Council of the
European Union

Brussels, 11 April 2017
(OR. en)

5250/1/17
REV 1 DCL 1

GENVAL 3
CYBER 9

DECLASSIFICATION

of document:	5250/1/17 REV 1 RESTREINT UE
dated:	17 March 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 Croatia

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, 17 March 2017
(OR. en)

5250/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 3
CYBER 9

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 Croatia

ANNEX

Table of Contents

1 EXECUTIVE SUMMARY

- The on-site visit to Croatia took place from 29 September to 1st October 2015. The visit was intense and efficiently organised within the allocated time; the evaluation of Croatia would have merited additional time in order to get a clearer and more detailed picture of the situation; however, the experts were able to interview very competent and committed colleagues from the major governmental stakeholders involved, namely the Office of the National Security Council of Croatia, CERT, the Ministry of the Interior, the Ministry of Justice; the State Attorney's Office and the judiciary were also represented and the latter made an impressive presentation about the case law.

- The European Commission, Europol/EC3, Eurojust and ENISA abstained from participating in the on-site visit and did not contribute otherwise to the evaluation of Croatia. Therefore, the evaluation team questions the involvement in the 7th round of mutual evaluations of the major EU actors in charge of cybersecurity and fight against cybercrime.

- The Office of the National Security Council of Croatia strongly recommends to the Croatian authorities that they fully implement the National Cyber Security Strategy and its Action Plan. The evaluation team can but endorse this appeal.

- The general feeling of the evaluation team is that Croatia does have appropriate structures and the available resources to take action against cybercrime. It might suffer from a lack of overall coordination, monitoring and financial support; during the visit the team noted shortcomings at the institutional level, due in some cases to insufficient awareness on the part of high-ranking decision-makers and to a lack to financial means.

- In particular, although most of the competent practitioners seem to know each other and try to coordinate as best as they can, institutional coordination deserves to be prioritised 'as a must' at all levels.

  "Cyber" offences as a proportion of crime officially recorded in Croatia in 2015 is about 0.5%. Questions may therefore arise about the efficiency of detection, prosecution and punishment of cybercrime in the country and about the accuracy of official statistical records. The evaluation team did not receive sufficient information to be able to identify the actual reasons for this situation.

- Only the police have structures and officers specialised in cybercrime. While there are no specific judicial structures focusing on this area, some highly skilled practitioners may be called upon to provide advice to their colleagues.

- Although general and specialised training in the area of cybercrime are provided for Croatian police officers, it was acknowledged that supplementary financial and organisational efforts should be made to enhance the training on offer and allow practitioners enough time to follow the courses.

- Before joining the European Union Croatia had participated successfully into various IPA Programmes, in particular the project entitled "Regional Cooperation in Criminal Justice: Strengthening Capacities in the Fight against Cybercrime in South-East Europe", and a Regional Pilot Centre for training judicial officials on combating cybercrime was established; the Centre, based in Zagreb (Croatia), deserves to be maintained and even developed as a main training resource for judicial practitioners.

- It should be noted that Croatian authorities are also active in connection with a number of other international and European activities and projects – to the extent that their resources and availability allow.

- Valuable efforts are made by the competent Croatian authorities to prevent cybercrime by carrying out activities to inform and educate the public. In particular, the Croatian national CERT is very active.

- In the same vein, the existence of a platform for cooperation between the police authorities and the banking system is to be seen as a constructive step towards an effective and in-depth cooperation with private partners.

2 INTRODUCTION

Following the adoption of the Joint Action 97/827/JHA of 5 December 1997[1], a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organised crime was established. 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 for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud, comprehensively examining the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with the relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and exploitation of children and child pornography[2] (transposition date 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

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

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

Experience from past evaluations shows that Member States will be at different stages as in the implementation of the relevant legal instruments, and the current process of evaluation could provide useful input also 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 focus on the implementation of various instruments relating to the fight against cybercrime only but rather on the operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, this will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from 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 cyberattacks and fraud, and also of child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to persons who fall victim to cybercrime.

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

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

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

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Croatia was the 14th Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request to delegations dated 28 January 2014 and 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, together with 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 national experts charged with undertaking the evaluation of Croatia were Mr Branislav Bohacik (Slovakia), Mr Andrea Raffaelli (Italy) and Mr Tamas Pal (Hungary), who visited the country together with Ms Claire Rocheteau from the General Secretariat of the Council. No observers were present on behalf of Europol/EC3, Eurojust, ENISA and the European Commission.

This report was prepared by the national experts with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Croatia between 29 September and 1st October 2015, and on Croatia's detailed replies to the evaluation questionnaire, together with their detailed answers to ensuing follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National cyber security strategy

At the time of the on-site visit draft of the National Cyber Security Strategy was being reviewed by the stakeholders and preparations for its adoption were taking place. The National Cyber Security Strategy was adopted on 7 October 2015 (Official gazette 108/2015). The Government of the Republic of Croatia has established the National Cyber Security Council and the Operational and Technical Cyber Security Coordination Group in June 2016 (Official gazette 61/2016).

The Croatian authorities confirmed that combating cybercrime is recognised in the Republic of Croatia as one of the priority areas of cybersecurity.

One of the strategic goals of the Strategy is to develop and raise awareness of cyberspace In this regard the Action Plan contains 8 implementation measures, one of which is specifically focused on informing the public should computer incidents occur that can be easily multiplied and affect a large number of users. Translation of the National Cyber Security Strategy in English is available at: www.uvns.hr/en.

3.2 National priorities with regard to cybercrime

In order to exercise **the right of a child to a non-violent environment** in the community in which the child lives and to achieve long-term, systematic, planned and organised activities for combating violence against children in the community and the media and combating electronic violence, the National Strategy as described to the evaluation team provides for the following measures:

- Use the media to promote zero tolerance for violence against children in the community and the media and for electronic violence, by emphasising the social responsibility of everyone where violence against children outside of the school and family is concerned;
- Consistently apply the law;
- Develop effective sanctions for non-compliance with the law regarding violence in the media and online;
- Report regularly to the competent institutions on the above.

In the area of training, the IPA 2010 project "Regional Cooperation in Criminal Justice: Strengthening Capacities in the Fight against Cybercrime in South-East Europe" led to the establishment in Zagreb of a Regional Pilot Centre (hereinafter: The Centre) for training judicial officials in the fight against cybercrime. The project was implemented in the period from November 2010 to April 2013. The establishment of the Centre is one of the key results of the project in which the following countries, now users of the Centre, were involved: Albania, Bosnia and Herzegovina, Montenegro, Croatia, Kosovo, Macedonia, Serbia and Turkey. The Republic of Croatia (the first among the states involved in the project to join the EU) was chosen as the state in which to establish the Pilot Centre.

At the conference held in Dubrovnik in February 2013, high officials from the ministries of justice and the interior of all states participating in the project signed a Declaration on Strategic Priorities in the Cooperation against Cybercrime, which also identifies the establishment of the Pilot Centre in Croatia as one of the strategic priorities.

Given that the adoption of the National Cyber Security Strategy is pending, the Judicial Academy will propose that the national and regional training of judicial officials in combating cybercrime be included in the Action Plan for the implementation of the National Cyber Security Strategy in the part related to the training of judges and State Attorneys.

Croatia actively participates in the EMPACT Sub-priority Cyber Attacks, and Croatian experts were part of the team developing Operational Action Plans 2014 & 2015. Croatia is Action Leader of the Activity 5.1: '*Draft guidelines and/or operational procedures for improving operational national contact points (NCP) for exchange of information in accordance with Article 13 of the Directive 2013/40/EU on attacks against information systems*'.

Croatia participates in the following activities as well: drafting of the Internet Organised Crime Threat Assessment (iOCTA 2015), the identification of current and emerging major cyber threats impacting on two or more Member States (MS); the development of a common tool kit to target and disrupt prevalent malware distributors, systems and services affecting two or more MS; the identification of high -value targets appropriate for a collaborative response involving two or more MS; the establishment of a European Expert Group on Cybercrime to address all the practitioner's level aspects of the fight against cybercrime; the collection of malware contributions on current attacks from the banking industry at EC3, passing them on to the EUROPOL Malware Analysis System (EMAS); support for the Member States and the operational partners in the integration of money laundering and asset recovery techniques as an inherent part of operational actions in this OAP, making maximum use of avenues for financial investigations aimed at targets identified in OAs of this OAP; the exchange of best practices and experiences in the co-operation with third states; measures to enable the development and maintenance of training material in accordance with the training needs; the Assessment/Training Competency Framework established in OAP 2014; the development and implementation of a solution to the pseudonymised cross-matching and de-confliction of data.

National Cyber Security Strategy lists the following general priorities:

- Systematic approach in the implementation and development of the national legislative framework;
- Implementation of activities and measures to increase the safety and the reliability of cyberspace;
- Establish a more efficient mechanism for the exchange and transfer of and access to data;
- Strengthen cyber safety awareness;
- Development of harmonised education programmes;
- Stimulate the development of e-services;
- Encourage research and development,
- Systematic approach to international cooperation.

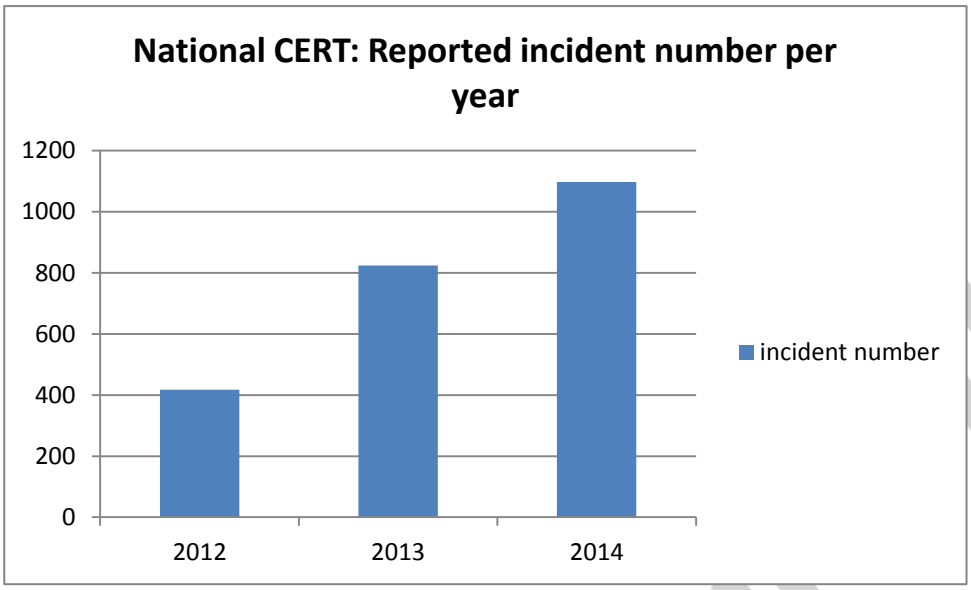
The Croatian national priority tasks are related to the strategic objectives and operational action plans of the EU, as the Croatian police have been actively participating in the EMPACT cyber attack projects, so this is also one of the goals in the prevention, combating and investigation of cybercrime.

3.3 Statistics on cybercrime

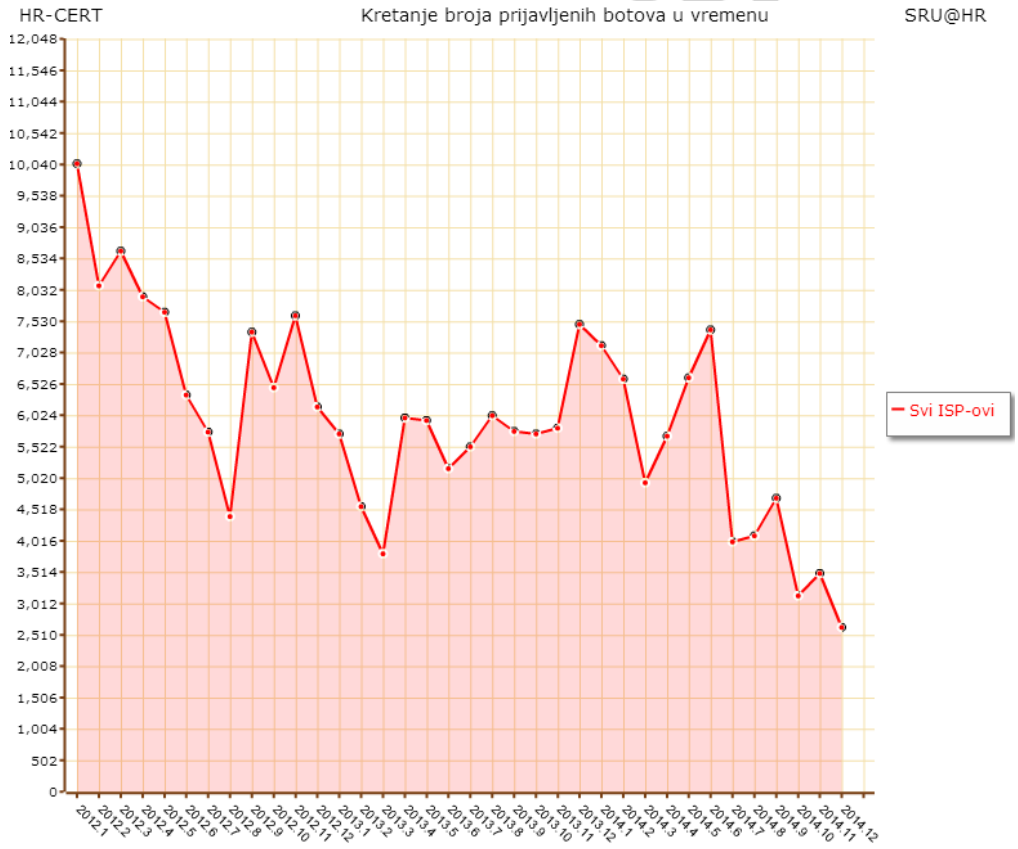
3.3.1 Main trends leading to cybercrime

During 2014, the increase in the number of reports of cybercrime offences involving known perpetrators continued as expected and 131 people were reported, which is 11% more than the previous year. The number of reports is low because cybercrime offences as a proportion of all crime committed by adult perpetrators is only 0.5%.

The number of cyber incidents processed by National CERT has increased in the last 3 years, as shown in the picture. Most of the incidents are related to compromised servers serving phishing or malware.



The number of identified bots in the country fell slightly over the last 3 years with an identified peak caused by infection of Zeus malware in the year 2014.



