instructing the perpetrator, on how to carry out the criminal offence; providing the perpetrator with instruments of criminal offence or removing the obstacles*

	for the committing of criminal offence; a priori promises to conceal the perpetrator's criminal offence or any traces thereof; instruments of the criminal offence or objects gained through the committing of criminal offence. Punishability of Those Soliciting or Supporting a Criminal Attempt Article 39 *If the perpetration of a criminal offence falls short of the intended consequence, those soliciting (hereinafter, the instigator) or supporting (hereinafter, the aide) the criminal attempt shall be punished according to the prescriptions that apply to the criminal attempt.* Limits of Punishability of Accomplices Article 40 *(1) The perpetrator, the instigator and the aide shall be punished for criminal offences within the limits of their intent.* *(2) If the instigator or the aide voluntarily prevented the intended criminal offence from being accomplished, his sentence may be withdrawn.* *(3) Personal relations, attributes and circumstances, on the basis of which the guilt or Punishability are excluded by law or sentence remitted, reduced or extended, shall be taken into consideration only with respect to the accomplice (hereinafter, the accomplice), by whom such relations, attributes and circumstances were determined.*

Acts where computer/IT systems were involved as tools or target, in particular online card fraud (Computer-related fraud or forgery, Computer-related identity offences, Sending or controlling sending of Spam):

The title and relevant provision Minimum/maximum penalties • Computer-related fraud or forgery (Article 211, Article 247, Article 248) • Computer-related identity offences (Article 143)	Penal Code (Official Gazette RS, no. 50/12 – Officially consolidated version) Penal Code in Article 211 provides a general provision on fraud. Fraud Article 211 (*1) Whoever, with the intention of acquiring unlawful property benefit for himself or a third person by false representation, or by the suppression of facts leads another person into error or keeps him in error, thereby inducing him to perform an act or to omit to perform an act to the detriment of his or another's property, shall be sentenced to* ***imprisonment for not more than three years***. *(2) Whoever, with the intention as referred to in the preceding paragraph of this Article, concludes an insurance contract by stating false information, or suppresses any important information, concludes a prohibited double insurance, or concludes an insurance contract after the insurance or loss event have already taken place, or misrepresents a harmful event, shall be sentenced to* ***imprisonment for not more than one year***. *(3) If the fraud was committed by at least two persons who colluded with the intention of fraud, or if the perpetrator committing the offence referred to in paragraph 1 of this Article caused large-scale property damage, the perpetrator shall be sentenced to* ***imprisonment for not less than one, and not more than eight years***. *(4) If the offence referred to in paragraphs 1 or 3 of this*

	Article was committed within a criminal organisation, the perpetrator shall be sentenced to ***imprisonment for not less than one, and not more than ten years.***
	(5) If a minor loss of property has been incurred by the committing of the offence under paragraph 1 of this Article and if the perpetrator's intention was to acquire a minor property benefit, he shall be punished by ***a fine or sentenced to imprisonment for not more than one year.***
	(4) Whoever, with the intention of causing damage to another person by false representation or the suppression of facts, leads a person into error or keeps him in error, thereby inducing him to perform an act or to omit to perform an act to the detriment of his or another's property shall be punished by a fine or sentenced to ***imprisonment for not more than one year.***
	(5) The prosecution for the offences under paragraphs 5 and 6 of this Article shall be initiated upon a complaint.
	Use of counterfeit non-cash means of payment Article 247
	(*1) Whoever installs on an automatic dispenser for money or an apparatus for payment by card a device for copying records of payment or credit cards, or acquires the recognition of such cards through a payment on the whole Internet, or makes a forgery thereof in any other way, or whoever uses such a counterfeit payment or credit card and thus gains property benefit, shall be sentenced to* ***imprisonment for not more than five years***.
	(2) Whoever forges or uses a forged other card or another non-cash means of payment and gains a property benefit by means of technical devices for the recognition of a card or any other non-cash means of payment recognition, shall be

	punished to the same extent. *(3) If a major property benefit has been gained through the offence under paragraphs 1 or 2 of this Article, the perpetrator shall be sentenced to* ***imprisonment for not less than one and not more than eight years.***
	Fabrication, Acquisition and Disposal of Instruments of Forgery Article 248
	(*1) Whoever fabricates, keeps, transfers, acquires, or sells instruments for forging money, stamps of value or securities, or for copying records of credit, debit or other cards or other non-cash means of payment, or otherwise makes such instruments available for use, shall be sentenced to* ***imprisonment for not more than two years***. *(2) The instruments of forgery shall be seized.*
	Abuse of Personal Data Article 143
	(1) Whoever publishes or causes to be published personal data processed on the basis of the law or the personal consent of the individual to whom the personal data relate without any basis in law or without the personal consent of the individual shall be punished by a ***fine or sentenced to up to one year in prison.*** *(2) Whoever breaks into a computer database in order to acquire personal data for his or a third person's use shall be* ***punished in accordance with the preceding paragraph***. *(3) Whoever publishes on the World Wide Web or otherwise*

	publishes or enables another person to publish personal data of victims of criminal offences, victims of violation of rights and liberties, protected witnesses, which are contained in judicial records of court proceedings, in which the presence of the public or witness identification or protected witnesses and personal records thereof related to the court proceeding was not allowed according to the law or court decision, on the basis of which these persons may be identified or are identifiable, shall be sentenced to ***imprisonment for not more than three years.*** *(4) Whoever assumes the identity of another person or, by processing his or her personal data, exploits his or her rights, gains proceeds or non-pecuniary benefits or adversely affects his or her personal dignity shall be* ***sentenced to between three months and three years in prison.*** *(5) Whoever commits the offence referred to in paragraph 1 of this Article by publishing or causing to be published sensitive personal data shall be* ***sentenced to up to two years in prison.*** *(6) If any offence from the preceding paragraphs of this Article is committed by an official through the abuse of office or official authority, such an official shall be sentenced to* ***imprisonment for not more than five years.*** *(7) The prosecution under paragraph 4 of this Article shall be initiated upon a complaint.*
Intent/recklessness	*Offences provided in Articles 211, 247, 248 and 143 of the Penal Code have to be committed intentionally. According to the Article 27 of the Penal Code the perpetrator shall be punished for the criminal offence committed through negligence only if the law so determines.*

Aggravating/mitigating factors	Penal Code provides in its general provisions, Article 49 general rules on sentencing: General Rules on Sentencing Article 49 *(1) The perpetrator shall be sentenced for a criminal offence within the limits of the statutory terms provided for such an offence and with respect to the gravity of his offence and his guilt.* *(2) In fixing the sentence, the court shall consider all circumstances, which have an influence on the grading of the sentence (mitigating and aggravating circumstances), in particular: the degree of the perpetrator's guilt; the motives, for which the offence was committed; the intensity of the danger or injury caused to the property protected by law; the circumstances, in which the offence was committed; the perpetrator's past behaviour; his personal and pecuniary circumstances; his conduct after the committing of the offence and especially, whether he recovered the damages caused by the committing of the criminal offence; and other circumstances referring to the personality of the perpetrator and to the expected effect of the punishment on the future life of the perpetrator in the social environment.* *(3) In fixing the sentence of a perpetrator who committed a criminal offence after he had already been convicted or had served his sentence, or after the implementation of his sentence had been barred by time, or after his sentence has been remitted (recidivism), the court shall pay particular attention to whether the earlier offence is of the same type as the new one, whether both offences were committed for the same motive and to the time, which has lapsed since the*

	former conviction or since the serving, withdrawing, remitting or barring of the sentence. *<u>Aggravating factors</u>: Penal Code in Article 41 provides a general provision for offences committed within criminal organisation.* Liability of Members and Leaders of Criminal Organisation Article 41 (*1) A member (hereinafter: the member) of a criminal organisation with at least three persons shall be punished with a severer sentence prescribed for a criminal offence committed within a criminal organisation if he commits the criminal offence to implement the criminal organisation's plan in association with at least one member as an accessory or accomplice.* *(2) In the case referred to in paragraph 1 of this Article, the leader of the criminal organisation, who led the implementation of the criminal plan or had at his disposal illegally gained property benefits at the time of committing the criminal offence based on the criminal plan, notwithstanding whether he participated at its implementation directly as the perpetrator or accessory pursuant to Articles 20 or 37 and 38 of this Penal Code, shall be punished the same as the perpetrator.* Penal Code in Article 294 also provides liability for participation in a criminal organisation as a separate criminal offence. Article 294 provides for a mitigating factor in the paragraph 3.

	Criminal Organisation Article 294 (*1) Whoever participates in a criminal organisation which has the purpose of committing criminal offences, for which a punishment by imprisonment of more than three years, or a life sentence may be imposed, shall be punished by imprisonment of three months up to five years.* *(2) Whoever establishes or leads an organisation as referred to in the preceding paragraph, shall be punished by imprisonment of six months up to eight years.* *(3) A perpetrator of a criminal offence from the preceding paragraphs who prevents further commission of these offences or discloses information which has a bearing on the investigation and proving of criminal offences that have already been committed, may have his punishment for these offences mitigated, in accordance with Article 51 of this Penal Code.*
Multiple crimes/recidivism	Penal Code provides in its general provisions, Article 49 general rules on sentencing: General Rules on Sentencing Article 49 (*1) The perpetrator shall be sentenced for a criminal offence within the limits of the statutory terms provided for such an offence and with respect to the gravity of his offence and his guilt.* *(2) In fixing the sentence, the court shall consider all circumstances, which have an influence on the grading of the sentence (mitigating and aggravating circumstances), in particular: the degree of the perpetrator's guilt; the motives,*

	for which the offence was committed; the intensity of the danger or injury caused to the property protected by law; the circumstances, in which the offence was committed; the perpetrator's past behaviour; his personal and pecuniary circumstances; his conduct after the committing of the offence and especially, whether he recovered the damages caused by the committing of the criminal offence; and other circumstances referring to the personality of the perpetrator and to the expected effect of the punishment on the future life of the perpetrator in the social environment. *(3) In fixing the sentence of a perpetrator who committed a criminal offence after he had already been convicted or had served his sentence, or after the implementation of his sentence had been barred by time, or after his sentence has been remitted (recidivism), the court shall pay particular attention to whether the earlier offence is of the same type as the new one, whether both offences were committed for the same motive and to the time, which has lapsed since the former conviction or since the serving, withdrawing, remitting or barring of the sentence.*
Incitement, aiding and abetting, and attempt	The provisions on incitement, aiding and abetting and attempt are provided in general provisions of the Penal Code: <u>Attempt</u> Attempt Article 34 *(1) Any person, who intentionally initiated a criminal offence but did not complete it, shall be punished for the criminal attempt, provided that such an attempt involved a criminal offence, for which the sentence of three years' imprisonment or a heavier sentence may be imposed under the statute; attempts involving any other criminal offences*

	shall be punishable only when so expressly stipulated by the statute. *(2) Against the perpetrator, who attempted to commit a criminal offence, the sentence shall be applied within the limits prescribed for such an offence or it may be reduced.* <u>Incitement, aiding and abetting</u> Participant Article 36a *The provisions of this Code that are applicable to the perpetrator shall also apply to a participant who solicits or supports a criminal offence, unless otherwise provided by the law.* Criminal Solicitation Article 37 *(1) Any person who intentionally solicits another person to commit a criminal offence shall be punished as if he himself had committed it.* *(2) Any person who intentionally solicits another person to commit a criminal offence, for which the sentence of three years' imprisonment or a heavier sentence may be imposed under the statute, shall be punished for the criminal attempt even if the committing of such an offence had never been attempted*. Criminal Support Article 38

	(1) Any person who intentionally supports another person in the committing of a criminal offence shall be punished as if he himself had committed it, or his sentence shall be reduced, as the case may be. *(2) Support in the committing of a criminal offence shall be deemed to be constituted, in the main, by the following: counselling or instructing the perpetrator, on how to carry out the criminal offence; providing the perpetrator with instruments of criminal offence or removing the obstacles for the committing of criminal offence; a priori promises to conceal the perpetrator's criminal offence or any traces thereof; instruments of the criminal offence or objects gained through the committing of criminal offence.* Punishability of Those Soliciting or Supporting a Criminal Attempt Article 39 *If the perpetration of a criminal offence falls short of the intended consequence, those soliciting (hereinafter, the instigator) or supporting (hereinafter, the aide) the criminal attempt shall be punished according to the prescriptions that apply to the criminal attempt.* Limits of Punishability of Accomplices Article 40 *(1) The perpetrator, the instigator and the aide shall be punished for criminal offences within the limits of their intent.* *(2) If the instigator or the aide voluntarily prevented the intended criminal offence from being accomplished, his sentence may be withdrawn.* *(3) Personal relations, attributes and circumstances, on the*

	basis of which the guilt or punishability are excluded by law or sentence remitted, reduced or extended, shall be taken into consideration only with respect to the accomplice (hereinafter, the accomplice), by whom such relations, attributes and circumstances were determined.

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

According to the Slovenian authorities, Directive 2011/93/EU has been completely implemented in national law. However, they plan to introduce an additional change and an amendment of the relevant legislative provisions in order to take effective measures against websites containing or disseminating child abuse material (CAM). There are many obstacles to this, including questions related to internet integrity and even freedom of speech (free internet) and censorship issues. The police see this topic from the perspective of child protection, and reject these issues as improper and degrading in relation to child victims.
There is also a data retention issue related to the decision rendered by the Constitutional Court of the Republic of Slovenia in July 2014.

The amendment of the Police Tasks and Powers Act plans to establish the legal basis for a new database to help identify victims (identifying abused children in images and video clips).

C/ Online card fraud

Online card fraud offences in Slovenia are treated in accordance with Article 211 of the Penal Code (KZ-1). Such cases relate to unauthorised use of information about payment cards for online payments.

Fraud - Article 211 KZ-1

(1) Whoever, with the intention of acquiring unlawful property benefits for himself or a third person, by false representation, or by the suppression of facts, leads another person into error or keeps him in error, thereby inducing him to perform an act or to omit to perform an act to the detriment of his or another's property, shall be sentenced to imprisonment for no more than three years.

(2) Whoever, with the intention referred to in the preceding paragraph of this Article, concludes an insurance contract by stating false information or suppressing any important information, concludes a prohibited double insurance contract, concludes an insurance contract after the insurance or loss event has already taken place, or misrepresents a harmful event, shall be sentenced to imprisonment for no more than one year.

(3) If the fraud was committed by at least two persons who colluded with the intention of fraud, or if the perpetrator committing the offence referred to in paragraph 1 of this Article caused large-scale property damage, the perpetrator shall be sentenced to imprisonment for no less than one, and no more than eight years.

(4) If the offence referred to in paragraphs 1 or 3 of this Article was committed within a criminal association, the perpetrator shall be sentenced to imprisonment for no less than one, and no more than ten years.

(5) If a minor loss of property has been incurred by committing the offence under paragraph 1 of this Article and if the perpetrator's intention was to acquire a minor property benefit, he shall be punished by a fine or sentenced to imprisonment for no more than one year.

(6) Whoever, with the intention of causing damage to another person by false representation or the suppression of facts, leads a person into error or keeps him in error, thereby inducing him to perform an act or to omit to perform an act to the detriment of his or another's property, shall be punished by a fine or sentenced to imprisonment for no more than one year.
(7) The prosecution for the offences under paragraphs 5 and 6 of this Article shall be initiated upon a complaint.