3.3.2 Number of registered cases of cyber criminality

The State Attorney's Office of the Republic of Croatia, acting within its field of competence, keeps statistical records on criminal offences committed in the area of cybercrime.

Within the Ministry of Justice, a specific report is currently being prepared as part of the project for upgrading the e-File system, which will enable statistical tracking of criminal cases using all criminal offences laid down in the Criminal Code, including cybercrime offences.

National CERT statistics are compiled on the basis of incidents reported and dealt with and kept separately.
According to the State Attorney's Office of the Republic of Croatia, the statistical data for 2013 are as follows:
- for the criminal offence of child enticement for the purpose of satisfying sexual needs (Article 161 of the Criminal Code ("Official Gazette" nos. 125/11, 144/12, 56/15, 61/1; hereinafter: the CC), five crime reports were filed, four indictments were issued and three judgements were rendered;
- for the criminal offence of exploitation of children for pornography (Article 163 of the CC), 26 crime reports were filed, three investigations were initiated, 23 indictments were issued and 16 judgements were rendered;
- for the criminal offence of introducing pornography to children (Article 165 of the CC), seven crime reports were filed and one indictment was issued;
- for the serious criminal offences of child sexual abuse and exploitation (Article 166 of the CC), 12 crime reports were filed, four investigations were initiated, 11 indictments were issued and eight judgements were rendered;

- for the criminal offence of unauthorised access (Article 266 of the CC), seven crime reports were filed, five indictments were issued and five judgements were rendered;
- for the criminal offence of computer system interference (Article 267 of the CC), one crime report was filed;
- for the criminal offence of computer-related forgery (Article 270 of the CC) one crime report was filed, one indictment was issued and two judgements were rendered;
- for the criminal offence of computer-related fraud (Article 271 of the CC), 105 crime reports were filed, one investigation was initiated, 103 indictments were issued and 64 judgements were rendered.

In 2014, most of the crime reports (113) still referred to the criminal offence of computer-related fraud as mentioned in Article 271 of the CC. A total of 102 people were charged with this type of crime in that period. In 2014, after indictment, the courts rendered 92 judgements, of which 88 were convictions, with ten perpetrators of the criminal offence of computer-related fraud being punished by imprisonment with confiscation of pecuniary gain.

The number of criminal offences related to the sexual exploitation and abuse of children covered by the definition of "cyber-crimes" is increasing, as shown by the following table which compares the figures for 2013 and 2014.

SEXUAL ABUSE AND EXPLOITATION OF A CHILD[7]

2013-2014

CRIMINAL OFFENCE	2013	2014
Art. 161. Grooming	14	11
Art. 163. Exploitation of children for pornography	61	141
Art. 164. Exploitation of children for pornographic performances	3	0
Art. 165. Introducing pornography to children	24	19
TOTAL	102	171

The crime incidence increased by 67.6%, mostly due to the large increase in the number of offences covered by "The exploitation of children for pornographic purposes" (Art. 163 CC) to 131.1%.

New and widespread form of abuse takes place through social networks; perpetrators create on line forums, social networks pages/space and other Internet- based communication tools to gather and publish photos of girls/boys taken without their knowledge in their daily activities, with offenders publishing the photos on social networks for the purpose of disclosure, labelling, insulting and ridiculing victims. Whoever endangers the welfare of the child by publishing personal data or the child's photo and disturbs the child or a makes a mockery of his or her peers or other persons, especially through a computer system or a network, faces prosecution for committing a criminal offence under Article 178, Violation of a child's privacy

Criminal offence	2013.	2014.
Art. 178. Violation of a child's privacy	9	35

After the on-site visit the following statistics on criminal offences against computer systems, programmes and data for the period of 2013 - 2015 were forwarded to the evaluation team:

[7] Criminal Code (Official Gazette 125/11, 144/12)

CRIMINAL CODE

CRIMINAL OFFENCES AGAINST COMPUTER SYSTEMS, PROGRAMMES AND DATA[8]

criminal offence/year(period)	2013	2014	January-August 2015
Article 266 **Unauthorised Access**	**16**	**16**	**15**
Article 267 **Computer System Interference**	**4**	**1**	**1**
Article 268 **Damage to Computer Data**	**2**	**4**	**2**
Article 269 **Unauthorised Interception of Computer Data**	**4**	**3**	**5**
Article 270 **Computer-related Forgery**	**86**	**169**	**72**
Article 271 **Computer-related Fraud**	**583**	**960**	**835**
Article 272 **Misuse of Devices**	**12**	**19**	**10**

[8] These statistics represent the number of criminal offences reported by the police to the state attorneys in Croatia for mentioned period. The numbers do not represent the number of the offenders. It should be noted that usually there are fewer offenders than offences reported because one offender can commit more than one offence and not all reported offences end up in courts.

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

Croatia is about to complete the twinning project ″Strengthening the capacities of the Ministry of Interior to combat Cybercrime″, jointly implemented by the Spanish Ministry of the Interior, the Austrian Federal Ministry of the Interior and the Croatian Ministry of the Interior. The project is a part of the twinning initiative launched by the European Commission with a view to assisting the beneficiary countries in strengthening their administrative capacities to implement the EU acquis. The objective of this project, which is worth € 700,000 and is financed by the European Union, was to strengthen the capacities of the Ministry of the Interior to effectively combat cybercrime at national and international levels, in line with the relevant EU policies and strategies.

The Ministry of the Interior in the pre-accession assistance programme of the European Commission IPA 2009 implemented a project called "Capacity Building in the Field of Fight against Sexual Exploitation and Sexual Abuse of Children, and on Police Assistance to Vulnerable Crime Victims". The purpose of the project was to further strengthen the institutional capacities of the law enforcement agencies and the social welfare and judicial systems; it is also aimed at improving public awareness in the area of the prevention and fight against the sexual exploitation and sexual abuse of children as well as in the area of police and judicial assistance to vulnerable crime victims. This strengthening is done by providing sustainable support which takes the form of establishing the system for further transfer of developed skills, knowledge and best practice and promotion of the holistic approach by cooperation between the relevant government agencies, NGOs and the business sector. The project consisted of two components (Twinning and Supply) which included the following activities: data collection and analysis of the Ministry of the Interior's and judicial system for fighting the sexual exploitation and sexual abuse of children, the adoption of

the Protocol on the Procedure in cases of child abuse and neglect, compiling the manual with Standard Operating Procedures on handling investigations into the sexual exploitation and sexual abuse of children, the establishment of a specialised Internet service to provide the necessary information to vulnerable victims of crime and the on-line reporting of crime, a public information campaign to encourage the reporting of crimes against children, guidelines for police officers on assistance to vulnerable crime victims, the training of police officers, prosecutors and judges in conducting criminal investigations into the sexual exploitation and sexual abuse of children, providing assistance to vulnerable crime victims, training in the use of technical equipment, and the training of police officers trainers, prosecutors and judges in order to transfer knowledge and skills further down the line.

Supply is the component that involves equipping the rooms for conducting interviews with children; IT equipment and forensic programmes that are intended to facilitate and improve criminal investigations and which are designed to search computers, mobile phones, media storage as well as data processing. The implementation of the project significantly raised the quality level of the situation of children victims in judicial proceedings and also in the procedures carried out by the police. During the project, from September 2011 to April 2013 in cooperation with police experts from the United Kingdom of Great Britain and Northern Ireland, there were five workshops attended by 100 police officers from all 20 police districts intended to provide a basic knowledge of various criminal acts against children on the Internet, a basic knowledge how to successfully conduct investigations, use open sources on the Internet in the police investigations. There were also workshops with practical exercises to improve the quality of criminal investigations and the collecting of evidence. Furthermore, at the advanced workshops 20 police officers were trained in the use of two forensic computer programs used by many police forces in the European Union (Net Clean Analyse DI and C4All) for the primary purpose of categorising the content of child pornography found during a search of the suspect's computer, in the construction and management of a database with child pornography, and finally in the identification of the victim as the only real and effective way to prevent further child abuse.

In addition, in cooperation with the Technical Assistance Information Exchange EU (TAIEX), a series of workshops aimed at strengthening the capacity of the police to combat the distribution of child pornography via the Internet was organised. Some topics at the workshops were: "Internet Intelligence Gathering - Open Source", "Crime Scene Searching", etc. Study visits to the EU Member States with greater experience in combating this type of crime were also organised. Croatia said it has taken and used access to the "Child Protection Software" as an effective way to combat child pornography.

National CERT has participated over the last 2.5 years in ACDC (Advanced Cyber Defence Centre), an EU project co-funded by EC. Croatia has benefited from the project since it launched the portal with free and commercial anti-malware tools for all Internet users in Croatia in order to help them to protect their workstations from infection. Croatia built a sensor network for the detection of spam and other malware campaigns affecting Croatia, with the goal of combating botnets. The evaluation team was informed of deeper cooperation between the Croatian CERT and partners in other Member States, such as Slovenia and Poland.

The Information Systems Security Bureau (ISSB) is financed through the annual Croatian state budget. ISSB does not have dedicated budget allocations for preventing and combating cybercrime nor does it receive EU funding.

3.5 Conclusions

- At the time of the on-site visit the first National Cyber Security Strategy, together with an Action plan for its implementation, was put forward for adoption. The evaluation team was informed after the on-site visit that the National Cyber Security Strategy was adopted on 7 October 2015 (Official Gazette 108/2015);

- The statistics on cybercrime are fragmented, as each competent authority keeps its own figures based on different criteria; overall, the statistics presented to the evaluation team do not seem to provide a clear picture on the situation as regards cybercrime in Croatia;

- During the on-site visit, some examples of good cooperation were presented by the national CERT, in particular with the Polish and Slovenian counterparts;

- Croatia participates in EUCTF, EMPACT CCF and EMPACT CA - and is particularly active in the latter; at the time of the on-site visit the country did not participate in EMPACT CSE, due to a lack of sufficient qualified resources;

- Croatia is also participating in a twinning project ″Strengthening capacities of the Ministry of Interior to combat Cybercrime", jointly with Spain and Austria.

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

When it comes to the prosecution of perpetrators of criminal and other offences, including cybercrime, the tasks are performed by the State Attorney's Office of the Republic of Croatia, the 15 county State Attorney's offices, the 22 municipal State Attorney's offices and the Office for the Suppression of Corruption and Organised Crime, as the special State Attorney's Office.

The State Attorney's Office is an independent and autonomous judicial body, headed by the Chief State Attorney of the Republic of Croatia. The internal structure of the State Attorney's offices mostly includes criminal and civil-administrative departments, and the Croatian State Attorney's Office has four departments (Criminal Department, Civil-Administrative Department, Internal Audit Department and the Department for Mutual Legal Assistance and Cooperation).

The Croatian authorities said that given the relatively small number of criminal offences against computer systems, programmes and data, there are no State Attorney's Offices in Croatia that specialise in computer crime.

Municipal and county courts as the courts of general jurisdiction are competent to deal with cybercrime. If these acts are, at the same time, under the jurisdiction of the Office for Combating Corruption and Organised Crime, the criminal proceedings will be conducted before the Municipal Criminal Court in Zagreb (there are especially organised departments for dealing with criminal offences under the jurisdiction of the Office), the municipal courts in Osijek, Rijeka and Split, and the four largest county courts in Zagreb, Split, Rijeka and Osijek.

4.1.2 Capacity and obstacles for successful prosecution

Following the ratification of the Convention on Cybercrime and the harmonisation of criminal legislation with the Convention, the State Attorney's Office in Croatia has already begun the preparations in terms of personnel and organisation, for the purpose of the efficient prosecution, investigation and processing of all forms of cybercrime. The latest amendments to the CC and the new position of the State Attorney under the CPA, according to which the State Attorney has been assigned a leading role in directing and conducting inquiries and investigations into these types of criminal offences as well, has seen new tasks and responsibilities conferred on the State Attorney's Office.

The Act on the areas and seats of State Attorney's offices (Official Gazette 128/14), led to a rationalisation of the network of State Attorney's offices, meaning the unification and merger of smaller State Attorney's offices into larger ones. This rationalisation and organisation of the State Attorney's offices, which are competent to deal with offences related to cybercrime, ensures effective search and investigation in the area of cybercrime, with constant liaison between the offices and the specialised Department for High Technology Crime within the police.

In the larger State Attorney's offices (Zagreb, Novi Zagreb, Velika Gorica, Split, Rijeka, Osijek), State Attorneys and deputies who work on matters of cybercrime are listed in the annual work schedule.

The State Attorney's Office has the institutional and human resources for the successful prosecution of cybercrime. A certain number of State Attorneys have specially been trained through the programme of the Judicial Academy in the implementation of several projects financed by the European Union (CARD and IPA programmes related to capacity building and the fight against cybercrime). Cybercrime requires not only basic training, but also special training and continuous improvement for the purposes of successful targeting, detection, investigation, prosecution and imposing sanctions.

During the regional IPA Project in 2010, the State Attorneys and deputy State Attorneys were actively engaged in education and training programmes for trainers. As part of the Regional Centre of the Judicial Academy for training judges and prosecutors, one of the coaches is from the ranks of prosecutors.

Through such additional specialist training in the State Attorney's Office, a group of State Attorneys has been formed who can deal with cases of cybercrime effectively, and also provide assistance to other State Attorneys in the Republic of Croatia.

Croatia pointed out that the introduction of the CTS system (Case Tracking System - a system for tracking criminal cases) allows the State Attorney's Office of the Republic of Croatia to statistically monitor the work of State Attorneys at all stages of the proceedings. Such monitoring makes it possible to detect defects and shortcomings in good time, and to point out the need to improve the work on these cases and conduct additional training, if needed. This will certainly improve the operation and efficiency of investigation and prosecution, and eventually lead to appropriate sanctions being imposed on the perpetrators of cybercrime.