What can be understood from the content of this Article is that the police treat offences related to online card fraud offences *ex officio* when they do not result in a minor property benefit (less than EUR 500). If a minor property benefit is gained from an offence, the police initiate a pre-trial investigation on the basis of a complaint submitted by the injured party. Such investigations can be divided into two categories in terms of complaints filed. Cases in which Slovenian citizens are victims of card fraud belong in the first category. In the majority of cases, information about cards is acquired by phishing or hacking information systems and is then used for payments on various websites abroad. In such cases, injured parties report criminal offences to the police themselves. If they report a criminal offence to the bank with which they hold a current account, the bank will refer them to the police.

In cases where payment cards issued by foreign banks are abused on websites in Slovenia, a criminal offence is reported by the bank which has signed a contract with the point of sale where the card was abused. In such cases, banks report criminal offences in accordance with the Protocol signed between the police and the ZBS to the single point of contact (Protocol defined below). The criminal offence is then referred for investigation to the competent regional unit. In accordance with the law, the police inform the injured party after the investigation has been concluded.

The Slovenian police also deal with criminal offences where perpetrators acquire payment card recognition information through payments over the entire internet. Such criminal offences are treated in accordance with Article 247 of KZ-1, which also covers the installation of devices that copy information from the magnetic strips on payment cards (skimming) and the use of counterfeit payment cards:

Use of a counterfeit non-cash means of payment - Article 247 KZ-1:
(1) Whoever installs on an automatic cash dispenser or an apparatus for payment by card a device for copying the records of bank or credit cards, or acquires the recognition of such cards through a payment over the whole internet, or makes a forgery thereof in any other way, or whoever uses such a counterfeit bank or credit card and thus gains a property benefit, shall be sentenced to imprisonment for no more than five years.
(2) Whoever forges a card or uses a forged card which enables the gaining of a property benefit by means of technical devices for card recognition shall be punished to the same extent.
(3) If a major property benefit has been gained through the offence under paragraphs 1 or 2 of this Article, the perpetrator shall be sentenced to imprisonment for no less than one and no more than eight years.

When they detect such criminal offences, banks report them to the single point of contact at the police in accordance with the Protocol signed between the police and the ZBS.

The Slovenian police have not detected any problems in acquiring reports of payment card fraud. As already mentioned, banks report any suspicion of payment card fraud to the single point of contact, while citizens usually report fraud at the police unit nearest to their residence.

5.2 Procedural issues

5.2.1 Investigative techniques

- Searching for and collecting data from information systems/computers

During the investigation of a criminal offence related to electronic devices and electronic data carriers, an investigation may be carried out to acquire data in an electronic form if there are reasonable grounds to suspect that a criminal offence has been committed, and if it is probable that the electronic device contains electronic data on the basis of which a suspect or accused person may be identified, discovered or arrested, or traces of a criminal offence may be discovered which are relevant to the criminal proceedings or may be used as evidence in the criminal proceedings.

- Interception/collection of data on traffic/content in real time

Article 150 of the Criminal Procedure Act sets out the options and conditions for the interception/collection of data in real time:

(1) If there are well-founded grounds to suspect that a particular person has committed, is committing or is preparing or organising to commit any of the criminal offences listed in the second paragraph of this Article, and if there is a well-founded suspicion that such person is using for communications in connection with this criminal offence a particular means of communication or computer system or that such means or system will be used, wherein it is possible to reasonably conclude that other measures will not permit the gathering of data or that the gathering of data could endanger the lives or health of people, the following may be ordered against such person:

1) the monitoring of electronic communications using listening and recording devices, and the control and protection of evidence on all forms of communication transmitted over the electronic communications network;

2) control of letters and other parcels;

3) control of the computer systems of banks or other legal entities which perform financial or other commercial activities;

4) wire-tapping and recording of conversations with the permission of at least one person participating in the conversation.

(2) The criminal offences in connection with which the measures from the previous paragraph may be ordered are:

1) criminal offences against the security of the Republic of Slovenia and its constitutional order, and crimes against humanity and international law for which the law prescribes a prison sentence of five or more years;

2) the criminal offences of kidnapping under Article 134, sexual assault on a person below fifteen years of age under Article 173a, exploitation through prostitution under Article 175, the showing, possession, manufacture and distribution of pornographic material under Article 176, unlawful manufacture of, and trade in, narcotic drugs, illicit substances in sport and precursors to manufacture narcotic drugs under Article 186, rendering opportunity for consumption of narcotic drugs or illicit substances in sport under Article 187, extortion and blackmail under Article 213, abuse of inside information under Article 238, unlawful acceptance of gifts under Article 241, unauthorised giving of gifts under Article 242, money laundering under Article 245, smuggling under Article 250, abuse of public funds under Article 257a, acceptance of bribes under Article 261, giving bribes under Article 262, acceptance of benefits for illegal intermediation under Article 263, giving gifts for illegal intermediation under Article 264, criminal association under Article 294, illegal manufacture of, and trade in, weapons or explosive materials under Article 307, and unlawful handling of radioactive or other dangerous substances under Article 334 of the Criminal Code;

3) other criminal offences for which the law prescribes a prison sentence of eight or more years.

Duties of operators in connection with facilitating lawful interception of communications are defined in Article 160 of ZEKom-1, which reads as follows:

(1) Operators shall be obliged to enable lawful interception of communications at a particular point in the public communications network immediately on receipt of a copy of that part of the order of a competent body stating the point of the public communications network at which lawful interception of communications should be undertaken, and other data relating to the method, extent and duration of such measure.

(2) The copy of the order from the preceding paragraph shall be made by the body that issued the order.

(3) Operators shall be obliged to enable lawful interception of communications in the manner, scope and duration laid down in the copy of the order referred to in the first paragraph of this Article.

(4) In exceptional cases, operators shall be obliged to enable lawful interception on the basis of an oral order if so stipulated by the law which also stipulates the conditions and circumstances for the issuing of an oral order. A written copy of the oral order shall be supplied to the operator as soon as possible, but not later than within 48 hours of it being issued.

(5) Operators shall ensure thirty-year indelible registration of each lawful interception of communications, which includes data from the first and/or fourth paragraphs of this Article and data on the implementation of the order (who implemented it and the duration of interception), and shall protect them during this period in line with the level of classification of the copy of the order. The authority implementing supervision of communications under the order from the third paragraph of this Article shall store such data in accordance with the regulation governing its operation.

(6) Operators shall be obliged at their own expense to provide adequate equipment in their networks and appropriate interfaces enabling lawful interception of communications in their networks. In the interception of communications in international electronic communications networks in accordance with the law governing the Slovenian Intelligence and Security Agency, the operator of the network shall provide, at its own cost, adequate equipment and appropriate interfaces enabling lawful interception of international communications in its network, or adequate transmission routes to interfaces in the control centre of the responsible body.

(7) The minister, in agreement with the minister responsible for internal affairs, the minister responsible for defence and the director of the Slovenian Intelligence and Security Agency, shall prescribe the functionality of equipment and determine appropriate interfaces referred to in the preceding paragraph.

(8) The Agency shall supervise operators' compliance with obligations referred to in this Article, which shall not interfere with the responsibility of competent authorities to supervise lawful interception pursuant to other laws.

- Saving computer data

During the criminal prosecution proceedings, the data confiscated during the investigation of a criminal offence are kept until the conclusion of the court proceedings. In the first phase, the police confiscate and protect the data, which is then submitted to the competent State Prosecutor's Office together with the criminal complaint. The State Prosecutor's Office then submits them to the competent court together with the indictment.

- Order regarding the saved data on traffic/content

Measures referred to in Article 150 of the ZKP are ordered by written order of the investigating judge at the written proposal of a state prosecutor. The investigation of an electronic device and data arising from the electronic device may be carried out pursuant to the second paragraph of Article 219a of the ZKP on the basis of the preliminary written consent of the owner and users of the electronic device known and available to the police, who justifiably expect privacy (user), or on the basis of an explanatory written order of the court issued at the proposal of a state prosecutor. If the investigation is carried out on the basis of a court order, a copy of this order is submitted to the owner or user of the electronic device to be searched.

- Order for information on the user

In the Republic of Slovenia, the manner of acquisition of the information on users kept by internet service providers was amended following Constitutional Court Decision no U-I-65/13 of 3 July 2014, which repealed the provision of Articles 162 to 169 ZEKom-1. The repealed provisions of the aforementioned Act defined the storage of data of all communications via fixed network telephony, mobile telephony, internet access, e-mail and internet telephony. The Constitutional Court decision obliged the operators referred to in the first paragraph of Article 163 of the ZEKom-1 to destroy all data kept on the basis of the repealed provisions immediately after the publication of the decision.

The provisions laid down in the third paragraph of Article 149b of the ZKP regulate the manner of and conditions for the acquisition of data on users of information services, but these provisions do not facilitate the acquisition of data to the same extent as the provisions of the ZEKOM-1 repealed by the Constitutional Court of the Republic of Slovenia.

During investigations of criminal offences related to cybercrime, investigation methods specific to a certain case of cybercrime are used. During all types of cybercrime investigation, the Slovenian police encounter digital data and digital evidence acquired in accordance with the provisions of the ZKP. Such data is acquired and coordinated according to the principles and rules of digital forensics. The tools and procedures of digital forensics are employed by the Slovenian police using suitable equipment, software and hardware which are in line with the latest trends in digital forensics.

A good example in which all cybercrime investigation and digital forensics procedures were used was a successful international investigation into malware called Mariposa/Butterfly Bot and a network of infected computers. On the basis of the provisions of the Convention on Cybercrime, there was an efficient exchange of data and evidence among various foreign police services, which led to the successful conclusion of the case, the tracking down of several perpetrators in countries around the world and several final judgments.

5.2.2 Forensics and encryption

Forensic examinations are performed by the police, specifically the computer investigation units. They are performed in line with the conditions laid down in Article 219a of the ZKP, which provides details of the investigation of electronic devices, devices connected to them and digital data carriers.

The Republic of Slovenia has no legal basis for remote forensic examinations.

It is the view of the Slovenian authorities that, in most cases, encryption and related data and digital evidence restrict the successful investigation of criminal offences. Most frequently, the Slovenian police solve problems with encrypted data within their own organisation, the funds and resources of which are, however, limited. There are no specialist centres; decryption is not carried out in cooperation with private companies.[10]

5. 2.3 E-evidence

According to Slovenian law, 'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; 'traffic data' means any data processed for the purpose of the conveyance of a communication on an electronic communications network, or for the billing thereof.

The protection of data from an electronic device is a preliminary procedure of the investigation of the electronic device, and is laid down by Article 223a of the ZKP. The aforementioned statutory provision prescribes in detail the manner in which this procedure and its mandatory constituents are to be implemented.

When confiscating a device in order to investigate it, the data must be protected by being stored on another data carrier in a manner which preserves the identity and integrity of the data, and the possibility of using them in further proceedings. An identical copy of the whole carrier may also be produced, whereby the integrity of the copy of the data must be ensured. If that is not possible, the device (or just the data carrier) must be sealed.

[10] After the on-site visit the evaluation team was informed that password-cracking and decryption equipment is currently being purchased, with delivery planned by the end of November 2016. In will be installed in the Computer Investigation Centre and available (also by remote access) to all computer investigation units. In case of encryption, the court has the possibility to additionally order the opinion of an expert and use their opinion as evidence. This is done where the police lack the adequate resources while the latter exist on the market.

The Article defines a requirement of permanent destruction of the copy of the data copied from the electronic device, confiscated without a court order, for which minutes must be made. The requirement is applicable if the court has not issued an order for the investigation of the electronic device within twelve hours and written consent for the investigation (second paragraph of Article 223a of the ZKP) has not been obtained in advance.

The owner, user, operator or manager of the device or anyone else who has access to it must, at the request of the authorities, make every effort to prevent the data being destroyed, modified or concealed. If the person does not wish to do so, they may be liable to punishment (except if they are a suspect, a person who must not be questioned as a witness or a person who has renounced testimony).

The owner of the device, their representative or lawyer, or an expert is invited to be present during the data protection procedure. If they do not respond to the invitation, or are absent or unknown, the data protection procedure is carried out without their presence. The data protection procedure must be carried out by a suitably qualified person (fourth paragraph of Article 223a of the ZKP).

During the data protection procedure, the control value is also recorded in the minutes, or the possibility of verifying the identity and integrity of the protected data is suitably provided in the minutes. A copy of the minutes is submitted to the person who was present during the data protection procedure (fifth paragraph of Article 223a of the ZKP).

In the confiscation and protection of data, the rights of persons who are not suspects must be interfered with to the least possible extent. The secrecy and confidentiality of data must be protected, and the occurrence of disproportional damage due to the inability to use the device must be prevented.

Copies of the confiscated data are kept for as long as the proceedings require them to be. Electronic devices are kept until the data is stored in a manner which ensures the identity and integrity of the confiscated data, but no longer than three months. If the production of such a copy of the data is not possible, the device (or the part of it which contains the data) is kept for up to six months. The device may be kept longer if it was used to commit a criminal offence or if the device itself is to be used as evidence in criminal proceedings (seventh paragraph of Article 223a of the ZKP).

Copies of data referring to the criminal prosecution of which the storage has no basis in legislation are excluded from the file and, if possible, destroyed. Their destruction is recorded in the minutes (eighth paragraph of Article 223a of the ZKP).

Electronic evidence:
In the first paragraph of Article 219a of the ZKP, the terms ‘electronic data’ and ‘data in electronic form’ are used, which refer to the investigation of electronic and related devices and electronic data carriers on the basis of which a suspect or accused person may be identified, discovered or arrested, or traces of a criminal offence may be discovered which are relevant to the criminal proceedings or may be used as evidence in the criminal proceedings.

In the first paragraph of Article 223a of the ZKP, the term ‘electronic data’ is used when it mentions the protection of these data. Regarding ‘data in electronic form’, the Electronic Commerce and Electronic Signature Act (Official Gazette of the Republic of Slovenia, No 98/04 – official consolidated text, No 61/06 – ZEPT and No 46/14; hereinafter ‘the ZEPEP’) defines ‘data in electronic form’ as data designed, stored, sent, received or exchangeable electronically. Data in electronic form must not be refused validity or evidence value merely because it is in electronic form.

Sending of electronic evidence to a prosecutor's office or court:

According to Article 219a of the ZKP, the investigation of electronic data is to be carried out in a manner which preserves the integrity of the original data and the possibility of using them in further proceedings. The investigation must be carried out in a manner which interferes with the rights of persons who are not suspects or accused persons to the least possible extent, which protects the secrecy and confidentiality of the data, and which does not cause disproportionate damage. The investigation should be carried out by a qualified person. Minutes are to be taken of the investigation and data protection procedure and attached to the criminal complaint as provided by the ninth paragraph of Article 148 of the ZKP. Additional attachments required include an identical copy of the original medium and the excluded data. At least two copies of the data attached to the criminal complaint must be submitted to a State Prosecutor's Office, one of which must be suitably stored in a manner which ensures the identity and integrity of the data. Such data is kept for as long as the proceedings require it to be.

In order to provide accurate and, above all, secure electronic storage (legal validity of digital documents), the contractors must adhere to the valid legislation in the field and other legal Acts which provide guidelines and standards for management of electronic documents.

5.3 Protection of human rights/fundamental freedoms

According to Slovenian legislation, fundamental rights and freedoms, in particular privacy, personal data and freedom of expression, may be limited in accordance with the law. Articles 149b, 150 and 156 of the Criminal Procedure Act set out investigative measures:

Article 149b

(1) If there are reasonable grounds to suspect that a criminal offence for which a perpetrator is prosecuted ex officio has been committed, is being committed or is being prepared or organised, and information on communications needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may, at the request of the public prosecutor adducing reasonable grounds, order the operator of the electronic communications network to furnish the competent body with information on the participants in and the circumstances and facts of electronic communications, such as: number or other form of identification of users of electronic communications services; the type, date, time and duration of the call or other form of electronic communications service; the quantity of data transmitted; and the place where the electronic communications service was performed.

(2) The request and order must be in written form and must contain information that allows the means of electronic communication to be identified, an indication of reasonable grounds, the time period for which the information is required and other important circumstances that dictate use of the measure.

(3) If there are reasonable grounds to suspect that a criminal offence for which a perpetrator is prosecuted ex officio has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the relevant directory, as well as information on the time that the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may demand that the operator furnish it with this information, at its written request and even without the consent of the individual to whom the information refers.

(4) The operator of networks may not disclose to its clients or to a third party the fact that it has given certain information to a competent body (first paragraph of this Article) or the police (preceding paragraph), or that it intends to do so.

Article 150

(1) If there are well-founded grounds to suspect that a particular person has committed, is committing or is preparing or organising to commit any of the criminal offences listed in the second paragraph of this Article, and if there is a well-founded suspicion that such person is using for communications in connection with this criminal offence a particular means of communication or computer system or that such means or system will be used, wherein it is possible to reasonably conclude that other measures will not permit the gathering of data or that the gathering of data could endanger the lives or health of people, the following may be ordered against such person:

1) the monitoring of electronic communications using listening and recording devices, and the control and protection of evidence on all forms of communication transmitted over the electronic communications network;

2) control of letters and other parcels;

3) control of the computer systems of banks or other legal entities which perform financial or other commercial activities;

4) wire-tapping and recording of conversations with the permission of at least one person participating in the conversation.

(2) The criminal offences in connection with which the measures from the previous paragraph may be ordered are:

1) criminal offences against the security of the Republic of Slovenia and its constitutional order, and crimes against humanity and international law for which the law prescribes a prison sentence of five or more years;

2) the criminal offences of kidnapping under Article 134, sexual assault on a person below fifteen years of age under Article 173a, exploitation through prostitution under Article 175, the showing, possession, manufacture and distribution of pornographic material under Article 176 , unlawful manufacture of, and trade in, narcotic drugs, illicit substances in sport and precursors to manufacture narcotic drugs under Article 186, rendering opportunity for consumption of narcotic drugs or illicit substances in sport under Article 187, extortion and blackmail under Article 213, abuse of inside information under Article 238, unlawful acceptance of gifts under Article 241, unauthorised giving of gifts under Article 242, money laundering under Article 245, smuggling under Article 250, abuse of public funds under Article 257a, acceptance of bribes under Article 261, giving bribes under Article 262, acceptance of benefits for illegal intermediation under Article 263, giving gifts for illegal intermediation under Article 264, criminal association under Article 294, illegal manufacture of, and trade in, weapons or explosive materials under Article 307, and unlawful handling of radioactive or other dangerous substances under Article 334 of the Criminal Code;

3) other criminal offences for which the law prescribes a prison sentence of eight or more years.

Article 156

(1) The investigating judge may, based on a properly reasoned request by the public prosecutor, order a bank, savings bank, payment institution or electronic money company to disclose to him information and provide documentation on the deposits, statements of account and account transactions or other transactions by the suspect, the accused and other persons who may reasonably be presumed to have been implicated in the financial transactions or deals of the suspect or the accused, if such data might represent evidence in criminal proceedings or are necessary for the confiscation of objects or the securing of a request for the confiscation of proceeds or property in the value of proceeds.

(2) The bank, savings bank, payment institution or electronic money company shall immediately send to the investigating judge the information and documentation referred to in the preceding paragraph.

(3) Subject to the conditions laid down in the first paragraph of this Article, the investigating judge may, based on a properly reasoned request by the public prosecutor, order a bank, savings bank, payment institution or electronic money company to keep track of the financial transactions of the suspect, the accused and other persons reasonably presumed to have been implicated in the financial transactions or deals of the suspect or the accused, and to disclose to him confidential information about the transactions or deals which the aforesaid persons are carrying out or intend to carry out at these institutions or services. In the order, the investigating judge shall set the time period within which the bank, savings bank, payment institution or electronic money company shall provide him with the information.

(4) The measure referred to in the preceding paragraph may be applied for a maximum of three months, but the term may, for weighty reasons, upon request of the public prosecutor, be extended to a maximum of six months.

(5) If there are reasonable grounds to suspect that the criminal offence for which a perpetrator is being prosecuted ex officio has been committed or is being prepared, and in order to uncover this criminal offence or the perpetrator thereof it is necessary to obtain information on the holder or the authorised person of a certain payment account, savings account or cash deposit, on the renter or the authorised person of a safety deposit box and on the period in which they were or are being used, the police may, by a written request, order the bank, savings bank, payment institution or electronic money company to furnish them without delay with such information, even without the consent of the person to whom the information refers.

(6) The bank, savings bank, payment institution or electronic money company may not disclose to its clients or to third persons that it has sent, or will send, the information and documents to the investigating judge or to the police (preceding paragraph).

Personal data protection act (Official Gazette RS, No 94/07 – officially consolidated version):

Restriction of the rights of an individual

Article 36

(1) The rights of an individual set out in the third and fourth paragraphs of Article 19 (Informing the individual of the processing of personal data), Article 30 (Right of the individual to information) and Article 32 (Right to supplement, correct, block, erase and object) of this Act may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, the political and economic interests of the state, the exercise of the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others.
(2) Restrictions under the previous paragraph may only be provided to the extent necessary to achieve the purpose for which the restriction was provided.

5.4 Jurisdiction

5.4.1 Principles applied to the investigation of cybercrime

Application of the Penal Code of the Republic of Slovenia to Any Person Who Commits a Criminal Offence in Its Territory

Article 10

(1) The Penal Code of the Republic of Slovenia shall apply to any person who commits a criminal offence in the territory of the Republic of Slovenia.

(2) The Penal Code of the Republic of Slovenia shall also apply to any person who commits a criminal offence on a domestic vessel regardless of its location at the time of the committing of the offence.

(3) The Penal Code of the Republic of Slovenia shall also apply to any person who commits a criminal offence on a domestic civil aircraft in flight or on a domestic military aircraft regardless of its location at the time of the committing of the offence.

Application of the Penal Code of the Republic of Slovenia
for Specific Criminal Offences Committed in a Foreign Country
Article 11

The Penal Code of the Republic of Slovenia shall apply to any person who, in a foreign country, commits

- a criminal offence under Article 243 of this Penal Code or the criminal offences referred to in Articles 332, 333 and 334 of this Code, provided that they were committed in the ecological protection zone or in the continental shelf of the Republic of Slovenia;

- criminal offences under Article 108 and Articles 348-360 of this Penal Code.

Application of the Penal Code of the Republic of Slovenia to Citizens
of the Republic of Slovenia Who Commit a Criminal Offence Abroad
Article 12

The Penal Code of the Republic of Slovenia shall be applicable to any citizen of the Republic of Slovenia who commits any criminal offence abroad other than those specified in the preceding Article.

Application of the Penal Code of the Republic of Slovenia to Foreign Citizens Who Commit a Criminal Offence Abroad

Article 13

(1) The Penal Code of the Republic of Slovenia shall apply to any foreign citizen who has, in a foreign country, committed a criminal offence against the Republic of Slovenia or any of its citizens, even though the offences in question are not covered by Article 11 of this Penal Code.

(2) The Penal Code of the Republic of Slovenia shall also be applicable to any foreign citizen who has, in a foreign country, committed a criminal offence against a third country or any of its citizens if he has been apprehended in the territory of the Republic of Slovenia, and not extradited to the foreign country. In such cases, the court shall not impose a sentence on the perpetrator which is heavier than the sentence prescribed by the law of the country in which the offence was committed.

Special Conditions for Prosecution

Article 14

(1) If, in cases under Article 10 and indent 1 of Article 11 of this Penal Code, the criminal procedure has been initiated or discontinued in a foreign country, the perpetrator may be prosecuted in the Republic of Slovenia only by permission of the Minister for Justice (hereinafter 'the Minister') with notice of the conditions under which the prosecution shall not violate the double jeopardy.

(2) In cases under Articles 12 and 13 of this Penal Code, the perpetrator shall not be prosecuted:

1) if he has served the sentence imposed on him in the foreign country or if it was decided in accordance with an international agreement that the sentence imposed in the foreign country is to be served in the Republic of Slovenia;

2) if he has been acquitted by a foreign court or if his sentence has been remitted or the execution of the sentence has fallen under the statute of limitations;

3) if, according to foreign law, the criminal offence concerned may only be prosecuted upon the complaint of the injured party and the latter has not been filed.

(3) In cases under Articles 12 and 13, the perpetrator shall be prosecuted only insofar as his conduct constitutes a criminal offence in the country in which it was committed.

(4) If, in the case under Article 12 of this Penal Code, the criminal offence committed against the Republic of Slovenia or the citizen thereof does not constitute a criminal offence under the law of the country in which it was committed, the perpetrator of such an offence may be prosecuted only by permission of the Minister for Justice of the Republic of Slovenia.

(5) If, in all other cases except the cases referred to in indent 2 of Article 11 and paragraph 4 of this Article of this Penal Code, the criminal offence is not punished in the country in which it was committed, the perpetrator may be prosecuted only by permission of the Minister for Justice and with the proviso that, according to the general principles of law recognised by the international community, the offence in question constituted a criminal act at the time it was committed.

(6) In the case under Article 10, the prosecution of a foreign person may be transferred to another country under the conditions provided by the statute.

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

The Slovenian police have so far not dealt with any cases which would involve such conflicts. There have, however, been a number of cases of foreign nationals being identified as perpetrators of cybercrime acts. In such cases, the Slovenian police forward gathered evidence (including digital evidence) on the perpetrator to the competent country via Europol.

However, according to the regulation on personal and territorial application of the Slovenian Penal Code and legal instruments for international cooperation, including the transfer of proceedings, extradition and surrender, such conflicts would be resolved according to Slovenian material and procedural law.

5.4.3 Perception of Slovenia with regard to legal framework to combat cybercrime

The Slovenian authorities expressed the opinion that national legislations of Member States still vary greatly, as do those of third states; much remains unclear on the subject of the retention, acquisition and status of data, which is essential for the efficient investigation of cybercrime and the identification of offenders. This largely applies to data kept by mobile and internet service providers: traffic and subscriber data. The legislation should specify in greater detail what data is defined as traffic, user and/or personal data (IP address, user name, password, etc.), and when it is so defined.

5.5 Conclusions

- At the time of the on-site visit Directive 2013/40/EU on attacks against information systems (transposition date 4 September 2015) has not yet been implemented into Slovenian legislation. After the on-site visit the evaluation team was informed that the directive has been implemented into the Slovenian legislation. Implementation was officially notified on 12 August 2016.
- According to the opinion expressed by Slovenian practitioners met, the criminal penalties relating to cybercrime imposed by the courts do not always reflect the gravity of the offences and their consequences.
- Existing Slovenian legislation lacks provisions on remote forensic examinations. Legislation is in place regarding the blocking/removal of illegal content (see detailed description in Chapter 6 below), but the evaluation team has noticed that practitioners do not use it finding it ineffective.
- The Slovenian authorities assessed that the legislation should specify in greater detail what data is defined as traffic, user and/or personal data (IP address, username, password, etc.), and when it is so defined. The evaluation team shares this opinion.

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

Number of incidents by category (*Source: SI-CERT*)

Type of incident	2008	2009	2010	2011	2012	2013	2014	% 2014-2013
Technical attacks	183	145	209	350	604	760	941	23.82%
Fraud	49	84	122	227	442	525	837	59.43%
Questions and requests	86	88	121	174	189	193	239	23.83%

According to data from SI-CERT, a total of 2 060 incidents were observed in Slovenia in 2014, which is an increase of almost 6.4 times compared to 2008. This increasing trend, which is worrying given the above-mentioned understaffing of the cyber security system, is observable both from the year-by-year incident statistics and from the table of categories of incidents, which shows an increase of 23.82% in technical attacks and of 59.43% in fraud compared to the previous year.

Cooperation between cyber security stakeholders has not been formalised, and primarily takes place at an informal level among response centres, except in cases when there is a legal basis. For example, Article 81 of ZEKom-1 sets out the procedure for information exchange between the Agency for Communication Networks and Services and SI-CERT in cases of security or integrity violations. The two bodies inform each other about incidents and provide help to resolve them; they exchange experiences or use the existing capacities. Certain owners/operators of critical infrastructure are also included in the information exchange.

6.1.2 Mechanism to respond to cyber attacks

When it is not possible to obtain data by means of international police cooperation, the Slovenian authorities use the institute of international legal aid, which sends the form of an initiative together with the available evidence to the competent state prosecution service. They consider such procedures to be very lengthy.

As part of international legal aid, the ZKP chapter on 'Procedure for international legal aid and implementation of international treaties in criminal law matters' (Articles 514 to 520) is used *mutatis mutandis*.

6.2 Measures against child pornography and sexual abuse online

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

As yet, there are no software databases in Slovenia specifically designed to identify victims. National authorities plan to establish a national child sexual exploitation database with the assistance of relevant foreign law enforcement agencies.

To avoid re-victimisation if images/videos are not deleted, there is close cooperation with the Safer Internet Centre established at the Faculty of Social Sciences at the University of Ljubljana through the hotline project *Spletno oko* (Web Eye). They are responsible for gathering all reports from the public of illegal websites or websites containing child abuse material; the *Spletno oko* hotline informs the police of these reports if they are uploaded on servers in Slovenia. Afterwards they secure this material for further investigation, and, if the administrator is not an offender, contact him or her to explain the illegal material uploaded (only for CAM!) to the website (notice and take-down procedure). The police warn the administrator that any further dissemination of CAM may be a violation of Article 176 of the Penal Code, and advise them to take the necessary steps to avoid any legal consequences.

The police have the legal power to issue warnings under Article 38(1) of the Police Tasks and Powers Act (which reads as follows: 'Police officers may warn natural persons, legal entities and state authorities of any circumstances, actions or failure to take action that threaten or could threaten public order, people's lives, personal safety or property.') The investigation will be carried on in order to identify the offender who uploaded the CAM, and also to identify child victims.

6.2.2 Measures to address sex exploitation/abuse online, sexting and cyber bullying

Slovenia has put in place measures to address sex exploitation/abuse online, sexting and cyber bullying, as follows:

- Training and awareness raising targeting teachers, counsellors, social workers, police officers and ombudsman officials; awareness raising targeting children and parents.
- Use of tools from the Safer Internet Centre, in which all relevant stakeholders participate (police, judiciary, academics, Ombudsman for Human Rights, Information Commissioner, SI-CERT, NGOs, etc.).
- MOOC awareness and training programmes provided by the ARNES network.