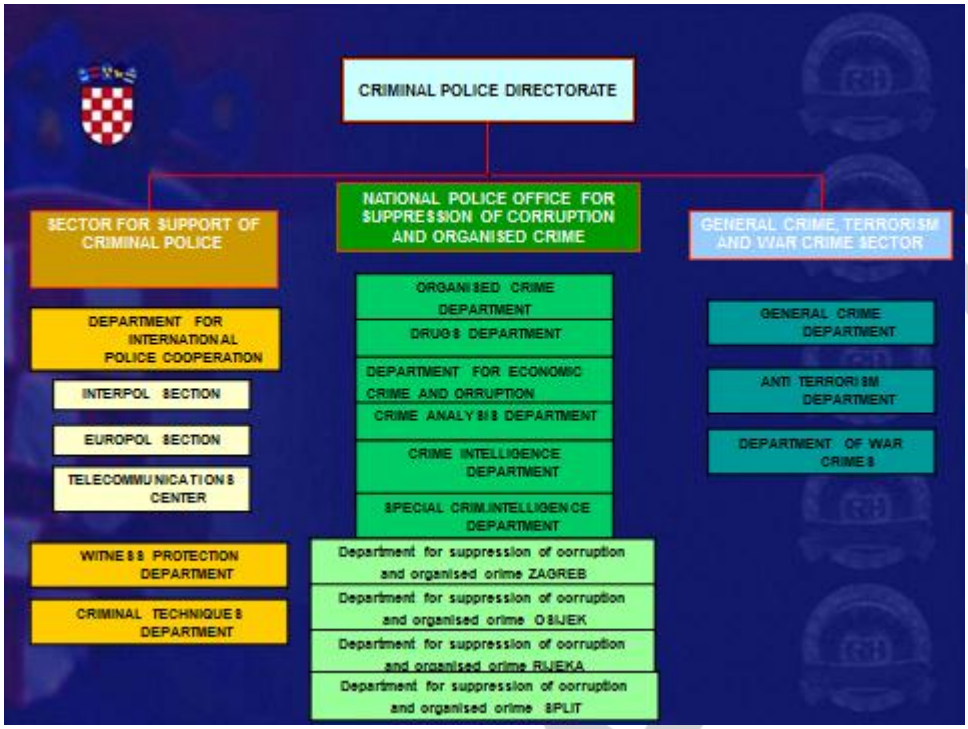
In practice, problems have been identified in the prosecution of perpetrators of computer crime, especially the offence of computer fraud laid down in Article 271 of the CC, in cases with an international element. Croatia has noticed an increased number of attacks with malicious computer programs to the detriment of users of Internet systems of Croatian commercial banks. These programs allow unauthorised bank transactions from the account of the victims to the accounts of private individuals or legal entities in Croatia or abroad (i.e. financial mules) who then raise money via Western Union or similar financial service providers and submit it to intermediaries or perpetrators abroad. The intermediaries, or so-called financial mules, keep a portion of the money, which is transferred to their current accounts.

Determining the identity of the perpetrators is more difficult when they are foreign citizens and the criminal offence is committed abroad while the consequence of the offence is suffered in Croatia. The Croatian authorities said that, although such cases are dealt with promptly and the "instruments" of judicial cooperation such as orders freezing property or evidence are used (Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence), in practice the perpetrator is rarely found, and the interim measures, in order to ensure the confiscation of material benefit from the crime, are rarely ordered.
During 2014, the State Attorney's Office of the Republic of Croatia issued 16 orders freezing property or evidence in proceedings related to computer fraud as laid down in Article 271 of the CC. There has not been a single case in which interim measures to ensure the confiscation of material benefit from crime have been ordered, because at the time of the orders freezing property or evidence were issued, the disputed funds had already been withdrawn from the bank accounts and were no longer in the bank accounts or were insufficient for the execution of the interim measures of confiscation of such material benefit.

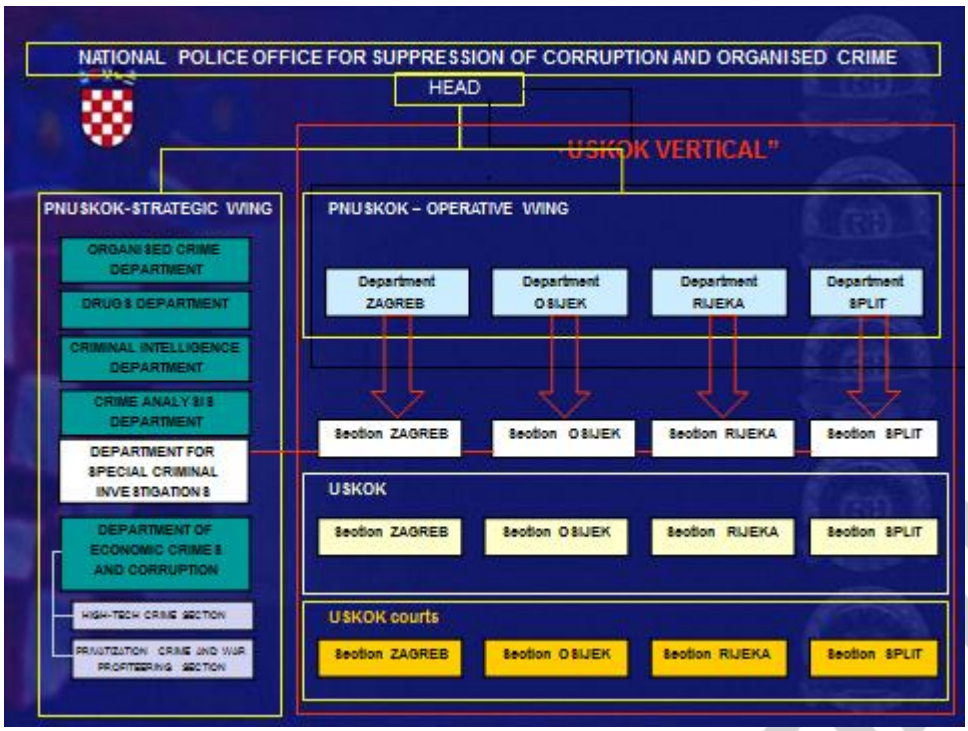
4.2 Law enforcement authorities

National level

A police department at national level, the **Criminal Police Directorate,** is responsible for investigations into all types of crime, including cyber-crime.

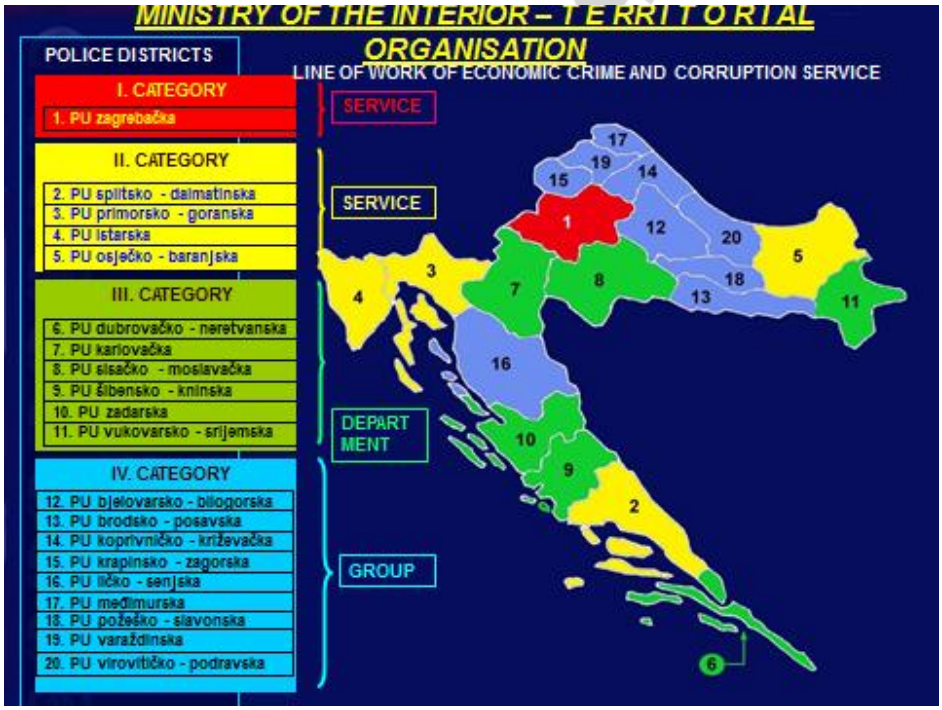


In 2008 a new unit called the **Police National Office for Suppression of Corruption and Organised Crime (PNUSKOK)** was established as part of this Directorate. PNUSKOK consists of a central, strategic wing (within the Criminal Police Directorate) and 4 regional departments in four major Croatian cities. This structure is organisationally compatible with the structure of the Office for Suppression of Corruption and Organised Crime (USKOK). The basic principles governing the operation of national units are adaptability and flexibility. A high-Tech Crime Unit is an integral part of the PNUSKOK and is responsible for fighting cybercrime at national level. See below the structure of the Police National Office for Suppression of Corruption and Organised Crime:



Regional Level

There are 20 regional police forces within Croatia, called **Police Administrations**. They carry out the police work of the Ministry of the Interior within the territory of their county. The Police Administrations are divided into 4 categories. See below the territorial structure of the regional police units :



For the time being, the **High-Tech Crime Unit** operates at national level only. In 20 regional police forces dedicated police officers within the Economic Crime Units are responsible for cybercrime investigations in addition to their other police duties e.g. carrying out economic crime investigations and crime analysis (see the chart below):

The High-Tech Crime Unit is responsible for investigations of tye cyber-crime offences indicated in the Council of Europe Cyber Crime Convention: unauthorised access, obstruction of computer systems, damage to computer data, unauthorised interception of computer data, computer forgery, computer fraud, misuse of devices, and serious offences against computer systems, programs and data. The High-Tech Crime Unit is responsible for investigating criminal offences against intellectual property and the criminal offence of counterfeiting medicines or medical products.

At the time of the visit the High-Tech Crime Unit was not responsible for investigations involving child pornography on a computer system or network (the Juvenile Delinquency and Crimes against Children and Family Unit has this responsibility) or for bank card fraud (here responsibility lies with the Organised Crime Department within PNUSKOK). Since October 2015, the High-Tech Crime Unit together with Juvenile Delinquency and Crimes against Children and Family Unit has taken on this responsibility.

The Juvenile Delinquency and Crimes against Children and Family Unit is the central police body at national level that monitors and analyses crimes against children, particularly those involving the sexual exploitation of children and young persons via the Internet. The jurisdiction of the Department includes; monitoring new forms of crimes; determining the most appropriate form of preventing such crimes and providing expert assistance to police departments; supervising, organising and undertaking criminal investigations into more complex crimes at national level. Furthermore, the Department is responsible for cooperation with other governmental bodies and civil society organisations, international organisations, other bodies and it also participates in the drafting of normative acts. The police officers in the Department are also responsible for victim identification and work on Interpol's International Child Sexual Exploitation Database - ICSE - and NCMEC reports are delivered through the SIENA channel. The Protocol on the Procedure in cases of child abuse and neglect standardises the procedures in the abovementioned framework, which includes multi-sector cooperation aimed at supporting child victims. The above mentioned cooperation means that police should immediately inform the competent social welfare authority about the sexual exploitation of a child in order to ensure that the child receives help and support.

One of the victim's fundamental rights is to be properly informed, and to that end the police inform victims of all their general and specific rights during the first contact. A written form of these rights is therefore delivered to the child and his or her custodian in a standardised form. Police officers specially trained to deal with young people interview child victims of sexual exploitation.

At national level the Department of Juvenile Delinquency and Crimes against Children and Family is in charge of the criminal investigations involving the sexual abuse of children (including abuse on the Internet). This Department, whose jurisdiction and characteristics are outlined above, employs six police officers, two of them primarily responsible for: implementation, monitoring and coordination of complex crime investigations into child abuse and exploitation via the Internet. These officers also provide technical assistance to the police districts, in addition to monitoring and responding in connection with the online reporting system "Red Button" and NCMEC reports. Furthermore, these two officers of the Department are responsible for identification of the victim and work on Interpol's international child pornography database, ICSE.

At the regional level of the police districts, departments or groups (depending on the size of the police district) have been set up to deal with juvenile delinquency and crimes against children and the family. Furthermore, at the local level, all police stations have a police officer with responsibility for young people. All such officers in the Republic of Croatia have passed a specialised course that trains them to conduct investigations into crimes against children and to work with child victims. In addition to the general course intended for the police officers working with young people, many of these officers have undergone various forms of additional training; there are courses organised by the Police Academy, as well as IPA projects, TAIEX workshops and international seminars and training courses.
In Croatia there are 260 specialist police officers dealing with young people.

The **"Ivan Vučetić" Centre for Forensic Science Research and Expertise** is an organisational unit of the police in charge with the process of transformation of material trace exempted from the place of committing a criminal offence in the valid physical evidence. It is based in Zagreb. The centre is a public institution which specialises in forensics and which carries out criminal - technical works and expertise, and which is directly involved in the detection of almost all crimes and their perpetrators on national territory.

The Centre has been in existence for almost six decades , during which time it has grown into a modern institution that can stands side by side with European and world forensic institutes. Since 1998, the Centre has been a full member of ENFSI (European Network of Forensic Science Institutes) - an umbrella organisation of Europe's national forensic institute, which brings together a total of 56 members from almost all the countries of Europe. There are two digital forensic examiner posts at the Centre. The evaluation team has been informed of the heavy workload of these examiners.

Police powers can be exercised in the course of investigations involving all criminal offences and there are no special police powers related to cyber-crime investigations.

The Criminal Police Directorate conducted an IPA 2009 project entitled "Capacity Building in the Field of Fight against Sexual Exploitation and Sexual Abuse of Children, and on Police Assistance to Vulnerable Crime Victims".

In addition to this project, there has been cooperation with the EU information exchange (TAIEX) on a series of workshops aimed at strengthening the capacity of the police to combat the distribution of child pornography via the Internet. Police officers are sent to various seminars and training courses organised by CEPOL.

Also, at the Police Academy, a variety of educational programs and professional courses are organised for police officers carrying out criminal investigations in this area.

The Police Academy, CEPOL and other bodies will in the future continue to cooperate in the provision of education and training for police officers dealing with criminal investigations of this kind.

4.3 Other authorities/institutions/Public Private Partnership

The Croatian Regulatory Authority for Network Industries (HAKOM), with its seat in Zagreb, is a legal entity with public authority within the scope and competence prescribed by the Electronic Communications Act that entered into force on 1st July 2008 and a special law regulating the field of postal services. HAKOM is an independent, autonomous and non-profit legal entity with public authority. The work of HAKOM is public. HAKOM is governed by a Council consisting of five members, including the Chairman and Deputy Chairman. The Chairman, Deputy Chairman and members of the Council are appointed for a period of five years and dismissed by the Croatian Parliament on the proposal of the Government of the Republic of Croatia. The Council of HAKOM adopts decisions by majority vote. HAKOM has an administrative service performing the expert, administrative and technical tasks of the Agency. The administrative service is organised in accordance with the HAKOM's statutes and its other internal rules. The competence of HAKOM is prescribed by Article 12 of the Electronic Communications Act (OG 73/08) and Article 38 of the Act on Postal Services (OG 88/09).

HAKOM strategic goals are:

to promote regulation of the electronic communications market;
to promote regulation of the postal services market;
to support growth of investments and innovations in the electronic communications market;
to support growth of investments and innovations in the postal services market;
to provide for the efficient use of limited resources;
to accelerate the growth of broadband products and services;
to provide affordable offers of communications and postal services;
to improve the protection of and the provision of information to users;
to build an efficient, comprehensive information system;
to define and implement efficient processes;
to acquire multi-disciplinary competencies in market regulation.

National CERT. Under Information Security Act, the Croatian national CERT is a national body for preventing and defending against computer threats to the security of public information systems in the Republic of Croatia. (2) CERT is a separate organisational unit which is organised within the Croatian Academic and Research Network (hereinafter: CARNet). (3) CERT coordinates security procedures for incidents within public information systems which occur in the Republic of Croatia or in other countries and organisations when they relate to the Republic of Croatia. (4) It coordinates the activities of bodies which operate to prevent and defend against computer threats to the security of public information systems in the Republic of Croatia and also determines the rules and methods of joint operations.

The **Information Systems Security Bureau (ISSB)** is the central state authority for the security of information and network systems of government bodies, local and regional governments and legal entities with public authority. As such, its most important activity is providing assistance to the state authority bodies of the Republic of Croatia in the implementation of preventive measures for reducing the risk of computer security incidents and, when an incident does occur, it is responsible for incident removal or intermediates in the process of incident removal. Cyber security for government bodies includes the prevention of computer security incidents and responding to computer security incidents. ISSB helps the LEA on request with expert knowledge in an LEA-led criminal investigation.

The technical areas of information systems security in which ISSB is involved are:

1. information systems security standards;
2. security accreditation of information systems;
3. management of encoded material used for exchanging classified information;
4. co-ordination of prevention and solutions for computer threats to information system security.

The national CERT and ISSB co-operate in the prevention and defence against computer threats to information systems security and also co-operate in drafting recommendations and norms in the Republic of Croatia within the area of information systems security.

ISSB as the government CERT has the task of coordinating the prevention of any computer security incident, some of which can often be classified as cybercrime within its area of responsibility. ISSB is responsible for government bodies, local and regional governments and legal entities with public authorities.

Under the Information Security Act the national CERT is responsible for coordination and incident handling on publicly accessible information systems in the country. It has a staff of 9 and its capabilities comprise incident response, the forensics of incidents and malware, together with cyber threat intelligence powered by collection and analysis of information related to cyber incidents.

With the scope of its activities ISSB is responsible for coordinating the prevention and removal of computer security incidents, some of which can be classified as cybercrime.

4.4. Cooperation and coordination at national level

4.4.1 Legal or policy obligations

Under the Regulation on the method and terms of implementation of measures to protect the security and integrity of networks and services (hereinafter: The Regulation), operators are required to annually submit to Croatian Regulatory Authority for Network Industries (HAKOM) a documented security policy for the previous year covering the security measures taken and the corresponding standards. Operators are required to notify HAKOM:

- In the case of security incidents related to the Internet in accordance with the criteria for reporting in Appendix 2 of the Regulation;

- In the case of unauthorised connection to the public telephone network or part of the network and in the event of a breach of security or integrity of public communications services, which significantly has impacted the performance of the public communications networks and / or services in accordance with the criteria for reporting in Appendix 2 of the Regulation;

Article 204 of the Criminal Procedure Act provides that anyone with knowledge of a criminal activity or material is obliged to report a criminal offence for which the procedure is initiated ex officio, no matter whether that knowledge came after a tip-off or was brought to the subject's attention. Croatia thus has practical examples of Internet service or hosting providers reporting that their services have been used by some of their users for distribution of child pornography.

In Croatia cooperation with the private sector in terms of cybercrime and cybersecurity is mainly regulated by the Electronic Communications Act and the Law on Electronic Commerce. This Act imposes certain obligations on Internet service providers to make investigations more successful. In particular, Article 109 stipulates that the public communication network providers and the providers of publicly available electronic communication services retain the electronic data for the detection, investigation and prosecution of criminal offences.

The National Cyber Security Strategy also provides some guidelines for cooperation between private and public sector.

Cooperation between the card industry, the banks, the police and the state prosecutors is the responsibility of the Payment Card Fraud Committee. This Committee operates within the Croatian Banking Association and is composed of representatives from the banks, the prosecution service and the police. Its activities are carried out at the working meetings held quarterly (4 times a year). At these meetings the Committee exchanges information on new forms of abuse and new protection technologies.

Information from members of the Payment Card Fraud Committee is shared via an e-mailing list, protected by PGP keys. The Committee trains employees of banks, state prosecutors and the police. It annually organises workshops where participants are informed of new developments and technologies. All Croatian issuers of credit cards have moved to chip technology (EMV Europay, MasterCard, Visa standards). Strengthening the authorisation code online transaction takes place using the "3D Secure" technology, and using the latest technology with the option of monitoring pro-active action which recognises fraudulent transactions.

Police officers are involved in multidisciplinary work aimed at providing an effective national response to the threat of cyber-crime. There is ongoing cooperation with the National CERT (National Computer Emergency Response Team). An agreement on cooperation in the prevention and resolution of computer incidents and other forms of computer crime was signed on 15 February 2015 between the Ministry of Interior, the Ministry of Science, Education and Sports and the Croatian Academic and Research Network (CARNet), as the National CERT.

The agreement includes:
-Resolving computer security incidents in which at least one of the parties is from Croatia;
-Prevention of computer security incidents;
-Increasing security for users of computer and information technology;
-Cooperation with other relevant institutions and bodies in the drafting of appropriate legislative solutions to monitor the development of society, requiring the need for specialised training of police officers, use of special equipment and the application of specific methods necessary for effectively combating forms of computer crime;

Continuing cooperation between the police and the *Information Systems Security Bureau (ISSB)* is ongoing as well, especially as regards the coordination of prevention and response to computer threats to information security.

4.4.2 Resources allocated to improve cooperation

There are no resources allocated specially for cooperation with the private sector.
Police officers investigating online card fraud are assisted in their investigations by the High-Tech Crime Unit police officers at national and/or regional level if forensic examination is needed. Forensic software and hardware used while investigating cyber-attacks is used in online card fraud cases as well. Since the number of cybercrime investigations requiring the use of computers and/or online forensics will grow in the future, this should be reflected in the number of police officers trained in computer and online forensics.

In practice, cooperation with the private sector in the prevention of and fight against cybercrime so far has been deemed generally successful.

When it comes to cooperation where the private sector is the victim or the party that has suffered loss, cooperation is usually very good, according to the Croatian authorities. In most cases the private sector assists the police in clarifying the circumstances related to the criminal offences and in providing the necessary data, preserving evidence etc. Cooperation is best with the financial sector (banks), especially regarding banking malware and computer frauds related to Internet banking. The majority of bank branches in Croatia are members of the Croatian Banks Association and the work of Association is organised within boards. A representative of the High-Tech Crime Unit sits on the Information Security Board that meets once a month and discusses all cybercrime and cybersecurity issues.

The Croatian authorities said that, as regards online card fraud, the equipment, resources, capacities and knowledge of the body in charge (the law enforcement agencies) are satisfactory. They also acknowledged that, taking into account the dynamics of the crime, cooperation needs to be promoted between the authorities in charge of law enforcement and all participants in the card business (credit card industry, banks, processors, suppliers).

4.5 Conclusions

- In general, Croatia has in place standard structures to deal with cybercrime; while various forms of cooperation exist among some of them, the country would benefit from better coordination between all stakeholders;

- The Central Unit in charge of high-tech crime is composed of only 5 policemen who coordinate investigations across the entire country and their responsibilities also cover international police cooperation and training activities in the field; card fraud is the responsibility of the Organised Crime Department; however, both services cooperate according to needs and availability;

- Child abuse via computer systems or networks is covered by the Department of Juvenile Delinquency and Crimes against Children and Family;

- It is acknowledged that police at local level should be better prepared to understand cybercrime issues.

- There are no state attorneys or judges specialising in computer or cybercrime matters; although the Croatian authorities indicated that some State attorneys have been trained to deal with cases of cybercrime effectively and to provide assistance to colleagues, there is still a need for additional structures dedicated to improving the efficiency of the fight against cybercrime at prosecution level as well as at court level (e.g. establishment of contact points);

- The Croatian authorities in charge of cybercrime have regular cooperation and meetings with the banking sector; however, a need to develop structured public/private partnerships has been identified, in particular in terms of cooperation between law enforcement authorities and service providers.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on cybercrime

The Republic of Croatia is Party to the CoE Convention on Cybercrime. On 3 July 2002, the Croatian Parliament adopted the Act on the Ratification of the CoE Convention on Cybercrime. The Convention entered into force with respect to the Republic of Croatia on 1 July 2004.
In accordance with commitments under the Convention, amendments to the Criminal Code were adopted in 2004. On the 26th March 2003 the Republic of Croatia signed the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. While the Additional Protocol entered into force on 21 June 2008, amendments to the Criminal Code of 2004 provided for the offence of racial and other forms of discrimination, laying down that denying, significantly reducing, approving or justifying the crime of genocide or crimes against humanity committed through computer systems are criminal offences.

5.1.2 Description of national legislation

The CC punishes intent to commit a criminal offence, but it also sets out a penalty for negligence.

Article 28 of the CC thus prescribes that a criminal offence may be committed with direct or indirect intent. A perpetrator acts with direct intent when he or she is aware of the material elements of a criminal offence and wants or is certain of their realisation, and acts with indirect intent when he or she is aware that he or she is capable of realising the material elements of a criminal offence and accedes to this.

Article 29 of the CC prescribes punishment for negligence and specifies that a criminal offence may be committed by advertent or inadvertent negligence. The perpetrator acts with advertent negligence when he or she is aware that he or she can realise the material elements of a criminal offence but carelessly assumes that this will not occur or that he or she will be able to prevent this from occurring. The perpetrator acts with inadvertent negligence when he or she is unaware that he or she can realise the material elements of a criminal offence, even though under the circumstances he or she should and, by virtue of his or her personal characteristics, could have been aware of such a possibility.

In relation to mitigating and aggravating factors, Article 47 of the CC prescribes what the court will take into account when assessing the punishment. When determining the type and range of punishment, the court will, starting from the degree of culpability and the purpose of the punishment, assess all the circumstances affecting the severity of the punishment by type and range (mitigating and aggravating circumstances), and especially the degree of threat to or violation of a legally protected good, the motives for having committed the criminal offence, the degree to which the perpetrator's duties have been violated, the manner of commission and the inculpatory consequences arising from the commission of the criminal offence, the perpetrator's prior life, his or her personal and pecuniary circumstances and his or her conduct following the commission of the criminal offence, the relationship to the victim and efforts to compensate for the damage.

Furthermore, in the case of multiple criminal offences or reoffending, the court will, under Article 418 paragraph 5 of the Criminal Procedure Act (“Official Gazette” nos. 152/08, 76/09, 80/11, 121/11 - consolidated text, 91/12 - Decision of the Constitutional Court of the Republic of Croatia, 143/12, 56/13, 145/13 and 152/14, hereinafter: the CPA), during the evidentiary proceedings as the last evidence at the close of those proceedings and before proceeding to the interrogation of the accused, read the data from criminal records as well as other data on convictions for punishable offences. Likewise, when determining the punishment for the perpetrator, the court will, under Article 47 of the Criminal Code, inter alia, assess the perpetrator's prior life.

The provisions of Articles 36, 37, 38 and 39 of the CC refer to the principal, solicitation, aiding and abetting and punishment of co-principals and accomplices.

Article 36 of the CC defines a principal as any person who commits the offence himself or herself or through another. If more than one person commits the criminal offence on the basis of a joint decision and each one of them takes part in or otherwise substantially contributes to the commission of the criminal offence, each shall be punished as the principal (joint principals or co-principals), while co-principals are liable for negligence on the basis of a joint violation of due care.

Provisions on solicitation are laid down in Article 37 of the CC. In that part, the Code prescribes that whoever intentionally incites another to commit a criminal offence will be punished as if he or she himself or herself had committed it. Likewise, whoever intentionally incites another to commit a criminal offence for which an attempt is punishable, but the solicited offence has never been attempted, will incur the penalty laid down for an attempt to commit such an offence. In the case of an inappropriate attempt of solicitation, the person who solicits may receive reduced sentence.

Under Article 38 of the CC, whoever intentionally aids and abets another in the commission of a criminal offence must be punished as if he or she committed the offence himself or herself.

Regarding the punishment of accomplices, under Article 39 of the CC, each co-principal and secondary participant (the persons who solicits and the aider and abettor) will be punished according to his or her own guilt and if the law proscribes that special personal circumstances remit or mitigate punishment or influence the seriousness of criminal offence, this will apply only with respect to the co-principal or secondary participant in whose person such special personal circumstances are present.

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

By adopting the Act on Amendments to the CC in 2015, the Republic of Croatia transposed into national legislation Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems. Taking into account the short period that has elapsed since the transposition of the Directive into national legislation, the Republic of Croatia has had no difficulties in its implementation so far.

Title XXV of the CC regulates criminal offences against computer systems, programs and data as follows:

Unauthorised Access

Article 266

(1) 'Whoever accesses a computer system or computer data without authorisation shall be punished by imprisonment not exceeding two years.

(2) Whoever commits the criminal offence referred to in paragraph 1 of this Article with respect to a computer system or computer data of a state authority, the Constitutional Court of the Republic of Croatia and an international organisation of which the Republic of Croatia is a member, a body of local or regional self-government, public institution or company of special public interest, shall be punished by imprisonment not exceeding three years.

(3) An attempt to commit the criminal offence referred to in paragraphs 1 and 2 of this Article shall be punishable.

(4) The person who commits the criminal offence referred to in paragraph 1 of this Article shall be prosecuted upon request.

Computer System Interference

Article 267

(1) Whoever prevents or hinders the functioning or use of a computer system, computer data or programs, or computer communication, shall be punished by imprisonment not exceeding three years.

(2) An attempt to commit the criminal offence referred to in paragraph 1 of this Article shall be punishable.