- Establishment of the E-Safer Point (*eVarna točka*) by UNICEF, the police and the Slovenian Safer Internet Centre.
- Publication of articles by law enforcement experts and academic research.
- Participation in various preventive and educational activities, e.g. internet self-defence (*Internetna samoobramba*), with companies, governmental institutions and NGOs.
- Taking care of police investigations in this field.

Within the Safer Internet Centre in Slovenia, the following measures address sex exploitation/abuse online and sexting:

- A national conference is organised by the Spletno oko hotline, the Criminal Police Directorate of the General Police Directorate at the National Police and the Association of Informatics and Telecommunications at the Chamber of Commerce and Industry of Slovenia; it is opened to and focuses on all professions related to child protection online (social services, teachers, LEAs, as well as the judiciary, the ministries, policy makers, ISPs, the media, human rights observers etc.).
- Workshops are held for children and young people.
- An online resource for teenagers, 'Naked online?', has been made available.
- This important topic is included in seminars for parents.
- Tips are provided to children, teenagers, parents and teachers at www.safe.si on how to prevent sexual abuse, as well as what to do if one is a victim of revenge porn or sexting.
- Cartoons and videos are available for target groups on these issues.
- The counsellors at the *Tom telefon* helpline offer help and advice to the victims of such crimes.
- Sexting photos and revenge porn material of minors can also be reported to the *Spletno oko* hotline as illegal content.

Within the Safer Internet Centre in Slovenia, the following measures address cyberbullying:

- Tips are provided to children, teenagers, parents and teachers at www.safe.si on how to prevent cyberbullying, as well as what to do if one is a victim or witness of online violence.
- Workshops on cyberbullying and cyber ethics are held at Slovenian elementary and high schools, and as part of seminars for parents in Slovenian schools.
- As part of the celebration of Safer Internet Day 2014, the Slovenian Awareness Centre safe.si organised an educational seminar about the role of teachers and social workers in the prevention of cyberbullying. The five-hour seminar took place at the Faculty of Social Sciences on 13 February 2014. The seminar was designed primarily for teachers and social workers, since they play a very significant role in the prevention of cyber violence. 218 of 262 registered participants attended.
- A puzzle leaflet about bullying has been published for youngsters.
- Online pledge against cyberbullying.
- Online decision tree: think about how to protect yourself online.
- A large campaign named 'Stop cyberbullying' was launched in 2009 with a TV advert on all major Slovenian TV stations, posters for schools and leaflets for young people. The campaign led to a noticeable increase in awareness of this topic both in the media and among children and teachers.
- Many videos and cartoons have been created on this topic.
- Many resources, both offline and online, include tips and information about this topic.
- The counsellors at the *Tom Telefon* helpline offer help and advice to the victims of online violence and cyberbullying.

Slovenia took a lead on scientific research to use better terminology that focuses on child protection and child victims of sexual exploitation, such as child sexual exploitation material and child sexual abuse material instead of child pornography. The outcome arises from the EMPACT Cybercrime CSE platform. The research was conducted also by representatives from the UK, Norway, Poland, Finland and Europol. The findings were a basis for a Luxembourg guidelines (for more information please refer to sub. 3.3.1).[11]

[11] Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, adopted on 28 January 2016.

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

Article 21 of Directive 2011/93/EU requires Member States to establish measures to prevent the advertisement of abuse opportunities and child sex tourism. In Slovenia, the dissemination of such advertising material as well as organisation of travels with the purpose to commit offences referred to in the directive is illegal in Slovenia (Article 170-176 of the Penal Code, as well as provisions regarding the accomplice (Article 20), criminal solicitation (Article 37), criminal support (Article 38) and punishability of those soliciting or supporting a criminal attempt (Article 39). Furthermore, the Media Act also prohibits such advertising (Article 47).

Slovenia has not yet developed specific measures to prevent real-time web-based child pornographic performance. The Slovenian police are aware of this topic, also known as live-stream abuse, online-stream abuse or live distant-child abuse (LDCA). The Slovenian police are involved in some international operations on such cases if offenders commit crimes in Slovenia. They as yet have no possibility of performing their own investigations (as identified based on own police activity).

However, Slovenia has implemented various preventive measures, in close cooperation with the Safer Internet Centre Slovenia (www.safe.si):

- A hotline is available at *www.spletno-oko.si* for the public to report illegal content online (such as child abuse material and hate speech). The *Spletno oko* hotline has developed material for the public (leaflets, posters, an annual report and bookmarks) in which it explains how to report illegal content on the internet. Recently, it has also made a video to present the role of the hotline and the possibility of reporting such content.

- The website http://otroci.safe.si/ contains many tips, resources, tools, cartoons and games for children with information on how to use the internet and mobile devices safely and responsibly. Children can also test their knowledge with tests and quizzes. Additionally, the national awareness centre SAFE.SI within the Safer Internet Centre Slovenia also provides offline resources (games, posters, gadgets, leaflets, etc.) for children and young people which are disseminated through workshops at schools, events, fairs, post to all Slovenian schools, other stakeholders' channels, etc. Information and tips for children and young people are also disseminated through relevant media for these target groups. Young people are also reached through the Facebook page of the Awareness Centre SAFE.SI, *'Deskam varno'* (Surfing safely), two Facebook apps, a Youtube channel and the SAFE.SI Twitter account.

- The Slovenian hotline *Spletno oko* has developed resources on illegal behaviour online: a video on measures to prevent child abuse images online, a leaflet on the same topic, a bookmark for wide dissemination, a poster and an annual report. Resources have also been developed on hate speech online, namely a handbook for moderators and editors of web portals, bookmarks, posters, a leaflet and an annual report on this topic.

6.2.4 Actors and measures counteracting websites containing or disseminating child pornography

Slovenia is taking steps towards a notice and take-down approach. The Slovenian national police are making efforts to establish Interpol's initiative, also called Access Blocking. The negotiations and explanations are in progress, and ISPs are more than willing to cooperate. Some gaps are foreseen by the Information Commissioner's Office, which issued opinion No 0712-1/2015/359 on 11 February 2015:

'The Information Commissioner considers that the current provisions of the Electronic Communications Act (ZEKom-1) contain the appropriate conditions and safeguards, which can be used to restrict access to illegal content online. The court decision is requested by the existing Article 203 of ZEKom-1 and by Article 9 of the Electronic Commerce Market Act (ZEPT). It is possible to provide the necessary preliminary judicial review and the balance between the relevant rights and at the same time the limitation of liability of operators.'

Interpol's Access Blocking initiative is completely dedicated to blocking users' access to child abuse material (websites containing images of raped or sexually assaulted children, or victims of crimes against their sexual integrity). More information on this is available at: http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking. Slovenia has not implemented any other measures.

The Electronic Commerce Market Act (Official Gazette of RS, No 96/09 and No 19/15; ('ZEPT'), which transposes into Slovenian legislation Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market, provides the possibility of removing and blocking access to certain web content. In accordance with ZEPT, only a court may order a service provider to remove illegal content or disable access to it, for the purpose of detection and prevention of crime, protection of privacy, and protection of classified information and business secrets. Additionally, Article 203 of ZEKom-1 provides that network operators and internet service providers must endeavour as far as possible to preserve the open and neutral character of the internet by not restricting, limiting or slowing down internet traffic at the level of individual services or applications, or by implementing measures for their degradation. But the third paragraph of Article 203 of ZEKOM-1, which allows for exceptions to the principle of net neutrality, permits court decisions as such an exception, which is also in line with the relevant provisions of ZEPT.

Deleting or blocking access to individual web pages is therefore possible only on the basis of a court order.

Blocking access can be done, for now, only based on a court decision. The removal of content in combination with notice and take-down is performed by the Slovenian police in cooperation with the *Spletno oko* hotline.

When the competent authority in Slovenia, usually the police, identifies a website containing CAM for which the server is located in another country, the police use official communication channels to inform the relevant law enforcement agency. The police suggest that the relevant LEA take the necessary legal action to remove or block the website. The Slovenian police use the official channels SIENA or Interpol i24/7 (ASF).

To investigate related crimes in the child sexual exploitation area in Slovenia, the national police has its own units, at national level – i.e. the Juvenile Crime Section in the Criminal Police Directorate – and regional level – i.e. four Juvenile Crime Groups within the Criminal Police Divisions at the Police Directorate. At the other four Police Directorates where no such units are in operation there are investigators. The total number of investigators is 24: three at the national level, and 21 at the regional level. Given the increased number of cases (see Answer 4(a), in sub-chapter 1) there is a great need for more specialised investigators.

In addition, officers specialised in the investigation of CSE cases also perform other activities and investigations, such as sexual offences against children offline, cyber bullying, domestic violence, child maltreatment, child abduction, missing or kidnapped children, child suicide or attempted suicide, other crimes against children, serious crimes committed by juveniles (14-18 years) and other illegal acts involving minors (less than 14 years).

6.3 Online card fraud

6.3.1 Online reporting

Online card fraud offences in Slovenia are dealt with in accordance with Article 211 of the Penal Code (KZ-1). Such cases relate to unauthorised use of information about payment cards for online payments.

Fraud

Article 211

(1) Whoever, with the intention of acquiring unlawful property benefits for himself or a third person, by false representation or by the suppression of facts leads another person into error or keeps him in error, thereby inducing him to perform an act or to omit to perform an act to the detriment of his or another's property, shall be sentenced to imprisonment for no more than three years.

(2) Whoever, with the intention as referred to in the preceding paragraph of this Article, concludes an insurance contract by stating false information or suppressing any important information, concludes a prohibited double insurance contract, concludes an insurance contract after the insurance or loss event has already taken place, or misrepresents a harmful event, shall be sentenced to imprisonment for no more than one year.

(3) If the fraud was committed by at least two persons who colluded with the intention of fraud, or if the perpetrator committing the offence referred to in paragraph 1 of this Article caused large-scale property damage, the perpetrator shall be sentenced to imprisonment for no less than one, and no more than eight years.

(4) If the offence referred to in paragraphs 1 or 3 of this Article was committed within a criminal association, the perpetrator shall be sentenced to imprisonment for no less than one, and no more than ten years.

(5) If a minor loss of property has been incurred by committing the offence under paragraph 1 of this Article and if the perpetrator's intention was to acquire a minor property benefit, he shall be punished by a fine or sentenced to imprisonment for no more than one year.
(6) Whoever, with the intention of causing damage to another person by false representation or the suppression of facts, leads a person into error or keeps him in error, thereby inducing him to perform an act or to omit to perform an act to the detriment of his or another's property shall be punished by a fine or sentenced to imprisonment for no more than one year.
(7) The prosecution for the offences under paragraphs 5 and 6 of this Article shall be initiated upon a complaint.

What can be understood from the content of this Article is that the police treat offences related to online card fraud offences *ex officio* when they do not result in a minor property benefit (less than EUR 500). If a minor property benefit is gained from an offence, the police initiate a pre-trial investigation on the basis of a complaint submitted by the injured party. Such investigations can be divided into two categories in terms of complaints filed. Cases in which Slovenian citizens are victims of card fraud belong in the first category. In the majority of cases, information about cards is acquired by phishing or hacking information systems and is then used for payments on various websites abroad. In such cases, injured parties report criminal offences to the police themselves. If they report a criminal offence to the bank with which they hold a current account, the bank will refer them to the police.

In cases where payment cards issued by foreign banks are abused on websites in Slovenia, a criminal offence is reported by the bank which has signed a contract with the point of sale where the card was abused. In such cases, banks report criminal offences in accordance with the Protocol signed between the police and the ZBS to the single point of contact (Protocol defined below). The criminal offence is then referred for investigation to the competent regional unit. In accordance with the law, the police inform the injured party after the investigation has been concluded.

The Slovenian authorities also deal with criminal offences where perpetrators acquire payment card recognition information through payments over the entire internet. Such criminal offences are treated in accordance with Article 247 of KZ-1, which also covers the installation of devices that copy information from the magnetic strips on payment cards (skimming) and the use of counterfeit payment cards.

Use of a Counterfeit Non-Cash Payment Means
Article 247

(1) Whoever installs on an automatic cash dispenser or an apparatus for payment by card a device for copying the records of bank or credit cards, or acquires the recognition of such cards through a payment over the whole internet, or makes a forgery thereof in any other way, or whoever uses such a counterfeit bank or credit card and thus gains a property benefit, shall be sentenced to imprisonment for no more than five years.
(2) Whoever forges a card or uses a forged card which enables the gaining of a property benefit by means of technical devices for card recognition shall be punished to the same extent.
(3) If a major property benefit has been gained through the offence under paragraphs 1 or 2 of this Article, the perpetrator shall be sentenced to imprisonment for no less than one and no more than eight years.

When they detect such criminal offences, banks report them to the single point of contact at the police in accordance with the Protocol signed between the police and the ZBS.

The Slovenian police have not detected any problems in acquiring reports on payment card fraud. As already mentioned, banks report suspicion of payment card fraud to the single point of contact, while citizens usually report fraud at the police unit nearest to their residence.

6.3.2 Role of private sector

The Slovenian criminal police successfully cooperate with the ZBS, and in this connection a police representative has already given several lectures as part of training courses organised by the ZBS. The police and the ZBS also organise panel discussions, which are attended by representatives of all the banks and processing centres, who are also contact persons in cases of abuse of non-cash means of payment. These panel discussions allow participants to exchange good and not-so-good practices and experiences among themselves.

The police and the ZBS have concluded a Protocol to ensure effective cooperation between the police and the private sector in cases of abuse of non-cash means of payment. The Protocol puts emphasis on cooperation and measures taken by banks and the police in cases of abuse of non-cash means of payment. The Protocol also covers the exchange of up-to-date information about new payment tools, services, other new developments and possible preventive measures.

The details of contact persons who cooperate and exchange information in cases of abuse of non-cash means of payment are indicated in the Protocol. The obligations of the police and of banks as regards the detection and handling of such criminal offences are also defined in the Protocol.

6.4 Other cybercrime phenomena

As part of the EU FACETRACE project, which aims to improve the facial recognition of perpetrators of criminal acts, the Slovenian criminal police have acquired funds, software and hardware which also serve for investigating criminal acts related to the abuse of non-cash means of payment.

When investigating cases of payment card abuse (including cases of physical payment card abuse), the police use various investigative and technical methods, such as inspecting the location of criminal acts, securing devices used to copy information from the magnetic strips on payment cards (skimming), looking for papillary and biological traces on devices, carrying out technical inspections of devices and securing data from devices. The Slovenian police focus on investigating devices, as conclusions and data acquired from such devices can significantly contribute to clarifying a criminal act. By using the currently available software and hardware, the police are capable of acquiring data from seized skimming devices which is important for investigations of this kind. However, since the technology used in skimming devices is constantly evolving, it would without a doubt be sensible to upgrade the equipment used by forensic investigators.

During investigations into criminal offences of fraud related to non-cash means of payment, the police discovered that there are lone individuals in Slovenia who belong to organised criminal groups and are recruited to commit specific criminal offences. The offenders, who are mainly from foreign countries (Romania, Bulgaria and Macedonia), install skimming devices on cash dispensers in Slovenia. In the next step, they forward the credit cards' magnetic strips to the members of the gang who operate abroad or in countries where the EMV standard is not applicable. There, credit cards with identical magnetic strips are made and used for cash withdrawals at cash dispensers or for fraud at points of sale (POS terminals). In recent years, the police have noted that exploitation of credit cards, the data of which was acquired at cash dispensers in Slovenia, occurs mainly in the USA, Thailand, Indonesia, Bolivia, the Philippines and Columbia. Slovenian banks suffer damages from these frauds.