Damage to Computer Data

Article 268

(1) Whoever damages, alters, deletes, destroys, renders unusable or inaccessible, or presents as inaccessible, in full or in part, another's computer data or programs without authorisation, shall be punished by imprisonment for a term of up to three years.

(2) An attempt to commit the criminal offence referred to in paragraph 1 of this Article shall be punishable.

Unauthorised Interception of Computer Data

Article 269

(1) Whoever intercepts or records without authorisation non-public transmissions of computer data, including electromagnetic emissions from a computer system, or makes available to another the data thus procured, shall be punished by imprisonment not exceeding three years.

(2) An attempt to commit the criminal offence referred to in paragraph 1 of this Article shall be punishable.

(3) The data derived from the commission of the criminal offence referred to in paragraph 1 of this Article shall be destroyed.

Computer-related Forgery

Article 270

(1) Whoever produces, inputs, alters, deletes, or renders unusable or inaccessible without authorisation computer data of value to legal relations with the intent that they be used as authentic, or whoever uses or procures for use such data, shall be punished by imprisonment not exceeding three years.

(2) An attempt to commit the criminal offence referred to in paragraph 1 of this Article shall be punishable.

(3) The data derived from the commission of the criminal offence referred to in paragraph 1 of this Article shall be destroyed.

Computer-related Fraud

Article 271

(1) Whoever, with the aim of acquiring for himself or herself or another an unlawful material gain, inputs, alters, deletes, damages, renders unusable or inaccessible computer data or interferes with the functioning of a computer system and thus causes damage to another, shall be punished by imprisonment from six months to five years.

(2) If as a result of the criminal offence referred to in paragraph 1 of this Article, a considerable material gain is acquired or considerable damage is caused, the perpetrator shall be punished by imprisonment from one to eight years.

(3) The data derived from the commission of the criminal offence referred to in paragraphs 1 and 2 of this Article shall be destroyed.

Misuse of Devices

Article 272

(1) Whoever produces, procures, imports, sells, possesses or makes available to another devices or computer programs or computer data designed or adapted for the purpose of committing any of the criminal offences referred to in Articles 266, 267, 268, 269, 270 and 271 of this Code with the intention that it be used for the purpose of committing any of the criminal offences laid down in Articles 266 through 271 shall be punished by imprisonment not exceeding three years.

(2) Whoever produces, procures, imports, sells, possesses or makes available to another computer any password, access code or other data by which a computer system is capable of being accessed with the intention that it be used for the purpose of committing any of the criminal offences referred to in Articles 266, 267, 268, 269, 270 and 271 of this Code, shall be punished by imprisonment not exceeding two years.

(3) The perpetrator of the criminal offence referred to in paragraph 1 of this Article shall not be liable to a punishment that is more severe than that prescribed for the criminal offence the perpetrator intended to commit.

(4) The special devices and programs referred to in paragraph 1 of this Article shall be forfeited while the data referred to in paragraphs 1 and 2 of this Article shall be destroyed.

Serious Criminal Offences against Computer Systems, Programs and Data

Article 273

(1) Whoever commits any of the criminal offences referred to in Articles 267 up to and including 270 of this Code with respect to a computer system or computer data of a state authority, the Constitutional Court of the Republic of Croatia and an international organisation of which the Republic of Croatia is a member, a body of local or regional self-government, public institution or company of special public interest, shall be punished by imprisonment from six months to five years.

(2) The same punishment as referred to in paragraph 1 shall be inflicted on whoever commits any of the criminal offences referred to in Articles 266 through 269 of this Code by concealing his or her real identity and giving rise to an error about the authorised identity holder.
(3) Whoever commits any of the criminal offences referred to in Articles 267 up to and including 269 of this Code through the use of a tool designed to launch attacks affecting a larger number of computer systems, or hereby occasions considerable damage, shall be punished by imprisonment from one to eight years.

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

By adopting the Act on Amendments to the CC and the Act on Amendments to the CPA (Official Gazette 145/13), Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA was transposed into Croatian legislation. The same Directive was transposed through the Juvenile Courts Amendment Act (OG 84/11, 143/12, 148/13 and 56/15).

The Republic of Croatia hasn't experienced any difficulties regarding the implementation of this Directive. Title XVII of the CC specifically regulates the criminal offences of sexual abuse and sexual exploitation of children, as follows.

Child Enticement for the Purpose of Satisfying Sexual Needs

Article 161

(1) An adult who, with the intention that he or she or a third party commits the criminal offence referred to in Article 158 of this Code against a person under the age of fifteen, proposes to this person, through information and communication technologies or in some other way, to meet up with him or her or a third party, where this proposal is followed by material acts leading to such a meeting, shall be punished by imprisonment not exceeding three years.

2) Whoever collects, gives or transfers data on a person under the age of fifteen for the purpose of committing the criminal offence referred to in paragraph 1 of this Article shall be punished by imprisonment not exceeding one year.

(3) An attempt to commit the criminal offence referred to in paragraph 1 of this Article shall be punishable.

Exploitation of Children for Pornography

Article 163

(1) Whoever entices, recruits or incites a child to participate in the child pornography or whoever organises or makes possible the production of child pornography shall be punished by imprisonment from one and eight years.

(2) The same punishment as referred to in paragraph 1 of this Article shall be imposed on whoever films child pornography or produces, offers, makes available, distributes, transmits, imports, exports, procures for himself or herself or for another person, sells, gives, presents or possesses child pornography or knowingly obtains access, through information and communication technologies, to child pornography.

(3) Whoever by means of the use of force or threats, deception, fraud, abuse of authority or of a situation of hardship or dependence coerces or induces a child to participate in child pornography shall be punished by imprisonment from three to twelve years.

(4) Special devices, means, computer programs or data intended for, adapted to or used for committing or facilitating the commission of the criminal offences referred to in paragraphs 1, 2 and 3 of this Article shall be confiscated, while the pornographic material that was created by the commission of the criminal offences referred to in paragraphs 1, 2 and 3 of this Article shall be destroyed.

(5) A child shall not be punished for producing and possessing pornographic material depicting him or her alone or him or her and another child, where this material is produced and possessed by them with their consent and solely for their own private use.

(6) Child pornography shall mean any material that visually or otherwise depicts a real child or a realistic image of a non-existent child or a person appearing to be a child, involved or engaged in real or simulated sexually explicit conduct, or any depiction of a child's sexual organs for sexual purposes. For the purpose of this Article, any material that is artistic, medical or scientific in character shall not be deemed pornography.

C/ Online Card fraud

Citizens usually do not report online payment card fraud. Usually, citizens / customers are not even aware that payment card fraud has occurred. Most commonly bank/card issuer detects fraud during the monitoring of transactions. Banks report online payment card fraud to the police.

5.2 Procedural issues

5.2.1 Investigative Techniques

Pursuant to Article 332, paragraph 1 of the CPA, it is permitted to conduct special evidentiary actions where criminal acts are committed against computer systems, programs and data, and the interception, collection and recording of computer data is allowed.

Furthermore, Article 257 of the CPA lays down the rules for the search and seizure of information systems / computer data. It is provided that searches of movable property include a search of computers and related devices, other devices for the gathering, storage and transfer of data, telephone, computer and other communications and data carriers. At the request of the authority that is conducting the search, the person who uses the computer or has access to the computer or other device or data carrier, or the provider of telecommunication services, is obliged to provide access to the computer, the device or data carrier and provide the information necessary for the smooth realisation of the objectives of the search. By order of the authority conducting the search, the person who uses the computer or has access to the computer and other specified devices and the provider of telecommunications services are obliged to take immediate measures to prevent the destruction or modification of data. The authority that undertakes the search can order a professional assistant to implement the measures.

Article 261 of the CPA (on the basis of Article 263 of the CPA) applies to data stored on computers and related devices and devices for generating and transferring files, data carriers and subscriber information available to the service provider. The above-mentioned article provides that objects that are to be seized under the CPA, or that could be helpful in establishing the facts in the process, will be temporarily seized and their preservation will be ensured, and the person in possession of such objects must turn them over at the request of the State Attorney, the investigators or the police. The State Attorney, the investigator or the police will warn the holder of the subject about the consequences arising from the refusal to act upon the request. The complete recording and documentation must be sealed and kept in the State Attorney's Office (Article 338, paragraph 2 of the CPA).

Under Article 263 of the CPA, such data must be submitted to the State Attorney on written request and in a complete, original, readable and understandable form. In the request, the State Attorney will specify the period in which the data must be submitted. The authority that is carrying out the action will record the relevant data in real time. Obtaining, recording, protecting and storing the data will take into account in particular the regulations relating to the confidentiality of certain data (Article 186 to 188 of the CPA). Data that is not related to the criminal offence and that is needed by the person against whom the measure is directed, can be recorded on appropriate means and returned to that person before the end of the proceedings.

At the proposal of the State Attorney, the investigating judge may decide to order the protection and storage of computer data stored on the computer, for as long as is necessary, but for no longer than six months. The computer data will then be returned unless, inter alia, it has been used in the commission of offences against computer systems, programs and data in accordance with the Criminal Code.

In the case of suspected criminal offences against computer systems, programs and data, except in the case of searches (Article 257 of the CPA), special evidentiary actions can be carried out (Article 332 of the CPA).

In the event of a search, the law provides that at the request of the authority carrying out a search, the person using a computer or having access to a computer or another device or data carrier as well as a telecommunications service provider must allow access to a computer, device or data carrier and provide the necessary information allowing for unhindered use and enabling the goals of the search to be achieved. Also, upon the order of the authority carrying out a search, the person using a computer or having access to a computer and other devices referred to in paragraph 1 of this Article or a telecommunications service provider must immediately take measures aimed at preventing the destruction or modification of data.

Special evidentiary actions under Article 332 of the CPA must be carried out if an investigation cannot be conducted otherwise or where this would entail disproportionate difficulty. Upon a written request from the State Attorney that includes a statement of reasons, the investigating judge may order, by a written warrant which includes a statement of reasons, that measures be taken. These will be directed against a person in respect of whom there are grounds for suspecting that he committed or together with other persons participated in the commission of a criminal offence against computer systems, programmes and data. These measures comprise the following special evidentiary actions temporarily restricting certain constitutional rights of citizens, inter alia: surveillance and technical recording of telephone conversations and other remote communications, as well as the interception, collection and recording computer data.

Investigative techniques used for investigating cyber -related crimes always depend on the type of investigation, on the modus operandi, as well as on what can be assumed about the offender. Also, conducting an investigation related to cybercrime requires various ranges of different expertise. Therefore, along with the police officers within the High-Tech Crime Department who are specially trained in cyber -related crimes, experts from Service for Special Investigative Techniques are often involved. Investigative techniques in any kind of investigation are regulated and conducted in accordance with the Code of Criminal Procedure.

One good recent example of investigative techniques was provided by a nationwide malware-related computer fraud investigation, which called for computer forensic investigation and malware analysis, as well as further international cooperation based on Budapest Convention and the use of the Cyber 24/7 network for data preservation and of mutual legal assistance in collaboration with the DOJ in order to retrieve the preserved evidence.

5.2.2 Forensic and Encryption

In accordance with Article 332(1) of the CPA, if an investigation cannot be conducted otherwise or if this would entail disproportionate difficulty, the investigating judge may, upon a written request from the State Attorney that includes a statement of reasons, impose special evidence-gathering measures that temporarily restrict certain constitutional rights, i.e. surveillance and the recording of telephone conversations and other remote communications.

In the Republic of Croatia electronic or remote forensic examinations are not carried out.

ISSB has been tackling the issue with Cryptolocker malware with the main aim of helping the parties concerned restore encrypted data. In this context ISSB has had problems decrypting and restoring compromised user data. ISSB is managing crypto material used for the exchange of classified information between the Republic of Croatia and foreign countries and is only implementing measures and standards for the protection of information systems. ISSB does not have legal jurisdiction for intercepting, decrypting or analysing traffic or user data that originates in or is in any way connected with parties involved in criminal investigations into cybercrime.

The Croatian Ministry of the Interior is aware of the problem arising from data encryption, but for the time being in the Republic of Croatia there is no institution capable of tackling this problem.

5.2.3 E-evidence

Article 87 (18), (19) and (20) of the CC provide definitions of a computer system, computer data and a computer programme:

• A computer system shall mean any device or group of inter-connected or inter-linked devices, one or more of which processes data automatically on the basis of a computer programme, as well as computer data stored, processed, read in it, or transferred into it for the purpose of its operation, use, protection or maintenance,

• Computer data shall mean any denotation of facts, information or ideas in a form suitable for computer processing,

• A computer programme shall mean a set of computer data that is capable of prompting the computer system to perform a certain function.

Electronic (digital) evidence is data that has been obtained as evidence in electronic (digital) form, and it shall be collected by applying the following provisions of the CPA - Article 257 (Search of a Movable or Bank Safe), Article 262 (Temporary Seizure of Objects) and Article 263 (Temporary Seizure of Objects).

According to Article 257, a search of movables shall also include a search of a computer and devices connected therewith, of other devices intended for collecting, saving and transferring data for telephones, computers or other kinds of communication and data carriers. At the request of the authority carrying out a search, the person using or with access to a computer or other device or data carrier, including a telecommunications service provider, shall allow access to a computer, device or data carrier and shall provide the necessary information allowing for their unhindered use and for the objectives of the search to be met. Upon the order of the authority carrying out a search, the person using or with access to a computer or other devices. including a telecommunications service provider, shall immediately take measures aimed at preventing the destruction or modification of data.

The objects that have been seized in accordance with the CC shall be seized temporarily, and their storage shall be ensured. This also refers to any data stored on computers or related devices, or on any devices used for data collection and transfer, including data carriers, and to any subscriber information in the possession of a service provider. Such data must be submitted at the request of the State Attorney in complete, original, readable and understandable form. At the proposal of the State Attorney, the investigating judge may decide to order the protection and storage of a computer for a maximum period of six months. After that, the computer data will be returned unless it is used in the commission of offences against computer systems, programmes or data in accordance with the CC.

Since this data constitutes evidence in proceedings, the State Attorney will bring charges after the investigation has been completed. According to Article 342 of the CPA, the indictment shall include, among other things, the evidence on which it is based, after which it will be used in the court.

In the Republic of Croatia there are no special rules for the admissibility of e-evidence, but the general rules on the inadmissibility of evidence are applied.

Article 10 of the CPA stipulates that court decisions may not be founded on unlawfully obtained evidence (unlawful evidence).