Slovenian processing centres control and prevent credit card fraud and control and monitor transactions for banks. In most cases, the processing centre discovers as part of the transaction monitoring that a large number of Slovenian holders' credit cards have been used abroad at a certain cash dispenser or POS terminal in a short period of time. After the discovery of the suspicious transactions abroad, it tries to find a common point. This is done by checking at which cash dispensers the credit cards had previously been used and notifying the card-issuing bank of the suspicion of fraud. The bank immediately cancels all credit cards that were used during a certain period at the cash dispenser on which it is suspected that a skimming device had been installed. The police are also notified of the criminal offence.

Slovenian banks introduced EMV protection for cash dispensers in Slovenia in 2011 and also provide anti-skimming equipment for cash dispensers. Certain banks have decided to block the use of Slovenian credit cards in countries where the EMV standard is not applicable (GEO-blocking) in order to prevent fraud. The 3-D Secure international security standard supported by MasterCard ('MasterCard SecureCode') and Visa ('Verified by Visa') is increasingly being introduced to online points of sale and is used to verify card users' identity for online payments.

6.5 Conclusions

- The Slovenian police have dedicated structures and resources in place to deal with both child sexual abuse and card fraud. During the on-site visit, the evaluation team appreciated the knowledge and commitment of the officers and the results presented.
- Police officers in charge have taken part in successful international operations against malware producers.
- Measures to prevent child sex tourism and other forms of child sexual abuse are mainly based on productive cooperation with NGOs. However, the implementation of Directive 2011/93/EU should be improved, as suggested by the Slovenian police.
- Slovenian police resources and tools for dealing with encrypted data are very limited and should be enhanced to allow for better investigation outcomes. After the on-site visit the evaluation team was informed that more equipment has been purchased in 2016.[12]
- Regarding cyber attacks, it is not clear what level of cooperation takes place between the authorities in charge of cyber security and those in charge of the fight against cybercrime.[13]

[12] The Slovenian police take the necessary steps towards increasing cyber knowledge, such as the execution of the action plan of Internal Security Fund (ISF-P) in the period 2016-2020. There are different activities planned in the next two years, including specialisation and education in the field of prevention and investigation of criminal offences. Objectives are to achieve better knowledge and practical use of investigation techniques and procedures regarding the criminal offences concerned.

[13] The evaluation team was informed after the on-site visit that the police cooperate with SI-CERT at a high level and regularly attend NATO's annual Cyber Coalition exercises. In 2016 the police cooperated with ENISA in the framework of the "European Cyber Security Month" on cyber incidents. Moreover, we cooperate with some private companies and educational institutions dealing with information security. At present there are no other specialised agencies dealing with cyber information security in the Republic of Slovenia. Should a national cyber security authority and a government agency (GOV-CERT) be established, the police will cooperate with those agencies as well.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

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

Cooperation with the Europol/EC3 agency is carried out based on Article 117 of the ZNPPol. As a full member of Europol, Slovenia is committed to passing on all information related to criminal offences which fall under the Europol mandate as set out in the EU Council Decision establishing Europol. Offences in the field of computer crime are among those mentioned. The exchange of information with Europol is carried out via the SIENA safe line.

Once a year, the Slovenian Agency for Communication Networks and Services informs ENISA of the cyber security incidents reported by operators during the year. It also notifies ENISA when cyber security incidents of large proportions occur.

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

The International Police Cooperation Division of the Directorate of Criminal Police is only authorised to exchange information with Europol, while the Computer Investigation Centre and other departments within UKP GPU are authorised to investigate criminal offences. The International Police Cooperation Division of the Directorate of Criminal Police assessed that cooperation with Europol/EC3 works very well. The mutual exchange of information is carried out promptly.

Europol, jointly with the EC3, provides trend assessments, which can be used to obtain future predictions and an overview of the criminal activities of organised criminal groups.

The Slovenian police successfully cooperate with Europol/EC3 and assess their contribution and cooperation as very good. The information exchange is relatively fast (mostly in comparison with other such instruments) and information is up-to-date and often useful for cybercrime investigations. The Slovenian police also cooperate in FP Cyborg, Twins and Terminal, where Europol contributes its share of information. Europol/EC3 organised operational meetings in some criminal cases, in which Slovenian police representatives participated and which allowed for a direct exchange of operational data and evidence (including digital evidence).

The Slovenian authorities recommend that more opportunities to visit the EU Member States be provided, especially visits to those Member States which lack experience, knowledge or capacity, in particular with respect to the cybercrime area, e.g. child sexual exploitation online.

The International Police Cooperation Division of the Directorate of Criminal Police suggests promptly sending all information from the field of computer crime which falls under the Europol/EC3 mandate to Europol for verification. Only through prompt information exchange can Slovenian criminal investigations be expected to benefit from the added value of Europol/EC3.

The Slovenian police use the ICSE database to perform their investigations in order to identify victims of CSE. At the time of the on-site visit, Slovenia was not yet connected. The Slovenian police had used the standard official channel (CD/DVD, hard disk) to send CAM to the ICSE database. After the on-site visit the evaluation team was informed that the direct access to ICSE database was established.

Through the international cooperation sector, which also includes the National Central Bureau of Interpol Ljubljana, the Slovenian police send requests regarding the verification and use of Interpol's ICSE database to the Interpol General Secretariat, but the competent service at the general crime sector has not yet established direct access to this international database. At the time of the on-site visit talks about this were already under way. After the on-site visit the evaluation team was informed that the Slovenian police established direct access to Interpol's ICSE database on 29 October 2015.

Slovenia does not participate in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol or in other forms of practical cooperation (including 'cyber patrols'). However, it participates in cyber patrols as part of the activities of the fast response team, which includes cyber crime.

7.1.3 Operational performance of JITs and cyber patrols

Slovenia is gathering experience of patrolling the internet within the EMPACT 'Crime priority G3 – Cyber Attack' OA 1.5 project. Cooperation within the activities of the group for rapid operation of so-called internet patrolling is included in cybercrime. Some of the activities are concerned with defining the group's purpose, goals, procedures and technical preparation, as well as with putting procedures into practice and examining the legal bases. Other Member States that had previously not cooperated in the group joined the group operation in 2015. The group thus increased from 11 to 17 states, meaning that the issues discussed are of interest to a broader range of states and that the operation of the group is focused on issues which include the activities of all Member States. An 'Open Source Compendium' user manual dedicated to open source investigations was drafted within the group. It is focused on the investigation of activities on the Facebook social network and should be kept up-to-date, expanded and adapted. Other materials dedicated to cybercrime investigations should be developed in a similar way.

At the moment, Slovenia's investigators and prosecutors cooperate in the Eurymus JIT (EJ ID 19714) common investigation group within Eurojust, in which the United Kingdom, Romania and Finland also participate. The experience has been very positive, since the exchange of data, information and evidence is more efficient (faster and of higher quality). Cooperation in the Eurymus JIT (EJ ID 19714) common investigation group is completely financed by Eurojust.

Units dedicated to the CSE area have not yet participated in a JIT.

Slovenia tried to apply for the 'INTERNAL SECURITY FUND POLICE (2014-2020) CALL FOR PROPOSALS HOME/2014/ISFP/AG/CYBR – HIFIGHTING CYBERCRIME AND CHILD SEXUAL ABUSE' EU project, but ultimately did not join the project because the partner states did not respond. Part of the planned equipment has therefore been financed through the national ISF fund.

Slovenia actively cooperates within the EMPACT 'Crime priority G3 – Cyber Attack' OA 1.5 project.

The Republic of Slovenia stated that it had had positive experiences with common investigation groups, and would therefore support such forms of operational cooperation as much as possible.

7.2 Cooperation between the Slovenian authorities and Interpol

The Slovenian authorities assess the cooperation via the Interpol channel to be good, insofar as the Member States cooperate within Interpol according to their national legislation. The Slovenian police use the Interpol channels for pre-trial procedures of criminal investigations related to non-cash means of payment if they find references to third party states. They ask third party states to provide certain data which is important for the clarification of circumstances in the pre-trial procedure via Interpol in the form of a notification or request. The Slovenian authorities cooperate well with Interpol in such cases, but the acquisition of information depends on the national legislation of the country to which the request is addressed. It must be emphasised that, to identify suspects on the basis of their IP identification for various criminal offences in individual cases that need a fast response, it is often necessary to go through quite complicated national data acquisition procedures. It is therefore rare for the offender to be identified, especially if the chaining procedure is established.

To acquire data such as video surveillance camera records, IP address ownership or transaction accounts, international legal aid is needed in most cases. In these cases, the police give the initiative to the responsible judicial authority (prosecution) with a proposal to ask a foreign judicial authority of a certain country to conduct certain activities or acquire the required documentation on the basis of the international legal aid. The use of such a procedure to acquire data extends the investigations.

In April 2015, Interpol opened the Global Centre for Innovation in Singapore, which is to include the field of computer crime in its activities. The opening of this centre will provide an additional tool for solving criminal investigations in the field of computer crime on a global level.

The Slovenian police have had excellent experiences with the Crimes against Children Unit at GS Interpol Lyon. This trust-based cooperation is consolidated through victim identification processes (VID), and the exchange of intelligence, training, knowledge, modus operandi and assistance in connecting with relevant investigators in third countries (e.g. Brazil) in concrete operations.

7.3 Cooperation with third states

In investigations of criminal offences related to cybercrime, the Slovenian police collect all information and notifications related to the offences themselves. If it is clear from the way the offence was committed and from the established facts that the investigation is connected to third party states, all gathered information is passed to the states in question. There they make use of the International Police Cooperation Division, which notifies the states or requests the acquisition of data needed for pre-trial procedures via Europol's or Interpol's official channels.

In the experience of the Slovenian police, the involvement of Europol/EC3/Eurojust has brought real added value to cases related to third countries, in particular through the provision of opinions on the trends collected by third countries, especially with the FVEY countries which are bound by their multilateral agreements.

According to the Slovenian authorities, the cases concerned were concluded fairly successfully. However, the time frames are significantly longer than in cooperation within the EU, since no institutional instruments exist to accelerate cooperation in the region mentioned. The success of police investigations is often related to informal connections within international police cooperation. Europol (EC3) and other Member States cooperating under the EMPACT project try to acquire the cooperation of third party states through common measures, where Slovenia also sees the added value.

The Slovenian police have had a positive experience of cooperating with Europol in connection with criminal investigations into abuse of non-cash means of payment. They gather confirmations and results from Europol via the SIENA safe line about concrete issues, which refer to the data inputted in the mentioned analytical dossiers. Foreign security authorities are notified at the same time. In their opinion, such cooperation with Europol has additional value for investigations since it allows investigators to get in contact and cooperate through operational meetings. It also provides help with analysis and the possibility of getting in touch with those responsible for such investigations in third party states.

Slovenia emphasised the example of good practice of the ROVER operation in 2011-2013, when the Slovenian police acquired notifications during the pre-trial procedure referring to bigger criminal offences related to the installation of skimming devices on cash dispensers in the Ljubljana area. They promptly notified Europol and AWF (present FP) Terminal about the findings, according to the directions. The Terminal analysed the gathered information and discovered that it concerned an organised gang operating across Slovenia, Croatia, Macedonia, Bosnia and Herzegovina and Bulgaria. In the described case, Europol organised an operational meeting for the above states to exchange the findings of their investigations. Following this information exchange, the suspect was arrested in the territory of the Republic of Croatia.

7.4 Cooperation with private sector

Some of the responsibilities of service providers are defined in Articles 8 to 11 of the ZEPT, e.g.:

- Service providers are responsible for the data provided by the recipient of the service according to the provisions of this law (Article 8).
- Service providers are responsible for the data they issue as part of the provision of the information society service, according to the general rules of obligation and criminal law (Article 8).
- Within three days of the receipt of a request from any responsible authority, service providers must provide data on the basis of which it is possible to identify the recipients of their service (name and surname, address, company, e-mail address) (Article 8).
- Where an information society service is provided that consists of the transmission via a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the service provider is not liable for the information transmitted, on condition that the provider does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained in the transmission (Article 9).
- Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider is not liable for the information stored at the request of a recipient of the service, on condition that the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, or, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information (Article 11).

ZEPT, which transposes into Slovenian legislation Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market, provides the possibility of removing and blocking access to certain web content. In accordance with ZEPT, only a court may order a service provider to remove illegal content or disable access to it, for the purpose of detection and prevention of crime, protection of privacy, and protection of classified information and business secrets. Additionally, Article 203 of ZEKom-1 provides that network operators and internet service providers must endeavour as far as possible to preserve the open and neutral character of the internet by not restricting, limiting or slowing down internet traffic at the level of individual services or applications, or by implementing measures for their degradation. But the third paragraph of Article 203 of ZEKom-1, which allows for exceptions to the principle of net neutrality, permits court decisions as such an exception, which is also in line with the relevant provisions of ZEPT.

Deleting or blocking access to individual web pages is possible on the basis of a court order. The Slovenian police have had positive experiences and cooperate well with service providers, mainly in blocking and removing CAM (child abuse material).

There is currently no cooperation with private companies having their main headquarters in a third state, but the Slovenian police are drawing up arrangements with Microsoft Slovenia and preparing to sign a contract on mutual cooperation (Government Security Programme Agreement).

In the CSE area, Slovenia reported the problem of insufficient responses from bigger corporations in the USA, which are not willing to cooperate in data sending procedures (users), even when a competent Slovenian authority issues a court decision on a particular case. Sometimes the corporations do not respond, and often they reply that they no longer have the data, or that the child in question is not in real danger (in the case concerned, in 2014, two young girls were in serious danger and a court order had to be delivered to obtain the data).

In the investigation of criminal offences related to online credit card fraud, the Slovenian police collect all information and notifications related to the offences themselves. If it is established that the investigation is connected to other states, the police pass all the gathered information to the states in question. The information is sent in the form of a request or notification via the International Police Cooperation Division, which notifies the states or requests the acquisition of the data needed for pre-trial procedures via Europol's or Interpol's official channels.

In cases of criminal investigations into non-cash means of payment fraud, the FP Terminal analytical dossier is notified. In addition to official channels, Slovenian practitioners also use direct contacts acquired during various official trips and training courses abroad. They also cooperate in the EMPACT European project in the field of cybercrime card fraud, which aims to bring about systematic improvements in credit card fraud investigations in the EU region and in the operational issues in this field.

7.5 Tools of international cooperation

7.5.1 Mutual legal assistance

Mutual legal assistance in general (MLA, transfer of proceedings, transfer of the execution of a sentence, and extradition) is regulated by the Criminal Procedure Act (ZKP), the Act on cooperation in criminal matters with Member States of the European Union (ACCMEU-1), and the Forfeiture of Assets of Illegal Origin Act. The provisions of the Criminal Procedure Act are applicable according to the principle of subsidiarity, i.e. only if there is no international legal instrument or if the provisions of the instrument do not regulate specific issues. Essentially, the basic constitutional principle (Article 8 of the Constitution of the Republic of Slovenia) of precedence of ratified conventions over national law is also valid for MLA in criminal matters.