Unlawful evidence is obtained in violation of the prohibition of torture, cruel or inhuman treatment as provided by the Constitution, domestic or international law; it is obtained in violation of the rights to defence, dignity, reputation, honour and inviolability of personal and family life guaranteed by the Constitution, domestic or international law and, it is obtained in violation of criminal procedure rules expressly provided for in the CPA, as well as those of which knowledge has been gained from unlawful evidence. The court decision may not be founded on unlawfully obtained evidence.

Article 419 of the CPA provides that the parties shall be entitled to call witnesses and expert witnesses and to present evidence. However, the panel may decide that evidence that was not put forward, or that the party putting forward evidence relinquished, should be presented after all.

The Act on Judicial Cooperation in Criminal Matters with the Member States of the European Union (Official Gazette 91/10, 81/13, 124/13 and 26/15) governs judicial cooperation in criminal matters between the national competent judicial authority and the competent judicial authorities of other Member States of the European Union and refers among other things to the European Evidence Warrant. In accordance with this act, the competent authority liable under national law shall issue a warrant for seizing property or evidence located in another Member State for the purpose of securing evidence or enabling the subsequent seizure of property for the purposes of criminal proceedings conducted in the Republic of Croatia.

The Act on Mutual Legal Assistance in Criminal Matters (Official Gazette 178/04) regulates mutual legal assistance in ongoing criminal proceedings in the Republic of Croatia or in a foreign country, such as the collection and transfer of objects to be presented as evidence. Requests for mutual legal assistance shall be sent to foreign competent authorities via the Ministry of Justice. Domestic judicial authorities may, under the terms of reciprocity, or when it is provided for by an international treaty, address procedural documents or judicial decisions to persons located abroad directly by mail.

5.3 Protection of Human Rights/Fundamental Freedoms

The Constitution of the Republic of Croatia guarantees the freedom of thought and expression, which shall in particular include freedom of the press and other media, freedom of speech and public opinion, and the free establishment of all public communication institutions. Censorship shall be forbidden. Journalists shall have the right to freedom of reporting and access to information. The rights guaranteed under the Constitution are regulated by the Media Act, the Electronic Media Act and the Croatian Radio and Television Act.

The right to access information is a right guaranteed under the Constitution. The Act on the Right of Access to Information elaborates the right of access to information and the re-use of information owned by public authorities, prescribes the principles governing the right of access to information and the re-use of information, the restrictions of the right of access to information and the procedure for the exercise and protection of this right.

One of the fundamental human rights, the right to the protection of personal data, is regulated in the Republic of Croatia by the Personal Data Protection Act (Official Gazette 103/03, 118/06, 41/08 and 130/11; 106/12 – consolidated text). According to Article 1(3) of the Act, the protection of personal data in the Republic of Croatia has been ensured for every natural person irrespective of his/her citizenship or place of residence, and regardless of race, skin colour, sex, language, religion, political or other convictions, national or social background, property, birth, education, social standing or other characteristics. In this regard, the Personal Data Protection Act is applicable in the event of cybercrime, depending on the particular circumstances of each case, especially through the implementation of surveillance activities concerning the protection of personal data, whether at the request of the respondent for the protection of rights, a third-party proposal or ex officio.

The National Programme for the Protection and Promotion of Human Rights for the 2013-2016 period, adopted by the Government of the Republic of Croatia in April 2013, identified the areas of freedom of media, the right to access information and the right to the protection of personal data as priority areas. A series of measures aimed at strengthening the protection and promotion of these rights were provided for all of these areas.

According to Article 332 of the CPA, special evidence-gathering measures temporarily restricting certain constitutional rights may also be taken for criminal offences against computer systems, programmes or data, as well as for criminal offences against intellectual property, if committed with the use of computer systems or networks.

If an investigation cannot be conducted otherwise or if this would entail disproportionate difficulty, the investigating judge may, upon a written request from the State Attorney that includes a statement of reasons, order, by a written warrant that includes a statement of reasons issued against a person against whom there are grounds for suspecting that he or she committed, or together with other persons participated in the commission of the aforementioned criminal offences, that the following special evidence-gathering measures be taken:

1) surveillance and recording of telephone conversations and other means of remote communication;

2) interception, collecting and recording of computer data;

3) entry into premises for the purpose of conducting surveillance and making recordings of the premises;

4) covert tailing and recording of individuals and objects;

5) use of undercover investigators and confidants;

6) simulated sales and purchases of objects, simulated bribe-giving and simulated bribe-taking;

7) the provision of simulated business services or the conclusion of simulated legal transactions;

8) controlled transport and delivery of objects of a criminal offence.

By way of exception, if there is risk of delay and if the State Attorney has reason to believe that they will not be able to obtain a warrant from the investigating judge, the warrant may be issued by the State Attorney for a period of twenty-four hours. The State Attorney shall deliver the warrant marked with the date of issue and a statement of reasons to the investigating judge within eight hours of issue. At the same time, if the State Attorney deems that the special evidence-gathering measure needs to be continued, the State Attorney will lodge with the judge a written request for its continuation that includes a statement of reasons. Immediately upon receipt of the warrant and statement of reasons, the investigating judge shall examine whether the conditions for the issue of the warrant were met, and whether there was a risk of delay.

The investigating judge shall decide immediately by order on the legality of the warrant issued by State Attorney. If the investigating judge authorises the warrant issued by the State Attorney and the State Attorney lodged a request for the continuation of evidence-gathering measures, these special measures shall be ordered. If the investigating judge rejects the warrant issued by the State Attorney, he or she shall request that the panel decide on that. The panel shall decide on the request of the investigating judge within twelve hours of receipt of the request. If the panel authorises the warrant issued by the State Attorney and the State Attorney asked for the continuation of evidence-gathering measures, the panel shall issue a warrant for evidence-gathering measures. If the panel does not authorise the warrant, it shall issue an order for the immediate suspension of the measures , while the data collected pursuant to the warrant of the State Attorney shall be handed over to the investigating judge, who shall destroy it. The investigating judge shall establish a protocol on the destruction of the data.

The special evidence-gathering measures of surveillance and recording of telephone conversations and other means of remote communication may also be ordered against persons against whom there are grounds for suspicion that they are disclosing to or from the perpetrator of any of the offences against computer systems, programmes or data information and messages in connection with the offence in question, or that the perpetrator is using their telephone connection or some other telecommunications device to conceal the perpetrator of a criminal offence or is assisting them in preventing their discovery by concealing the means by which a criminal offence was committed, the traces of criminal offences or objects resulting from or acquired through the commission of a criminal offence.

The Operational Technical Centre for the Supervision of Telecommunications, which is responsible for the technical coordination of telecommunications operators in the Republic of Croatia is obliged to provide the necessary technical assistance to the police authorities. Special evidence-gathering measures are conducted by the police.

Under Article 339a of the CPA, if there is a suspicion that a registered owner or user of a telecommunications device committed a criminal offence against computer systems, programmes or data, the police may, based on a warrant issued by the investigating judge for the purpose of collecting evidence, request via the Operational-Technical Centre for the Supervision of Telecommunications, request from the operator of public communications services proof of the identity, duration and frequency of communications with certain electronic addresses, determine the location of a communications device, and the location of persons engaged in electronic communication, as well as the device's identifiers.

5.4 Jurisdiction

5.4.1 Principles applied to the investigation of cybercrime

According to Article 11 of the CC, the criminal laws of the Republic of Croatia shall also apply to anyone who commits a criminal offence aboard a Croatian vessel or aircraft, regardless of the location of the vessel or the aircraft at the time the criminal offence was committed.

In addition, the criminal laws of the Republic of Croatia shall apply to a Croatian citizen or to a person who is resident in the Republic of Croatia who commits an offence outside the territory of the Republic of Croatia, if the offence is punishable under the law of the country in which it was committed. This provision will apply if the perpetrator acquires Croatian citizenship after committing the criminal offence.

Furthermore, the criminal laws of the Republic of Croatia shall apply to a foreigner who commits an offence outside the territory of the Republic of Croatia for which, underCroatian law the punishment is a sentence of five years' imprisonment or more, if the offence is also punishable under the law of the country in which it was committed and if the extradition of the perpetrator is permitted by law or international treaty. This situation has never occurred so far.

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

The criminal laws of the Republic of Croatian applies to Croatian citizens and to any persons resident in the Republic of Croatia who commit an offence outside the territory of the Republic of Croatia, if the offence is punishable under the law of the country where it was committed.

When it comes to the criminal offences of the solicitation of children for the satisfaction of sexual needs, the exploitation of children for pornography and serious crimes of sexual abuse and exploitation of children, the criminal laws of the Republic of Croatia will apply if the offence is not punishable under the law of the country where it was committed.

The criminal laws of the Republic of Croatia shall apply to a foreigner who, outside the territory of the Republic of Croatia, commits any criminal offence against a Croatian citizen, a person resident in the Republic of Croatia or a legal entity registered in the Republic of Croatia, if such an offence is punishable under the law of the country in which it was committed. The court may not impose a more severe sentence than the one prescribed by the law of the country where the criminal offence was committed.

In such cases, criminal proceedings shall only be instituted if the perpetrator is present on the territory of the Republic of Croatia.

The Republic of Croatia has not yet applied in practice the communication underprovided for in Council Framework Decision 2009/948/JHA.

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

The fact is that offenders who sexually abuse children via the internet are increasingly 'hidden' as they are making greater use of on-line 'Cloud' storage to store illegal content. This has made it more difficult to detect offenders and to provide evidence of criminal liability in criminal proceedings. In cases where the suspect is willing to cooperate or there are other sources of information concerning usernames and passwords, a court order to search his/hers accounts for such services, with aim of gathering and registering the content, is obtained. Furthermore, in some cases Croatia sends a preservation request to the owner of the service asking that they keep illegal content on the suspect's account until Croatia provides a request for international legal assistance.

5.4.4 Perception of Croatia with regard to the legal framework for combating cybercrime

The Croatian authorities expressed the view that the national law is in full compliance with European legislation in this area and said that the Convention on Cybercrime of the Council of Europe had been transposed, thus the Republic of Croatia considers the existing legal framework to be adequate for both the investigation and prosecution of cybercrimes committed outside the territory the Republic of Croatia.

They also found, however, that the legislation was outdated and that it did not reflect any technological developments, and that it was necessary to amend it, not only at national level but also internationally, in order to address a number of doubts in this area. The biggest problem was the general lack of a universal minimum standard act obliging service providers to provide the law enforcement authorities with information which would help identify offenders.

5.5 Conclusions

- The evaluation team has not had the opportunity to analyse the relevant Croatian legislation in depth , in the absence of an English translation of the consolidated legislation in place;

- While the Croatian authorities repeatedly stated that national legislation complied with all EU and international obligations, some weaknesses were highlighted in the effectiveness of legislation to combat cybercrime; an example of the absence of a specific legal framework in relation to JITs on cybercrime and to cyber patrols was given.

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

Incident types reported to National CERT in the year 2015 are as follows.

Incident type in period 1.1.2015-17.7.2015	Number of incidents
Compromised servers providing malware	148
Compromised servers providing phishing pages	135
Phishing attacks	45
Web defacement	27

The compromised servers were mostly providing malware or phishing content to foreign internet users and were used as infrastructure. In 2014 and 2015 Croatia had two mass infections related to 3 types of Zeus malware, and recently there was a malware campaign where cyber criminals used compromised portals or third-party servers providing ads to spread malware.

In addition, 2 botnet command and control servers were recently taken down, its content analysed and the relevant CERTs or LEA informed. Lesson learned is that data should be shared on a need to know basis in order to deal with such cases effectively.

6.1.2 Mechanism for responding to cyber attacks

Croatia has multidisciplinary mechanism for responding to a serious cyberattack provided for in the National Cyber Security Strategy. A serious cyberattack would be dealt with through the coordination of national CERT, LEA and internet service providers.

The central state administration bodies, in cooperation with the competent regulatory agencies, are responsible within their remit for identifying (establishing) certain systems or their parts as critical national infrastructures, and for ensuring the management of critical infrastructures and their protection.

The head of the central state administration body makes a decision on determining critical national infrastructure based on the decision of the Government of the Republic of Croatia confirming identified critical infrastructure, and forwards it for implementation to the owner/operator of those infrastructures and to the central state administration body responsible for the area of protection and rescue.

The owners/operators of the identified (established) critical infrastructures have direct responsibility for operating and protecting critical infrastructures in all circumstances.
The National Cyber Security Strategy and Action Plan for the implementation of the Strategy envisages activities aimed at improving the organisation of this area, in terms of defining more precisely the criteria for recognising critical communication and information infrastructure, establishing the minimum security standards for the information systems that are crucial for the proper functioning of critical infrastructures, and ensuring the implementation of those standards (implementation by owners/operators, supervision).”

The Croatian authorities, both in their replies to the questionnaire and during the on-site visit, emphasised that 'Responding to cyber-attacks is almost never a matter of one jurisdiction only, i.e. it usually means getting two or more different institutions involved in the investigation/evidence gathering/analysis/legal process'. The Ministry of the Interior also has to cooperate with the prosecutors' office, and often cooperates with national and/or government CERT, internet service providers, the private sector, academia, etc. as well as with other LE agencies on an international level. Therefore, Croatia needs fast and effective communication in order to shorten proceedings dealing with cases of cyber threat.

Having a network of different types of expertise would allow the police to obtain the relevant support in cases which require a higher level of technical knowledge and specific skills (for example, cooperation with the government CERT in some specific malware-related cases). Irrespective of this, taking into account rapid technological progress and the need to adjust to new trends and more advanced modus operandi on a daily basis, training at all levels (police, prosecutors and judges), both legal and technical, is of crucial importance in order to deal with cyber-related crimes successfully.

Apart from the general training programs needed for all the relevant bodies involved in an investigation, there is still a lack of experts who are sufficiently knowledgeable and technically equipped to perform an independent investigation starting from collecting evidence and processing/analysing it for use in the subsequent legal proceedings. This often gives rise to errors and misunderstandings in relation to the prosecutor in charge.

International cooperation and requesting data from another country often require longer periods of time, which in cyber-related crimes can be of crucial importance (because of the data volatility).On account of the various legal obligations regarding data retention, obtaining the relevant information from different countries is sometimes impossible, or very slow.

Analyzing large (and growing) amounts of data requires more and more time and more efficient technology, as well as greater expertise.

6.2 Actions against child pornography and sexual abuse online

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

There are no specific national or local databases. The Croatian law enforcement authorities only use Interpol's International Child Sexual Exploitation Database - ICSE for identifying victims.