Furthermore, the Criminal Procedure Act explicitly states that MLA should be administered pursuant to the provisions of that Act unless provided otherwise by international agreements. This principle enables the direct use of international agreements (such as the Convention on Cybercrime and bilateral treaties) in cases of different regulation of a certain question in national legislation versus an international agreement. There are no specific provisions in Slovenian national legislation on MLA for cybercrime, since general provisions on MLA are applicable.

Cooperation with the Member States of the European Union

Judicial cooperation between the competent authorities of the EU Member States is regulated by the ACCMEU-1, which incorporates all adopted instruments of mutual recognition in criminal matters and relevant procedural provisions regarding mutual legal assistance, transfer of proceedings and cooperation with entities such as Eurojust and the European Judicial Network. The main goal of this Act is to enable smoother and faster cooperation as well as to simplify and accelerate procedures. Therefore, the ACCMEU-1, in connection with relevant multilateral instruments (such as the Schengen Convention, and the Convention established by the Council in accordance with Article 34 of the Treaty on European Union on Mutual Assistance in Criminal Matters between the Member States of the European Union) enables direct communication between the judicial authorities of EU Member States.

Cooperation with third countries

MLA with third countries is regulated by the ZKP. According to the ZKP (Article 515), mutual legal assistance requests are transmitted through the diplomatic channel. The Ministry of Foreign Affairs transmits passive requests through the Ministry of Justice (central authority) to the competent Slovenian authorities, i.e. courts or state prosecutor's office (passive mutual legal assistance requests).

Active requests are transmitted from the competent Slovenian authorities to the Ministry of Justice (central authority) and then through the diplomatic channel to the responsible foreign authorities. The procedure through the Ministry of Foreign Affairs and the Ministry of Justice is carried out as swiftly as possible, usually in no more than a day or two. In practice, the requests are generally submitted directly through the central authority (MOJ) on the basis of bilateral treaties as well as multilateral treaties, which define the Ministry of Justice as the central authority and enable communication through central authorities. Direct communication between domestic and foreign judicial authorities is regulated by Article 515(3) of the ZKP:

'(3) If reciprocity applies or if so determined by an international treaty, international legal aid in criminal matters may be exchanged directly between the domestic and foreign bodies participating in the pre-trial procedure and criminal proceedings. In this, modern technical facilities, in particular computer networks and devices for the transmission of picture, voice and electronic impulses, may be used.'

The competent authorities for the execution of requests for MLA stand at district court level - investigative judges or district prosecutors' offices, depending on the requested investigative measure. The competent authorities for the issuing of MLA requests are local and district courts, district prosecutors' offices and the Specialised State Prosecutors' Office.

The Slovenian authorities stated that they are not in a position to provide detailed statistics on MLA requests, since criteria such as the outcome of the request, the duration of the procedure, the specific criminal offence or the specific investigative measures are not included in the statistics. The Ministry of Justice only collects general information regarding MLA with third countries for the yearly statistics, since cooperation between the competent judicial authorities of EU Member States is carried out directly.

There are no specific procedures or conditions that need to be fulfilled as regards the various categories of MLA requests related to cybercrime, since general provisions on the procedure and conditions for MLA are applicable. The courts comply with a mutual legal assistance request if the execution of the measure would not be in conflict with the legal order of Slovenia and would not prejudice its sovereignty and security.

Requests for MLA are executed in accordance with national legislation, but the Slovenian authorities may also comply with the formalities and procedures expressly indicated by the requesting Member State, provided that such formalities and procedures are not incompatible with the fundamental principles of the national criminal system.

Measures that are considered as coercive according to the ZKP, such as house searches and personal searches (Articles 214-219 ZKP), the confiscation of objects (Articles 220-224 ZKP), secret surveillance (Article 149a ZKP), electronic surveillance (Article 149b ZKP), surveillance and monitoring of communications including phone tapping (Article 150 ZKP), listening and surveillance of the home of a person (Article 151 ZKP), controlled delivery (Article 155 ZKP), undercover operations (Article 155a ZKP) and the lifting of banking secrecy (Article 156 ZKP), must be implemented according to the requirements of Slovenian law, which in most cases lays down a requirement for a judicial order and some additional requirements.

All MLA and extradition requests that are transmitted through the Ministry of Justice are dealt with in accordance with the principles of procedural efficiency and rapidity and are transmitted either to the competent Slovenian or foreign authorities as soon as possible, usually in no more than a day or two.

The average duration of MLA proceedings in the Republic of Slovenia is 1-2 months, but their duration depends on several factors, such as the urgency of the case and its complexity and extensiveness.

With respect to cybercrime, assistance is possible at all stages of the proceedings and for all investigative or procedural measures (hearings, service of documents, obtaining bank information, expert evaluations, tracing of telecommunications, identification of users of telecommunications, interception and recording of telecommunications and other forms of communication, interception of e-mails, search and seizure, confiscation, etc.). Tracing of telecommunications and identification of users of telecommunications are the most common reasons for MLA requests with respect to cybercrime.

The Slovenian authorities do use informal pre-MLA consultation with the respective competent authorities of the other Member States in relation to cybercrime. They communicate via the European Judicial Network or Eurojust.

To date they have not encountered any specific problems in providing/requesting MLA assistance for offences committed in the 'cloud'.

The agreement between the European Union and the US on mutual legal assistance in criminal matters in relation to the USA is in use. Requests for MLA have been addressed to the competent US authorities in order to trace telecommunications and identify users of telecommunications. The only difficulty is that the competent US authorities execute the requests of the competent Slovenian authorities on average within six months to one year, which is quite lengthy.

7.5.2 Mutual recognition instruments

It is the understanding of the evaluation team that, as yet, Slovenia has no experience in the use of EU mutual recognition instruments in relation to the fight against cybercrime.

7.5.3 Surrender/extradition

EAW

In accordance with Article 9 of the ACCMEU-1, surrendering a person on the basis of a warrant is admissible if the warrant is issued for acts punishable by the law of the issuing Member State by deprivation of liberty for a maximum period of at least one year, or for the purpose of enforcing a custodial sentence, safety measure or other measure imposed by a criminal court involving deprivation of liberty for at least four months, and if the act for which surrender is requested is also considered a criminal offence under the national penal code (double criminality). Double criminality should not be verified if a warrant is issued for a criminal offence punishable under the law of the ordering Member State by deprivation of liberty for a maximum period of at least three years, and if such a criminal offence is classified under the law of such state as, for example, computer-related crime, among other categories.

Extradition

With regard to the minimum penalty under Slovenian national law, Article 522 of the ZKP provides that, in the event of extradition for the purpose of criminal prosecution, a prison sentence of one year or more or a security measure lasting over one year may be imposed for the offence under the law of both states. Furthermore, in the event of extradition for the purpose of the execution of a final sentence or security measure, the sentence or security measure and/or the remainder of such a sentence or security measure to be carried out must be at least four months.

The wording ‘may’ be imposed is interpreted as referring to the maximum penalty of the relevant offences.

The maximum penalties for computer-related offences (such as 'attack on information systems' - Article 231 of the Penal Code, 'information system abuse' - Article 237 of the Penal Code, 'solicitation of persons under fifteen years of age for sexual purposes' - Article 173a of the Penal Code, 'abuse of personal data' - Article 143 of the Penal Code and 'presentation, manufacture, possession and distribution of pornographic material' - Article 176 of the Penal Code) are between one and eight years, which means that, according to Slovenian national law, all criminal offences of computer-related crime fall under the scope of the EAW list and are extraditable.

The authority responsible for sending/accepting surrender/extradition requests is the Slovenian judicial system, which also takes decisions on transfer/extradition. The judicial authority then notifies the International Police Cooperation Division of its decision by a decree, as it represents the National Central Bureau which, in the event of a positive response, will conclude an agreement with the responsible foreign police via the adequate information channel (Interpol or Schengen information system II).

Cooperation with EU Member States - surrender

As mentioned above, the legal basis for the cooperation is the Act on Cooperation in Criminal Matters with the Member States of the European Union (ACCMEU-1), as well as relevant international instruments. The ACCMEU-1 implements all mutual recognition instruments adopted within the EU. Consequently, the extradition procedure has been replaced by the surrender procedure on the basis of Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

Issuing authorities: The judicial authorities in the Republic of Slovenia competent to issue a European arrest warrant are local courts (*okrajna sodišča*) and district courts (*okrožna sodišča*). Local courts are competent in cases of criminal offences carrying as principal penalty a fine or a prison term of up to three years, while the jurisdiction of district courts covers the rest of the decision-making in the first instance.

Executing Authorities: The judicial authorities in the Republic of Slovenia competent to execute European arrest warrants are district courts.

Cooperation with third states

Articles 521 - 536 of the Criminal Procedure Act (ZKP) focus on extradition and envisage detailed solutions regarding the conditions for extradition and for subsequent proceedings (applied in accordance with the principle of subsidiary).

Passive procedure

The extradition request is received through the diplomatic channel. The Ministry of Foreign Affairs transmits it through the Ministry of Justice to the competent court. If so prescribed by the international treaty the extradition request could be forwarded directly to the Ministry of Justice as a central authority. The extradition procedure is divided between judicial authorities (competent courts) and the administrative authority (Ministry of Justice) and is consequently two-phased.

Active procedure

Competence for the submission of the request for extradition or provisional arrest lies with the Ministry of Justice, but the request may only be submitted on the motion of the competent court, which is also responsible for preparing the extradition documentation.

As cooperation between the competent judicial authorities of EU Member States in the field of surrender procedure under Council Framework Decision 2002/584/JHA of 13 June 2002 is direct, the Slovenian courts dispose of information on the surrender procedure. Therefore, they will be contacted to provide statistics on the number of requests as regards EU Member States.

Third countries

Three requests for extradition have been received by the US authorities under the Agreement between the Government of Slovenia and the Government of the USA comprising the instrument as contemplated by the Agreement on extradition between the European Union and the USA of 25 June 2003 (one in 2013 and two in 2014). The first request was related to the criminal offences of access device fraud, aggravated identity theft and wire fraud under US law (computer-related fraud and a computer-related identity offence). The second request was related to the criminal offence of illegal access to an information system. The third request was related to the criminal offence of wire fraud under US law (computer-related fraud).

There are no specific procedures or conditions that need to be fulfilled as regards requests related to cybercrime, since general provisions on extradition are applicable.

Extradition cases are dealt with as a priority, since in most cases extradition detention is ordered. Consequently, the extradition documentation is sent to competent judicial authorities on the same day that the Ministry receives it or the day after at the latest. Requests for extradition and decisions of the Minister for Justice on extradition are transmitted or issued with the same rapidity - consequently, if no translation and no additional information is required, requests and decisions are transmitted or issued within one to two days.

Provisional detention and extradition detention are regulated in the ZKP. Detention is not mandatory and may only be imposed if a reasonable suspicion exists that a person has committed a criminal offence, if they are in hiding, if their identity cannot be established or if other circumstances exist which point to the danger of a flight attempt, if there is reasonable ground for concern that they will destroy the traces of crime or if specific circumstances indicate that they will obstruct the progress of the criminal procedure by influencing witnesses, accomplices or concealers, or if the seriousness of the offence, or the manner or circumstances in which the criminal offence was committed and the person's personal characteristics, history, environment, living conditions or other personal circumstances indicate a risk that they will repeat the criminal offence, complete an attempted criminal offence or carry out a threat of a criminal offence. As an alternative to the extradition detention, other measures may be imposed to ensure the presence of the accused, such as bail, house arrest or reporting to a police station.

Provisional detention may be imposed for a maximum period of three months, with an extension of another two months due to special circumstances, by a panel of three judges of the district court. As stated above, in practice extradition detention is ordered in most cases.

The Agreement on the surrender procedure between the EU Member States, Iceland and Norway has never been used by Slovenia in relation to cybercrime.

7.6 Conclusions

- Slovenian practitioners are willing to cooperate as much as they can and are asked to. Slovenia's experiences concerning cooperation with other Member States and with or through EU competent bodies does not raise any problematic issues and meets normal standards.
- At police level, they actively contribute to and benefit from opportunities for information exchange and sharing provided by the competent EU agencies.
- Slovenia experiences limitations/obstacles in cooperation with third country-based electronic services providers, which are similar in nature and result in similar consequences as in other Member States.
- The Slovenian authorities are still applying traditional legal MLA standards for new types of crime, such as cybercrime. The relevant provisions of the CoE Cybercrime Convention (e.g. Article 25, section 3) are also used such as in the referred international investigation called "Iserdo" and "Mariposa", in which the Slovenian police cooperated at a high level with the US FBI, Spanish and Canadian authorities, the authorities of the Serbian Republic and other law enforcement authorities. According to the police assessment, the provisions of the Convention on Cybercrime are in general not sufficiently applied by the states signatories. In addition, the Slovenian authorities reported that in practice, all MLA requests regarding cybercrime that are addressed to the competent foreign authorities (mostly USA) are transmitted by e-mail as well as communications related thereto. In order to accelerate the MLA procedures, communications via contact points of the European judicial network and members of the EUROJUST are used. The competent judicial authorities as well as the Ministry of Justice accept and respond to the requests that are communicated by e-mail or fax. Furthermore, modern technologies, such as video conference, are often used in criminal procedures instead of »standard« MLA requests for hearing of witnesses and suspects by the requested courts. For that purpose, all the Slovenian courts have the necessary equipment to conduct video conferences. Video conferences with a number of judicial authorities of different countries have thus been conducted, for instance with Australia, USA, UK, etc. Thus, the Slovenian judicial authorities (courts and prosecutors) can communicate directly with the judicial authorities of EU member states.

8 TRAINING, AWARENESS RAISING AND PREVENTION

8.1 General and specific training

Since its establishment in 2009, the Computer Investigation Centre has been implementing individual training programmes (or educational modules) for forensic investigators on the basis of two verified programmes, i.e.:

- computer crime investigation – basic training (280 hours; implemented when needed),
- computer crime investigation – advanced training (40 hours; implemented three to four times a year with different content).

In 2014, upgraded educational modules were prepared and divided into:

- computer investigation – introductory training (40 hours),
- computer investigation – basic training (80 hours),
- computer investigation – advanced training (organised twice; 40 hours each),
- computer investigation – specialist training (40–200 hours).

Educational modules are currently being verified. When the investigators complete the basic training course, they thus meet legal and formal conditions of professional competence and may begin conducting procedures of electronic device protection and investigation independently.

The Computer Investigation Centre also organises five-day (40-hour) specialist and advanced courses for forensic investigators where they become familiarised with individual topics in the field of cybercrime investigation in more detail.

The Slovenian police have a forensic investigator who deals with the investigation of devices for capturing data from the magnetic strips on payment cards, or 'skimming devices'. They make every effort to ensure that this investigator is as qualified as possible for this type of investigation. At the invitation of Europol within the EC3 Group (European Cybercrime Centre), this investigator thus attended the training course on forensic investigation of skimming devices which was organised at the headquarters of the German Federal Criminal Police Office (BKA – *Bundeskriminalamt*) in Wiesbaden in 2013.

The Computer Investigation Centre at the Criminal Police Directorate is responsible for the organisation and implementation of training relating to cybercrime, in cooperation with the Police Academy of the General Police Directorate.

As a rule, investigators attend the CEPOL conferences three or four times a year, but the contribution of the ECTEG and Eurojust/EC3 to the training of law enforcement authorities in Slovenia is minimal.