In all cases of publication, exchange, possession, or storage of child abuse material on servers or computers in Croatia, the content will be seized, blocked, deleted (removed), and any persons who access such materials will be prosecuted because possession, publication, exchange, storage or access to child sexual exploitation material is a criminal offence. All of the above mentioned material will be seized and destroyed under criminal law.

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

Article 161 of the CC defines the criminal act of the solicitation of children for the satisfaction of sexual needs. An adult person who suggests a meeting with another person under the age of fifteen, with the intent of committing an offence of sexual abuse of a child under fifteen years of age, or assisting another person in committing the offence through information and communication technologies, or otherwise, or by taking actions to bring about such a meeting, shall be punished by imprisonment for up to three years. Any person who collects, provides or transmits data on a person under the age of fifteen in order to commit this crime shall be punished by imprisonment for up to one year. The attempted offence of the solicitation of children for the satisfaction of sexual needs shall also be punishable.

Furthermore, the CC provides for the possibility of imposing security measures against perpetrators of the criminal acts of the sexual abuse and exploitation of children. A security measure of prohibition from accessing the internet shall be ordered by the court for a perpetrator who commits the offence via the internet, if there is a risk that they will abuse the internet in order to commit the offence repeatedly (Article 75 of the CC). The security measure of prohibition from accessing the internet shall be imposed for a period of six months to two years. In cases where perpetrator is sentenced to prison, but is not given a suspended sentence or the sentence of imprisonment is replaced by community service, the measure will be imposed for a period of six months to two years longer than the prison sentence. Regarding the final punishment, the court will notify the regulatory authority responsible for electronic communications in order to ensure its implementation.

In accordance with Article 76 of the CC, protective supervision shall be provided in cases where the prison sentence is fully served and if the perpetrator is sentenced to imprisonment for the offence of the sexual abuse and exploitation of children. If the sentence was fully served, because the convicted person was not granted parole, he/she will be placed under immediate protective supervision upon release from prison. The supervision is based on an individual treatment program that establishes, helps to implement and oversees the implementation by the competent authority for probation. The probation lasts for three years. The court may, upon a proposal from the competent authority for probation, extend the probation period before its expiry for another year if there is a risk of recommitting any of the offences of the sexual abuse and exploitation of children.

In order to tackle or alleviate the consequences of the above mentioned criminal activity, Croatia has stepped up the training given to police officers responsible for young people so that they can recognise the various forms of this type of crime more easily, and can provide a more effective response. This training is conducted in cooperation with the Police Academy, and also forms part of the previously mentioned cooperation with various international and EU institutions (CEPOL, TAIEX).

The police officers responsible for young people at local level, in cooperation with the police officers responsible for prevention and some local educational institutions organised some talks for pupils and students in order to give them information about various crimes or inappropriate behavior on the internet, on self-protective behaviour and on the various risks, as well as some information and advice on where and how they can ask for help.

6.2.3 Preventive actions against sex tourism, child pornography performances and other offences

Pursuant to Article 14 of the CC, the criminal laws of the Republic of Croatia apply to citizens and residents of Croatia who commit a criminal offence punishable under the law of the State where the offence was committed. This provision shall also apply to a perpetrator who acquires Croatian citizenship after committing a crime.

Bearing in mind the above, the criminal laws of the Republic of Croatia will apply in cases where the perpetrator has committed the criminal offence of sexual abuse of a child under fifteen years of age in accordance with Article 158 of the CC, the offence of sexual abuse of a child over fifteen years of age in accordance with Article 159 of the CC , the offence of the solicitation of children for the satisfaction of sexual needs in accordance with Article 161 of the CC, the offence of molesting? a child in accordance with Article 162 of the CC, the offence of exploiting children for pornographic purposes in accordance with Article 163 of the CC, the offence of exploiting children for pornographic performances in accordance with Article 164 of the CC or for serious offences of sexual abuse and exploitation of a child under Article 166 of the CC, if the offence is not punishable under the law of the State where it was committed.

In addition, when Croatian citizens take part in peacekeeping operations or other international activities outside Croatian territory and commit a criminal offence in the course of such operations or activities, the application of Croatian laws shall be governed by the provisions of the CC, unless an international treaty to which Croatia is a party provides otherwise.

The criminal law prohibits advertising of child pornographic performances and it is punishable under Article 162 of the Penal Code. Croatia has not developed specific measures to counteract real time web-based child pornography performances.

On 29 September 2013, the 'Red Button' website (https://redbutton.mup.hr) allowing any form of child abuse to be reported online. Since the launch of the application mid- 2015, Croatia has received over 2 300 reports, but most of them related to legal pornography content.

The website of the Ministry of the Interior (http://www.mup.hr/main.aspx?id=13047) and the web pages of the Centre for Safer Internet (http://www.sigurnijiinternet.hr) contain tips for children and their parents on online safety, highlight the risks and give advice on, what to do if a child became a victim.

On the website of the Ministry of the Interior (http://www.mup.hr/main.aspx?id=13047) information on illegal, harmful or punishable behaviour is available.

6.2.4 Actors and measures combating websites which contain or disseminate child pornography

The investigation of these crimes is the responsibility of the Department of Juvenile Delinquency and Crime against Children, which cooperates with police officers from other units trained in gathering forensic evidence.

The provisions of the Electronic Communications Act (Official Gazette 73/08, 90/11, 133/12, 71/14) regulate the implementation of measures regarding the sending of unsolicited e-mails, as well as the obligations of the e-mail service providers. The Act also regulates the implementation of measures for the protection of data and the safety of electronic communication, as well as the powers of the Croatian Regulatory Authority for Network Industries.

The Ordinance adopted by the Council prescribes the manner and conditions for the effective prevention and suppression of abuse and fraud in the provision of electronic mail services. Furthermore, the aforementioned Act imposes the payment of a fine if a legal person in the capacity of an e-mail service provider does not enable the filtering of incoming e-mails, does not publish the e-mail address for reporting abuse, does not handle complaints regarding e-mail abuse or does not take the necessary measures in the event of abuse of a subscriber's e-mail account or does not take measures for the prevention or suppression of abuse and fraud in the provision of electronic mail services.

Croatia does not apply filtering or block access. But as already mentioned, all content which shows the sexual abuse and exploitation of children must be removed by the force of law. Consequently, all internet or electronic service providers in the Republic of Croatia are obliged to remove such contents posted or stored on their service and to notify the police or the State Attorney's Office.

The Croatian Academic and Research Network, which is the service provider for all schools and universities in Croatia, filters content by blocking access to several groups of websites dedicated to gambling, sex, weapons etc.

If the Croatian authorities find out that the illegal content is located on servers outside the jurisdiction of the Republic of Croatia, they notify the competent State law enforcement agency through the regular police channels (Europol or Interpol). Before doing so, they try to secure the evidence they can get online.

6.3 Online card fraud

Croatian citizens do not usually report online payment card fraud. According to the Croatian authorities, citizens / customers are usually not even aware that payment card fraud has occurred.
In most cases, the bank/card issuer detects fraud during the monitoring of transactions. Banks report online payment card fraud to police.

6.4 Other cybercrime phenomena

In order to limit the possibility of access to organised crime data cards and transactions, all Croatian issuers / acquirers of payment cards strictly implement the measures of the card industry PCIDSS (Payment Card Industry Data Secure System). The following anti-skimming measures are being implemented: installation of anti-skimming equipment (TMB technology), video surveillance at ATMs, a media campaign launched by the Croatian Banking Association, and the introduction of contactless cards.

Croatia does not have a specific legal framework for Bitcoins and other virtual currencies, although Bitcoin ATM machines are available in the country and virtual currencies are used as a payment method on websites; for the time being, no cases involving virtual currencies have been reported.

The evaluation team was informed by the Croatian prosecutors that virtual currencies may be covered by the legal definition of property and that their seizure would therefore be possible.

6.5 Conclusions

- In the same way as there is a general need for a more structured and systematic coordination/exchange of information between the various entities involved in cybersecurity and the fight against cybercrime, Croatia would gain from a closer cooperation at operational level between the national CERT and the police authorities;

- The evaluation team was impressed by the knowledge and ability of the Croatian law enforcement authorities dealing with child sexual exploitation in particular;

- The on-site visit also made it obvious that, although Croatian forensic experts have a solid knowledge of IT and devices, they have difficulties in adapting their skills rapidly to new crime trends (which change very fast) due to workload pressures. Forensics experts should be given sufficient resources, time and tools to keep them in regular training and allow them to develop their skills.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

7.1.1 Formal requirement cooperate with Europol/EC3, Eurojust, ENISA

Cooperation with Europol:

The Agreement on operational and strategic cooperation between Croatia and Europol was signed in 2006 and was valid until Croatia`s accession to the EU on 1 June 2013. The Europol Enlargement Project was launched in 2012, with the aim of harmonisation prior to accession to full membership of Europol and had been successfully completed by 1 July 2013. After that date, EU Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/ JHA) became the legal basis for cooperation between Croatia and Europol. There are no special national laws on cooperation between Croatia and Europol.

Under Article 40 of the Regulations on Police Procedures, a police officer can collect data, inter alia: from data received from Interpol, Europol and other international organisations or the police of other countries.

Under the Data Secrecy Act, the ISSB is obliged to refrain from sharing information with a classification marking. Security agreement between countries has to be signed in order to share classified information. The ISSB is allowed to share non-classified information about a cyber security incident if that information can help clear up the incident. Usually, a formal request by e-mail or in writing should be forwarded to the ISSB.

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

Croatia participates in the EUCTF and is represented there by the Head of the High-Tech Crime Unit. Croatia at the moment is not taking part in the cyber patrols.

In cases of cybercrime with an international element, the Republic of Croatia generally applies the 2001 Council of Europe Convention on Cybercrime, as well as the 24/7 network. In urgent procedures involving cybercrime, Croatia is assisted by the European Judicial Network in Criminal Matters and by Eurojust in cases of transnational organised crime committed on the territories of multiple EU MS.

The Republic of Croatia participated in a coordination meeting organised by Eurojust in relation to a cybercrime case. The Croatian authorities found Eurojust's contributions very useful.

With regard to cooperation with Europol/EC3, the High-Tech Crime Department has been involved in an on-going investigation which started in March 2014, covering numerous malware attacks and serious financial damage in Croatia. The investigation is being conducted at both national and international level and concerns computer fraud carried out through the use of banking malware, as well as money laundering cases involving a wide network of national/international money mules.

The Department of Juvenile Delinquency and Crime against Children and Families cooperates with Europol / EC3 / FP Twins on an ongoing basis. The cooperation is in most cases concerned with the preparation and exchange of information on specific operational actions that FP Twins prepare independently or in cooperation with other law enforcement agencies. Also, FP Twins informs the national authorities about the reports from US NCMEC's.

As far as Croatia's contacts with ENISA are concerned, they have more of an advisory function than an operational one .

Croatia has worked on several cases that involved cooperation with Europol, ENISA and CERTs in other MS. The biggest case was a ZeuS campaign that culminated in spring 2014 with large numbers of infected machines in Croatia. Croatia has delivered all the details from its investigation to Europol and shared information with CERTs in all other MS.

Croatia has limited human and technical resources in the cybercrime area and in that regard Croatia very much welcomes the establishment of the EC3 with its analysis department (e.g. AWF Cyborg). Croatia especially appreciates EC3`s role in data collection and analysis, malware analysis and the "Malware sandbox" tool for direct upload and malware analysis.

The Department of Juvenile Delinquency and Crime against Children and Families assessed the contribution of Europol / EC3 as very positive and appreciates their help and cooperation.
The Croatian National CERT would welcome information about bots following EUROPOL/EC3's removal of botnets in order to inform end users about infections on their workstations.

Croatia has been satisfied with the cooperation with all listed organisations. Croatia believes that there is always a way to improve these aspects, especially in information-sharing.

EC3 (FP Cyborg), EUCTF, EMPACT Cyber Attacks and ECTEG are the four pillars which lend solid support to cooperation and coordination between MS law enforcement agencies in the cybercrime area. There is room for improvement in the training area in particular. Training police officers is crucial for responding to cyber-attacks and tackling on line child abuse. Tailor-made training programmes for police officers are of utmost importance. As an excellent example of Europol training, Croatia would highlight the Europol Training Course on Combating the Sexual Exploitation of Children on the Internet. Croatia appreciates the work done by the ECTEG members so far, especially the projects conducted in cooperation with University College Dublin (UCD). In order to provide similar training in the area of cyber-attack investigations, Croatia is of opinion that it would be more fruitful for the ECTEG to be fully incorporated in the EC3.

7.1.3 Operational performance of JITs and cyber patrols

The Republic of Croatia did not participate in the JITs related to cybercrime. This might be linked to the fact that Croatia has not yet acceded to the 2000 MLA Convention.
A legal framework on cyber patrols does not exist in the Republic of Croatia.
However, the Croatian authorities said it would support such forms of operational cooperation to the greatest possible extent.

7.2 Cooperation between the Croatian authorities and Interpol

Since June 2013, law enforcement in the Republic of Croatia has been connected to the "ICSE database" and the police officers in the Department of Juvenile Delinquency and Crime against Children and Families are working on it actively.

In general, they rate the cooperation with Interpol as good. The Interpol channels are mainly used for communication with third parties, otherwise Europol is preferred. Each State cooperates via Interpol according to their national legislation, so experience may vary. As regards cybercrime, in most cases Croatia asks for data relevant to criminal investigations by submitting a notification or request.

Obtaining information depends on the country Croatia asks for information and its national legislation. For example, to acquire data about IP address ownerships, traffic data, transaction accounts etc. most countries require mutual legal assistance (international legal aid). The requests for MLA are sent via the Ministry of Justice; this procedure usually complicates the investigations and takes time.

Although they have yet to avail themselves of assistance from this source, of it, it is their opinion that Interpol's Global Centre for Innovation in Singapore could be provide valuable support in fighting cybercrime on a global level.

The cooperation with Interpol's Crimes against Children Unit, in the area of establishing and constructing the ICSE data base and "Baseline project" has expanded the possibilities for identification of victims and has helped in the criminal investigations as well as in exchanging information with other law enforcements agencies via EC3.

7.3 Cooperation with third states

In cybercrime investigations the Croatian police is open to any cooperation that could help to gather necessary data and information. If the investigation involves third party states, they usually communicate through their International Cooperation Service and all data are shared through Interpol or Europol communication channels. Croatia also uses the tools set up by the Budapest Convention, such as the 24/7 contact points. When it comes to cooperation with the third countries in the region, Croatia has taken part in joint training on preventing and combating cybercrime.