Participation in four residential training courses is planned for 2015:
- activity no 14/2015: 'Combating child sexual exploitation on the internet through undercover activities' between 21 and 24 September in Budapest, Hungary;
- activity no 15/2015: 'Train the trainers to combat child sexual exploitation on the internet' between 22 and 26 June 2015 in Belgium;
- activity no 16/2015: 'First responders and cyber forensics' between 8 and 12 June 2015 in Tallinn, Estonia;
- activity no 17/2015: 'Cybercrime – Strategic' between 25 and 27 March 2015 in Jurmala, Latvia.[14]

[14] After the on-site visit the evaluation was informed that the Slovenian police, depending on the capacities (financial, personnel) also attended training courses in the area of cybercrime organised by OLAF, Europol/EC3 (Focal Point Cyborg and this year also EUCTF), as well as by ILEA and ECTEG. In addition to other activities, the Slovenian police – Criminal Police Directorate of the General Police Directorate – also take active part in the four-year policy cycle (2013-2017) regarding the issue of IOCTA (Internet Organised Crime Threat Assessment). This is Europol's project EMPACT (European Multidisciplinary Platform against Criminal Threats), with projects defined in Operative Action Plans in three sub-priority areas of cybercrime: CA (Cyber - attack), CSA (Child sexual exploitation) in CCF (Cybercrime card frauds).

The Criminal Police or the Computer Investigation Centre and its departments organise individual training courses for police officers who deal with cybercrime in their work as such needs arise. These are specific and target-oriented training courses where investigators are provided with the concrete solutions that they need in their work. These short training courses take 8 to 16 hours (1-2 days).

Training courses for criminal police officers working within computer investigation departments at Police Directorates are also arranged periodically (half-yearly), to introduce the participants to new technologies, new methods of committing crimes and other developments. These training courses usually last five working days. Prompt assistance in concrete cases is provided to criminal police officers if possible.

Discussions are under way to organise training for judicial authorities (state prosecutors and judges) to familiarise them with police procedures implemented when protecting and investigating information. At the time of the on-site visit no such training courses have been conducted as yet.[15]

In 2014, the police implemented a new three-day training initiative, Digital Days, which will become a regular form of training in the field of cybercrime. There are plans for other state bodies, non-governmental organisations, universities and the private sector to also participate in this training.

[15] After the on-site visit the evaluation team was informed that the police conducted two one-day seminars on cybercrime and digital evidence for prosecutors and judges, and we will respond to all future requests to that effect by judicial authorities.

Training in the field of online child sexual abuse is also a regular form of police training which is being implemented independently or in cooperation with other competent institutions. Nationally, annual training courses/conferences are held between LEAs and the judiciary, as well as specific training for LE officers (annually, on a specific topic, e.g. certification on the usage of Interpol's ICSE database).

Internationally, Slovenia sends one participant to attend Europol's COSEC training course in Selm, Germany, almost every year. In addition, ten officers have been trained at the FBI training course on CSE in Budapest (January 2015), as well as two officers at the European Financial Coalition training course on ways of investigating sexual abuse of children by misuse of financial instruments (Paris, 2014; Budapest, 2015) and the EU KIRAT system (twice in 2015, April and November).

The topic of cybercrime is encompassed in the 'Criminology' course, which takes 65 hours (of which 10 hours are dedicated to cybercrime) of the basic training programme for new criminal police officers (criminal police investigation training course).

There are no national centres of excellence in the Republic of Slovenia.

The Police Academy implements a higher education programme, 'Police Officer', where police officers are trained to conduct their work on the basic level. There are no plans to include special courses on cybercrime within this programme. Following the evaluation of the study programme, there are plans to introduce certain informative content on cybercrime to the criminology course.

Within its educational programme, the Jožef Stefan International Postgraduate School implements a study programme on computer forensics.

The University of Maribor features two courses relating to cybercrime:

Within its professional higher education study programme on 'Information Safety', the Faculty of Organisational Sciences features in its syllabus:

- organisation and management of information systems,
- information system security.

Within its professional higher education study programme on 'Information Safety', the Faculty of Criminal Justice and Security features in its syllabus:

- information security: management, standards and digital identity,
- data protection and computer forensics.

The faculties of the University of Ljubljana offer two courses relating to cybercrime:

- The Faculty of Computer and Information Science features a study course referring to cybercrime, 'Computer Forensics – Digital Forensics'.
- The Faculty of Social Sciences offers a course on 'Information Science for Defence Studies' (within the undergraduate programme of 'Political Science - Defence Studies') which covers the influence of information technology on the development of security policies.
- The Faculty of Social Sciences covers the topics of 'Organisation and management of information systems' and 'Information security: standards and digital identity' as part of the e-Business course (within the professional higher education course on Social Informatics, Undergraduate Programme of Social Informatics).

Centre for Judicial Training within the Ministry of Justice

The Centre for Judicial Training within the Ministry of Justice of the Republic of Slovenia is responsible for the organisation of education and training for the judiciary. In this capacity, it arranged the videoconference on cyber crime.

The budget of the Centre for Judicial Training within the Ministry of Justice for criminal law judges, judges for minor offences and public prosecutors was EUR 60 000 in 2014. Annual costs for training in the field of cybercrime amount to between EUR 2 500 and EUR 3 000.

In April 2014, the Centre for Judicial Training organised, in collaboration with the Embassy of the United States of America, a videoconference on the topic of cybercrime, which was attended by 14 judges and prosecutors, and 3 police officers. The 3-hour lecture was given by an American expert in this area, Arnold Bell, and chaired by Igor Bernik from Ljubljana's Faculty of Security Studies.

No special training is organised (or planned) for persons participating in the process of international cooperation.

8.2 Awareness raising

Slovenia runs two awareness-raising programmes. The *Safe on the Internet* programme, which is also part of the European Union advocacy campaign called European Cyber Security Month, is aimed at a wide public, with specific content for SMEs. The other programme, SAFE.SI, is aimed primarily at younger generations.

In 2011, the Slovenian national CERT (Computer Emergency Response Team) took over the coordination of the national project aimed at raising public awareness on information security, ***Safe on the Internet***. The number of reported online scams has been increasing since 2009. A growing number of users are being targeted each year with social-engineering attacks. SI-CERT continue to receive more and more reports concerning identity theft, stolen passwords, and Nigerian and lottery scams. This indicates that internet users in Slovenia need clear, precise and understandable instructions on how to protect themselves. This was the main motive in launching the awareness-raising programme ***Safe on the Internet***.

The project was financed by the Information Society Directorate of the Slovenian Ministry of Education, Science and Sport and currently is co-financed by the Ministry of Public Administration. It has been envisaged as a long-term activity, with the main objective being to help improve the information-security literacy of the average internet user in Slovenia. The project also has the following short-term objectives:

- raise awareness about the different threats that users are facing on the web,
- inform users about safe use of online banking,
- inform users on how to shop and sell online safely,
- inform users about the various types of online fraud and offer practical solutions on how to protect themselves,
- inform users on how to protect their personal identity on social networks.

Safe on the Internet addresses the wider Slovenian population, with an emphasis on adult users. The target audience is members of the general public aged between 24 and 54 years, since in Slovenia they are the main users of online shopping, online banking solutions and social networks. An additional, more specific audience is small and medium enterprises, which are more vulnerable because of their limited budget for professional IT support.

Other organisations in Slovenia working in the field of information security have been approached and invited to participate in the project. Working together can be a big advantage, since it raises media and public attention. There is some cooperation with the Consumer Protection Association NGO, as well as with the European Consumer Centre of Slovenia and the Ministry of Economic Affairs, where the Centre is located. As e-banking is widely used in Slovenia, cooperation takes place with banks and their association both in awareness raising, for which competent authorities provide materials, and also with incident handling. Additionally, Slovenia mentioned joint projects with the Information Commissioner's Office in the area of personal data protection and privacy, and membership of the Safer Internet Centre (SAFE.SI) Advisory Board.

COMMUNICATION CHANNELS

The most important communication channel through which the target audience is reached is the educational portal https://www.varninainternetu.si/. The portal represents the platform of the entire programme; it constitutes a knowledge base on information security and receives an average of 100 000 unique visitors per year. The portal presents the latest news and alerts on security threats relevant to the scope of the campaign. SI-CERT is very active on social media networks, especially Facebook and Twitter, which allow for sharing and interaction. It currently has 19 000 fans on Facebook (https://www.facebook.com/varninainternetu) more than 1 000 followers on Twitter (https://twitter.com/varninanetu) and over 143 000 views on its YouTube channel (https://www.youtube.com/user/VarniNaInternetu).

Two to three times each month the 'Safe News' newsletter is sent out to 3 000 e-mail subscribers. The campaign not only uses digital communication channels, but also produces, prints and distributes various leaflets, brochures and posters about online safety, safe online shopping, etc.

NATIONAL CONTACT POINT: 'REPORT FRAUD!'

Slovenia's main focus here is on sharing knowledge on network and information security and raising awareness, but sometimes that is not enough. Internet users who have already fallen victim to online scams such are identity theft or Nigerian scams need help. For this reason, Slovenia has set up an online form (https://www.varninainternetu.si/prijavi-prevaro/) where users (individuals, companies, organisations, etc.) can report a scam or an incident and get support from the SI-CERT team of network security experts. Since all SI-CERT and *Safe on the Internet* activities were financed by the Ministry of Education, Science and Sport, the service is free of charge.[16] Statistics show that the number of reported online frauds increased sixfold since 2010. This confirms that such support was needed and that it was appreciated by the online community in Slovenia.

[16] After the on-site visit the evaluation team was informed by the Slovenian authorities that *Safe on the Internet* is currently co-financed by the Ministry of Public Administration and not by the Ministry of Education, Science and Sport.

Table: Number of online frauds reported to SI-CERT

2008	49
2009	84
2010	122
2011	227
2012	442
2013	525
2014	837

EUROPEAN CYBER SECURITY MONTH

The strategy is based on a long-term programme of activity throughout the year, but the most important communication campaign is the European Cyber Security Month (ECSM). ECSM is a European Union advocacy campaign which takes place once a year. ECSM aims to promote cyber security among citizens, to change their perception of cyber threats and to provide up-to-date security information through education and sharing good practices. The pilot Cyber Security Month was held in 2012. Slovenia was among the nine participating EU Member States. In 2014, more than 60 partners from 30 European countries participated with more than 50 activities.

During ECSM, the focus is on three activities:

- generating public interest and drawing attention to the educational portal www.varninainternetu.si with a strong advertising and public relations campaign (TV, social media ads, social media activities);
- engaging users by sharing educational content and positive messages via different online tools (quizzes, Facebook applications, active bookmarks and videos);
- incident response: due to the advertising, media coverage and social media activities in October the web site received more than 20 000 visitors, which consequently raised the number of phone calls, questions and reports received via the 'Report fraud!' contact point.

The other programme is the SAFE.SI awareness centre within the Safer Internet Centre Slovenia, which was initiated by the EU (the Connecting Europe Facility) and is an EU co-funded project (the remaining 50 % of the funds are provided mainly by the Slovenian Ministry of Education, Science and Sport[17], and in small part by the industry (a few telecommunication operators) as requested by the EC call). The Centre has three components:

- SAFE.SI awareness centre (www.safe.si), which raises awareness of safe and responsible use of the internet and new technologies among children, adolescents, parents, teachers, youth workers and social workers;
- toll-free *TOM telefon* helpline for young people and their parents who experience internet-related issues (116 111 and chat and e-mail service at www.e-tom.si);
- the *Spletno oko* hotline for anonymous reporting of illegal content online (child abuse material online and hate speech) at www.spletno-oko.si.

The SAFE.SI awareness centre is, to a greater extent than the other two components, responsible for raising awareness among its target groups: children, adolescents, parents and professionals (teachers, social workers, youth workers, etc.). The most important part of its awareness raising programme are the following activities:

BROAD TRAINING SYSTEM

- 150 schools visited per school year
- 400 workshops for 8 000 children and adolescents per school year
- 100 seminars for 3 000 parents per school year
- seminars for headmasters, teachers, future teachers (students), social workers, etc.
- 1 700 teachers and school workers trained in this school year through MOOC.

[17] Currently co-financed by the Ministry of Public Administration.

ONLINE PRESENCE

- the www.safe.si website for teenagers, parents and teachers, and the otroci.safe.si website for children, which receive 120 000 visits yearly
- SAFE.SI Facebook page – www.facebook.com/safe.si – for parents and teachers, with 10 239 likes
- *Deskam varno* Facebook page – www.facebook.com/deskamvarno – with 9 172 likes
- YouTube channel – www.youtube.som/saferinternetsi – with 147 000 views
- Twitter account – www.twitter.com/Safe_si – with 50 000 tweet impressions per year.

RESOURCES

- offline and online resources for all target groups
- leaflets, brochures, games, video guides, quizzes, tests, gadgets, cartoons and videos
- wide dissemination through workshops, seminars, events, fairs, post and media.

COMPETITIONS

- school competition for elementary schools (drawings, poems, stories, videos on different online safety topics), in which 80 schools and 1 000 pupils participate yearly
- best online content for children competition through national online Netko awards
- PEN International literary contest for secondary schools on 'The world wide web and me'.

SAFER INTERNET DAY (SID) AND MONTH CELEBRATIONS IN FEBRUARY

- school toolkits (decentralised approach – 300 schools and 376 teachers on SID 2015)
- big events, training courses for target groups, media
- intense media communication (100 items in newspapers, TV, radio, online media)
- new resources for target groups
- webinars, experts, online advice, etc.

The private sector also plays a part in the awareness raising. Through its years of running the Safer Internet Centre Slovenia (since 2005) the country has fostered very fruitful cooperation with the industry in creating joint resources for the target groups, using the industry's communication channels to reach the target groups, and creating joint events and training courses for the target groups. A good example of cooperation and of the involvement of industry players is the SID celebrations in 2013. **On Safer Internet Day, 5 February 2013, the CEOs of all eight major national telecommunications operators signed the renewed** 'Code of practice of Slovenian telecommunications operators for user protection'. The main added value of this document is that it ensures minimum protective measures for safer use of mobile devices not just by children and under-18s, but also by all other users, especially elderly users.

Additionally, to promote SID 2013, SAFE.SI and the national telecommunications operators carried out a **joint promotional advertisement campaign entitled 'Let's encourage safe and responsible use of mobile devices'**. This advertisement has been included on the printed version of the telecommunications operators' monthly phone bills. It is estimated that around 1 000 000 people, which is more than 50 % of the active population aged 10-75, were reached through this campaign.

8.3 Prevention

8.3.1 National legislation/policy and other measures

The key responsibility for preventing cybercrime in Slovenia lies with:

- the criminal police, particularly the Computer Investigation Centre and its six computer investigation departments, the Economic Crime Divisions (abuse of payment cards, internet fraud) and the Juvenile Crime Section;
- SI-CERT – Slovenian Computer Emergency Response Team.

These bodies operate within general legislative frameworks and authorisations which govern their work. Legal regulations and procedures adopted specifically for the purpose of cybercrime prevention have not yet been established in the Republic of Slovenia.

The Resolution on the National Plan on the Prevention and Combating of Crime (ReNPPZK12-16) for the 2012–2016 period was adopted within governmental institutions to combat all types of crime in the Republic of Slovenia. The Resolution also discusses *inter alia* the field of cybercrime prevention, proposing certain solutions which would contribute to more efficient work in this field. These solutions could be combined into three larger sets, namely education of all bodies involved in the prevention and investigation of cybercrime, cooperation between the public and private sectors, and the establishment of one or more institutions to monitor and coordinate all work in this field. Most of the solutions proposed by the Resolution have yet to be put into practice.

The Slovenian police are a partner in the Advisory Board set up by the Safer Internet Centre Slovenia. They participate by providing knowledge of trends and by organising joint prevention and educational activities. The Slovenian police also cooperate with UNICEF and the Safer Internet Centre Slovenia in running the e-Safety point (for children to get on-the-spot advice). Additionally, they are part of the annual Safer Internet Day, and are also a partner in the Awareness and Prevention Forum within Europol/EC3. Moreover, they hold an annual conference for the wider audience (social services, schools, police officers, judiciary, industry, NGOs), which is attended by approximately 200 participants.

Since 2005, Slovenia has been co-funding the activities of the Safer Internet Centre Slovenia, which has developed many prevention campaigns in schools, social service centres, the media and online on various cyber safety and cybercrime topics for the target groups of children, teenagers, parents and professionals. Information on this can also be found in English (http://safe.si/en/center/safer-internet-centre).

Since 2011, the Slovenian Ministry of Education, Science and Sport has been financing the national project of raising public awareness on network and information security, *Safe on the Internet*.[18] The programme is coordinated by the Slovenian National Computer Emergency Response Team (SI-CERT) and has been envisaged as a long-term activity, with the main objective being to help improve the information-security literacy of the average internet user in Slovenia. The project's short-term objectives are to inform internet users about the various types of online fraud, to offer practical solutions on how they can protect themselves, and to inform them about safe online banking and online shopping. The programme is aimed at a wide Slovenian audience, with a focus on adult users and with specific content for SMEs.

8.3.2 Public-private partnership (PPP)

Public-private partnership in the prevention of and fight against cybercrime is present in Slovenia as cooperation within different conferences on topical issues relating to cybercrime. Cooperation takes place in individual cases in the form of information exchanges (e.g. on current attacks on information systems), the public information system, operative meetings, joint preventive measures and similar. Such partnerships and cooperation should be reinforced.

[18] After the on-site visit the evaluation team was informed by the Slovenian authorities that *Safe on the Internet* is currently co-financed by the Ministry of Public Administration and not by the Ministry of Education, Science and Sport.

8.4 Conclusions

- Slovenian police cooperation with, and involvement in the activities of, Europol/EC3 is active and successful. At the time of the on-site visit their attendance at training courses offered at EU level was mainly limited to CEPOL conferences. According to the information provided after the on-site visit the number of training attended by the police officers has increased.
- Efforts are made at police force level to provide basic training to all new police officers, and occasionally specific training sessions for cybercrime investigators and forensic experts, but all of these initiatives are limited as the available resources.
- At national level, there is a lack of training for judges and prosecutors on both the fight against cybercrime and international cooperation, and the latter do not even make use of training offers provided by Eurojust and EJTN. This also raises the question of the motivation and awareness of the judiciary regarding the cybercrime phenomena.
- Slovenia actively runs two major awareness-raising programmes:
    - *Safe on the Internet*, a national project targeting the adult population, coordinated by the National CERT;
    - 'SAFE.SI', within the EU-initiated Safer Internet Programme, which is dedicated to children, parents and professionals.

9 FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Slovenia

In the last five years, the Criminal Police Directorate at the General Police Directorate has upgraded its human resource, equipment, technical and organisational capacities for the investigation and prevention of cybercrime. This is particularly noticeable in the field of digital forensics and the investigation of typical computer crimes. The police monitor, coordinate and investigate crimes against children (CSE area), but believe that they still do not have enough capabilities and resources available to take legal action in TOR/hidden networks or the P2P environment. Police also lack IT/forensic experts dedicated to CSE investigations, who could perform open source investigations, *inter alia*.

The limited resources have been noted, but successful provision of cyber security requires more effective application of the existing resources and suitable multi-level organisation. The state must establish a national body in charge of cyber security at a sufficiently high political level to ensure its stable operation. At the strategic level, this body should be responsible for coordinating all cyber security capacities at lower levels in the country and represents a point of contact for international cooperation.

The National Cyber Security Strategy was adopted on 25 February 2016. The strategy contains the measures for strengthening the national cyber security system. The evaluation team was informed that an action plan for the implementation of the strategy has been prepared and the strategy is planned to be implemented in five years.

Examples of good practice in combating cybercrime

Participation in international operations, working groups and exercises (e.g. the *Iserdo* case relating to investigation of the *Mariposa botnet*; cooperation within the 'Cyber Attack' group as part of Europol's EMPACT project; the internationally coordinated 'BLACKSHADES' project; the 'Cyber Coalition' within the NATO exercise) proved to be a good opportunity to verify the country's capacity to ensure cyber security at the national level, and also to exchange experiences and forge contacts between participants.

Worth mentioning are those cases which clearly show that there is a child who must be protected from the 'paedophile ring', especially when the relevant data to locate him or her are found. All investigators dedicated to the CSE area would contribute their knowledge, experience and best potential in order to identify the child. The result: rescued and protected children. Good practice exists and takes place because of the excellent team work of dedicated investigators.

Suggestions with a view to strengthening prevention and counteracting cybercrime

Sufficient financial, staffing and material resources to efficiently fight cybercrime should be provided. The legislation and procedures in this field have to keep up with the fast development of information technologies. All law enforcement authorities participating in the prosecution of cybercrime should maintain suitable competence in the field of procedural regulations and processes in society relating to cybercrime, including the development and implementation of processes in the field of ICT technologies. Monitoring should be carried out and procedures developed for legislation governing cybercrime which is already in the initial phase, including pointing out practical and systemic deficiencies and ambiguities. Preventive activities should be intensified in all fields. Relationships between all stakeholders participating in the fight against cybercrime should be reinforced.

The child abuse investigation policy should also encompass the following:

- setting up a national strategy on the fight against CSE off- and online, with a designated coordination body;
- amending the provisions on obtaining data from criminal records;
- courts should provide law enforcement authorities with all convictions in the CSE area to allow further steps to be taken in child protection procedures;
- establishing an initiative to prevent any future harm from being done to children by convicted and criminally charged offenders;
- establishing a national child sexual exploitation database;
- introducing Interpol's Access Blocking initiative in the Slovenian environment;
- re-establishing a cybercrime educational centre within the Police Academy to better train all police officers and judiciary;
- designing a basic and introductory training course for all police officers in Slovenia, to be attended systematically;
- establishing a National Cybercrime Centre within the Slovenian national police (some steps have been taken in this direction, but the police were not successful in attracting the relevant foreign police partners on board);
- possibly establishing victim identification training courses on the national and international levels.

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 Slovenia was able to satisfactorily review the system in Slovenia.

Slovenia 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 Slovenian authorities. Furthermore, based on the various good practices, related recommendations to the EU, its institutions and competent agencies are also put forward.

9.2.1 Recommendations to Slovenia

1. Slovenia should implement all necessary action plans related to the National Cyber Security Strategy.

2. The Slovenian authorities should continue their intensive efforts to focus public attention - in particular that of parents and children - on the dangers posed by the internet.

3. Slovenia should monitor the need to increase the human and technical resources dedicated to the fight against cybercrime, in particular within the investigative and forensic police services.

4. Slovenia should ensure more coherence in the methodologies of the competent authorities in the field of cybercrime, with a view to achieving higher accuracy and consistency of the related statistical data.

5. With a view to accurately transposing Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems, Slovenia is invited to review its legal system with regard to the definition of cybercrime and other legal definitions in use, as well as to the level of penalties and efficiency procedures regarding removal of/blocking access to illegal online content and services.

6. Following the ruling of the Constitutional Court of the Republic of Slovenia which fully repealed Articles 162 to 169 of the ZEKom-1, Slovenia is strongly encouraged to reflect on the most efficient way to remedy the lack of law regarding the retention of electronic data, while fully considering both operational needs and the protection of fundamental rights.

7. In order to prevent secondary victimisation of children, it is recommended that Slovenia introduce a scheme to effect compliance with Directive 2011/93/EU in relation to the provision of audio-visual recorded interviews for child victims, and that such audio-visually recorded interviews may be used as evidence in criminal court proceedings in order to prevent additional trauma as a result of interviews or visual contact with offenders to the extent possible.

8. Slovenia should provide adequate training for all law enforcement agencies involved in combating cybercrime, as well as for prosecutors and judges.

9. Slovenia should consider improving its MLA procedures related to cybercrime investigations, with a view to establishing direct, expeditious and efficient communication and cooperation between competent operational stakeholders.

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

10. The European Union and its institutions, in particular the European Commission, should 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, and should better engage in a dialogue with the private sector, the academic world and third state authorities to this end.

11. The European Union and its institutions should more actively promote the identification and expansion of Member States' best practices, including toolkits used in the fight against cybercrime. They should also proactively encourage the use of open-source tools and materials by Member States' competent authorities, with a view to facilitating the sharing of relevant expertise.

12. Member States should develop well-designed statistics which correctly reflect the reality of the cybercrime phenomenon. This is important to check the effectiveness of the legal and investigative measures in place and to respond in a more agile and efficient manner.

13. Member States and EU institutions are encouraged to use and promote better terminology that focuses on child protection and child victims of sexual exploitation, such as child sexual exploitation material and child sexual abuse material instead of child pornography.

9.2.3 Recommendations to Eurojust/Europol/ENISA

14. Europol should encourage and facilitate the setting-up of a framework under which tools can be exchanged or shared by Member States' competent authorities.

15. Europol/EC3 should consider proposing to Member States a standard approach on structural elements for criminal intelligence databases in cybercrime, and should facilitate the adoption of a common taxonomy on cybercrime.

16. EJTN should examine ways to help spread basic cybercrime awareness and knowledge to members of the judiciary throughout the Member States.

17. Eurojust, with the support of EC3 on the one hand and the JIT network on the other, should proactively identify suitable cases where a JIT would be of assistance in the area of cybercrime; in particular, it should encourage those Member States that have not used JIT before to make use of this process.

18. Europol/Eurojust/ENISA are encouraged to use and promote better terminology that focuses on child protection and child victims of sexual exploitation, such as child sexual exploitation material and child sexual abuse material instead of child pornography.

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

7th Round of Mutual Evaluations - Slovenia 11 - 13 May 2015

Monday 11 May 2015

9.00 *Venue:* **Ministry of Interior**

- Welcoming speech by State Secretary Mr. Boštjan Šefic

10.00- 13.00 *Venue:* **Ministry of Education, Science and Sport**

- The relevant legislation, covered by the Ministry of Education, Science and Sport
- Raising public awareness programmes
- The draft of the National Cyber Security Strategy

15.00 - 18.00 *Venue:* **Ministry of Justice**

- Introductory greetings by Mrs. Tina Brecelj, State Secretary
- Legal aspects and implementation of Directives 2011/93/EU and 2013/40/EU
- MLA, Surrender and Extradition
- Judiciary (Prosecution and Courts)

Tuesday 12 May 2015

9.00 - 13.00 *Venue:* **Ministry of Interior, Criminal Police Directorate**

- Welcoming speech by representative of Criminal Police Directorate
- Card Fraud
- Presentation of the Computer Investigation Centre

- Presentation of International Police Co-operation Division
- Presentation of International Police Co-operation Division
- Discussion, questions

Wednesday 13 May 2015

9.30-13.00 *Venue:* **Ministry of Interior**

- The Role of Police Force in the fight against on-line child sexual exploitation
- Discussion, questions.

ANNEX B: PERSONS INTERVIEWED/MET

Meetings 11 May 2015

Venue: **Ministry of Interior**

Person interviewed/met	Organisation represented
Mr. Matej Torkar, Head of Service	Ministry of Interior, European Affairs and International Cooperation Service
Mr. Marko Bečan, GENVAL national delegate	Ministry of Interior, European Affairs and International Cooperation Service
Katia Rejec Longar, Head of Department	Ministry of Justice, International Cooperation and EU Law Department
Ms. Tanja Trtnik, Criminal Law Expert	Ministry of Justice, International Cooperation and EU Law Department
Mr. Anton Toni Klančnik, MA, Senior Criminal Police Inspector Specialist	Juvenile Crime Section, Criminal Police Directorate, General Police Directorate

Venue: **Ministry of Education, Science and Sport**

Person interviewed/met	Organisation represented
Mrs Barbara Pernuš Grošelj, Head of Sector	Ministry of Education, Science and Sport, Information Society Directorate, Information Society Legislation Sector
Ms Marija Režun	Ministry of Education, Science and Sport, Information Society Directorate, Information Society Legislation Sector
Dr Radovan Pajntar	Ministry of Education, Science and Sport, Information Society Directorate, Information Society Development Sector
Mr Marjan Kavčič	Ministry of Education, Science and Sport, Information Society Directorate, Information Society Development Sector

Ministry of Justice

Person interviewed/met	Organisation represented
Katia Rejec Longar, Head of Department	Ministry of Justice, International Cooperation and EU Law Department
Ms. Tanja Trtnik, Criminal Law Expert	Ministry of Justice, International Cooperation and EU Law Department

Meetings 12 May 2015

Venue: **Ministry of Interior, Criminal Police Directorate**

Person interviewed/met	Organisation represented
Ms Lilijana Obreza Kadilnik, Head of Division	Criminal Police Directorate, Economic Crime Division
Mr. Toni Kastelic, Head of Centre	Criminal Police Directorate, Computer Investigation Centre
Mr. Savin Svet	Criminal Police Directorate, Computer Investigation Centre

Venue: **Ministry of Interior, Criminal Police Directorate**

Person interviewed/met	Organisation represented
Mr. Gabrijel Gajšek, Head of Division	International Police Co-operation Division

Meetings 13 May 2015

Venue: **Ministry of Interior, Criminal Police Directorate**

Person interviewed/met	Organisation represented
Mr. Anton Toni Klančnik	MA, Senior Criminal Police Inspector Specialist

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN ORIGINAL LANGUAGE	ORIGINAL LANGUAGE	ENGLISH
CAM	-	-	Child Abusive Material
CEPOL	-	-	European Police College
CERT	-	-	Computer Emergency Response Team
CFCS	-	-	Centre for Cyber Security under the Danish Ministry of Defence
CMS	-	-	Case Management System
CoE	-	-	Council of Europe
CSA	-	-	Child Sexual Exploitation
CSE	-	-	Child Sexual Exploitation
ECJ	-	-	European Union's Court of Justice
EC3	-	-	European Cybercrime Centre
EGTEC	-	-	European Cybercrime Training and Education Group
EJN	-	-	European Judicial Network
EC3	-		European Cybercrime Center at Europol
EJTN	-	-	European Judicial Training Network
EMPACT	-	-	European Multidisciplinary Platform against Criminal Threats

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN ORIGINAL LANGUAGE	ORIGINAL LANGUAGE	ENGLISH
ENISA	*court-*	-	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
T-CY	-	-	the Committee of Parties to the Council of Europe Convention on Cybercrime
VOIP	-	-	Voice Over IP
ZNPPol	*Zakon o nalogah in pooblastilih policije*	-	The Slovenian Police Tasks and Powers Act