At the Ministerial Conference on 5 December 2012 the Republic of Croatia participated in the foundation of the Global Alliance against Child Sexual Abuse Online. Croatia thereby defined its policy regarding cybercrime child sexual exploitation.

Since cooperation with third countries usually differs from cooperation with EU countries, especially because there is no institutional framework and it usually takes more time and involves more steps, Europol can help to unify the procedures and thus significantly contribute to the effectiveness of cooperation with the third countries. Also, EC3's analytical capabilities are very useful when it comes to investigations carried out in several countries (Croatia has practical experience with OA MIR regarding Cyber frauds and banking malware, and with the help of Europol an operational meeting was organised).

The evaluation team was briefed on practical cases of cooperation with third countries, both successful and unsuccessful. In particular, in one serious malware case, a large neighbouring third country did not cooperation, and not even MLA worked.

7.4 Cooperation with the private sector

Article 339a of the CPA stipulates that, in the event of a suspicion that the registered owner or user of a telecommunications device has committed a criminal offence against the computer system, programme and data or another offence punishable by a sentence of more than 5 years' imprisonment, the police may, on the basis of an order by the investigating judge, and for the purpose of gathering evidence, request the examination of the identity, duration and frequency of communications with certain electronic communications addresses, determination of the location of the communications device, determination of the location of persons establishing electronic communications and determination of the identification marking of the device from the public communications service provider via the Operational Technology Centre for the Surveillance of Telecommunications. Similarly, in the case of a registered owner or user of the telecommunications device connected with the person suspected of committing a criminal offence against the computer system, programme and data or another offence punishable by a sentence of more than 5 years' imprisonment, the police may, on the basis of an order by the investigating judge, request the said investigation from the public communications service provider via the Operational Technology Centre for the Surveillance of Telecommunications.

According to the Law on Electronic Communications ISPs have certain obligations and responsibilities, as follows:

ISPs must adopt appropriate technical and organisational measures to protect the security of their services, while operators of public communications networks are required take the necessary measures to protect the security of electronic communications networks and services. The measures must provide a level of safety equivalent to the existing level of risk for the security of the network, taking into account the available technical and technological solutions and the costs involved. The measures taken are carried out in order to prevent and minimise the impact of security incidents on users and interconnected providers of electronic communications networks. (Article 99)

ISPs and publicly available electronic communications services and legal and natural persons that, under specific regulations, provide electronic communications networks or provide electronic communications services on Croatian territory are required to ensure and maintain at their own expense the function of secret surveillance of electronic communications networks and services, as well as electronic communications lines to the operational and technical body responsible for the activation and management of the measure of secret surveillance of electronic communications, in accordance with the law regulating the field of national security (Article 108);

ISPs and publicly available electronic communications services must retain data on electronic communications under Article 110 of the Act for the purpose of enabling the investigation, detection and prosecution of criminal offences in accordance with the law on criminal procedure and to protect national security in accordance with the legislation in the field of defence and national security (Article 109) etc.

Regarding the removal of websites, in the Republic of Croatia only a court may order the service provider to remove illegal content or disable access to it. Access to individual web pages or their deletion can also be blocked on the basis of a court order.

The Croatian Academic and Research Network (CARNET), as manager of the national top-level domain, in accordance with the Regulations on the Organisation and Management of the National Internet domain, can temporarily deactivate a specific Croatian (.hr) domain if they have violated certain provisions of this Ordinance, or if there is serious suspicion that a user is acting contrary to the principles of good faith and the use of the domain violates the rights of third parties and thus causes serious and irreparable damage, or if he intends to make an unauthorised transfer of a registered domain to another person.

Cross-border cooperation on Internet Payment Card fraud is routinely carried out with credit card companies (Visa, MasterCard, and American Express), by exchange of information through Europol and Interpol, and through bilateral cooperation.

Croatian law enforcement authorities have established some cooperation and contacts with the local branches or the nearest branch in the region. An example is cooperation with Google Croatia whom they have addressed in cases where the country needed some data they could provide.

7.5 Tools of international cooperation

7.5.1 Mutual Legal Assistance

Croatia is not party to the 2000 MLA Convention. During the on-site visit, the evaluation team was told that the process of accession to the Convention was still on-going.

The Ministry of Justice of the Republic of Croatia is the competent authority for receiving/sending requests for MLA. By way of exception, the domestic judicial authority may directly submit a request for MLA to a foreign judicial authority when this is expressly laid down in the provisions of the Act on International Legal Assistance in Criminal Matters or in international agreements (direct communication) and on the basis of reciprocity. In those cases, the domestic judicial authority sends a copy of the request for MLA to the Ministry of Justice. In urgent cases, and in the case of reciprocity, the Ministry of Justice may send and receive requests for MLA via Interpol. In the case of direct communication, the domestic judicial authority may do the same.

The Republic of Croatia does not have a comprehensive statistical system covering the whole area of MLA. The Ministry of Justice said that there are some projects in progress to improve the system, which is under its responsibility. There are no specific procedures or conditions that need to be fulfilled in the Republic of Croatia regarding MLA requests related to cybercrime. Such requests are handled in the same manner as requests related to other types of criminal offences.

The domestic authorities apply national law when providing international legal assistance. The CPA lays down the conditions for verifying that contact has been established via telecommunications in order to provide evidence. Since this action encroaches on basic human rights, it is governed by a special Article of the Act, which guarantees a higher degree of protection of the basic rights, and especially the privacy rights, of the registered owners or users of telecommunications devices. The action itself may include:

- examination of identity, duration and frequency of communications with certain electronic communications addresses
- determination of the location of the communications device
- determination of the location of persons establishing electronic communications
- determination of the identification marking of the device.

Urgent requests are handled promptly. The average response time, if using regular means of communications, with central authorities and authorities determined by the Convention, is approximately 2 months.

All actions permitted by the CPA may be requested. Electronic evidence may be gathered by searching computers and related devices, other devices used for gathering, storing and transferring data, telephone, computer and other communications and data media. At the request of the authority conducting the search, a person using a computer or having access to a computer or another device or data media, and the telecommunications service provider, must ensure access to the computer, device or data media and provide the necessary information for its uninterrupted use and achieving the purposes of the search. At the request of the authority conducting the search, a person using a computer or having access to a computer or another device or data media and the telecommunications service provider must immediately take measures to prevent the destruction or alteration of data.

Data stored on the computer and related devices and other devices used for gathering and transferring data may be temporarily seized and stored if they are objects identified for seizure according to the CC or if they can help establish the facts in the proceedings.

If inquiries into the offences cannot be carried out in a different way or if carrying them out would give rise to disproportionate difficulties, the investigating judge may, at the reasoned written request of the State Attorney, issue, against a person concerning whom there are grounds for suspicion that he committed or, together with other persons, participated in the commission of a criminal offence, an order that imposes special evidence collection measures which temporarily restrict the constitutional rights of the citizen, as follows:

1) surveillance and technical recording of telephone conversations and other means of remote communication,

2) interception, collecting and recording of computer data,

3) entry into premises for the purpose of conducting surveillance and technical recordings of the premises,

4) covert tailing and technical recording of individuals and objects,

5) use of undercover investigators and informers,

6) simulated sales and purchases of objects, simulated bribe-giving and simulated bribe-taking,

7) provision of simulated business services or conclusion of simulated legal transactions,

8) controlled transport and delivery of objects of a criminal offence.

One of the most common reasons for requesting MLA is the verification of an IP address, i.e. the interception of content in the computer system.

In order to urgently take action regarding cybercrime, the Republic of Croatia is aided by the European Judicial Network in Criminal Matters and by Eurojust in cases of transnational organised crime committed on the territories of multiple EU Member States. To this date, the Republic of Croatia has not initiated any coordination meeting regarding the aforementioned cases, but has been invited to participate in such a meeting.

The Police Force operates a 24/7 network for Cyber Crime.

The exchange of evidence and obtaining of evidence abroad is carried out mostly in accordance with the provisions of the Convention on Cybercrime of 2001 and its Additional Protocol of 2003 (especially in terms of the retention of data in accordance with Articles 29 and 30 of the Convention for the purpose of their temporary seizure as a form of mutual legal assistance regulated by Article 31 of the Convention), the European Convention on Mutual Assistance in Criminal Matters of 1959 and bilateral agreements.

The maximum period for data retention in Croatia is one year. In the event of a request for preservation, data may be preserved for a period of 30 days; the MLA request should be submitted within the said period.

Criminal prosecution will be surrendered in cases where the terms set out in Article 65 of the Act on Mutual Legal Assistance in Criminal Matters apply (a criminal offence must not be punishable by a sentence of imprisonment of more than ten years, the offence was committed on the territory of the Republic of Croatia, and the perpetrator is a foreigner who resides abroad).

As previously stated, in cases where MLA is provided in relation to the United States of America the principle of reciprocity constitutes the legal basis pursuant to Article 17 of the Act on International Legal Assistance in Criminal Matters, which stipulates that the domestic judicial authority shall only comply with the request for an MLA sent by the judicial authority of a state with whom the Republic of Croatia has not concluded an MLA agreement if it is expected that the request would be reciprocated, based on an assurance issued by the requesting state. In these cases, the Republic of Croatia has not had any problems regarding the execution of MLA requests.

Where cyber attacks involve criminals from outside the EU, Croatia also applies the instruments of mutual legal assistance, such as the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. For example, in cases involving mutual legal assistance in relation to the United States of America, a legal basis for any action is the principle of reciprocity referred to in Article 17 of the Act on Mutual Legal Assistance in Criminal Matters, which stipulates that a request for mutual legal assistance from the judicial authority of a country with which the Republic of Croatia has not signed an agreement on mutual legal assistance will only be complied with by the domestic judicial authorities if it is expected that the state concerned would submit a comparable request to a domestic judicial authority, based on an assurance by the requesting state.

The basic procedures regarding international cooperation assume the use of instruments of mutual legal assistance for Croatia to be able to retrieve evidence from abroad.

In some cases, police officers use the services which some providers of electronic services provide to the police authorities to communicate and to ensure a faster and more effective response to, for example, the exploitation of children for pornography (e.g. Facebook, Skype, and Instagram Law Enforcement Response Team). International police co-operation with the police authorities in some countries (e.g. United States, Australia, New Zealand, etc.) has also been very successful in cases involving sexual abuse and exploitation of children.

7.5.2 Mutual recognition instruments

Problems have been detected regarding the criminal prosecution of computer-related crime offenders, especially computer crime offenders. Croatia has noticed an increased number of attacks with malicious computer programmes to the detriment of users of the Internet systems of Croatian business banks. These programmes allow unauthorised bank transactions from the accounts of the injured parties to the accounts of private individuals or legal entities in Croatia or abroad (i.e. financial mules) who then send money via Western Union or similar financial service providers and to intermediaries or perpetrators abroad. The intermediaries or so-called financial mules keep a proportion of the money, which is transferred to their current accounts.

The Republic of Croatia is affected by these offences, which are often committed by foreign citizens abroad, which makes it more difficult to identify the offenders. Despite taking urgent measures and utilising tools of judicial cooperation, such as orders freezing property or evidence (Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence), in practice the offender is rarely identified, i.e. the interim measures of freezing and confiscating the proceeds of the criminal offence are rarely imposed.

In 2014, the State Attorney's Office of the Republic of Croatia forwarded 16 orders freezing property or evidence in criminal proceedings for computer fraud, as stated in Article 271 of the CC, however no proceeds of a crime were frozen or confiscated in any of the cases, because the money had been withdrawn from the bank account at the time of the execution of the orders freezing property, leaving an insufficient amount to execute the freezing and confiscation of the proceeds of the criminal offence.

Regarding the other EU mutual recognition instruments, the Republic of Croatia has not developed any practice.

During the on-site visit the prosecutors underlined the importance of direct contacts between judicial authorities.

7.5.3 Surrender/Extradition

a/ Cyber-crime offences punishable by a sentence of imprisonment for a term of three years or more and criminal offences within the scope of the list for European arrest warrants included in the CC are as follows:

- Child enticement for the purpose of satisfying sexual needs (Article 161)
- Exploitation of children for pornography (Article 163)
- Exploitation of children for pornographic performances (Article 164)
- Introducing pornography to children (Article 165)
- Serious criminal offence of child sexual abuse and exploitation (Article 166)
- Unauthorised access (Article 266)
- Computer system interference (Article 267)
- Damage to computer data (Article 268)
- Unauthorised interception of computer data (Article 269)
- Computer-related forgery (Article 270)
- Computer-related fraud (Article 271)
- Misuse of devices (Article 272)
- Serious criminal offences against computer systems, programmes and data (Article 273)

b/ Article 34 of the Act on International Legal Assistance in Criminal Matters stipulates that extradition for purposes of criminal proceedings may only be approved for offences that are according to domestic law punishable by a sentence of imprisonment or a precautionary measure involving deprivation of liberty for a maximum period of at least one year or stricter penalties. Extradition for purposes of enforcing penalties of deprivation of liberty may be approved after the judgment sentencing the offender to imprisonment or imposing a precautionary measure involving deprivation of liberty has become final, for a minimum period of four months. By way of exception, if the extradition request includes several separate offences, some of which do not meet the requirements with regard to the length of the sentence or in the case of offences that only carry financial penalties, extradition may be approved for those offences also.

District State Attorney's offices are competent to receive European arrest warrants depending on the location of the person against whom the warrant has been issued, while District State Attorney's offices and domestic courts are competent to send European arrest warrants to the LEA of the executing state.

The Ministry of Justice of the Republic of Croatia is competent for sending/receiving extradition requests. Communication is effected in the usual way via Interpol/S.I.Re.N.E offices and the European Judicial Network in Criminal Matters.

In its reply to the questionnaire Croatia stated that it does not possess statistics in this area.
However, it was said during the on-site visit that the MoI keeps statistics on extradited persons. No figures have been provided to the evaluation team.

There are no specific procedures or conditions that need to be fulfilled in the Republic of Croatia, as regards extradition requests related to cybercrime. Such requests are handled in the same way as requests related to other types of offences.

Temporary arrests for extradition purposes may occur. Besides the form and content required for every extradition request, the request for temporary arrest must include a statement from the judicial authority on the existence of a final judgment or the decision on detention as well as a statement on the arrest for extradition purposes.

In the Republic of Croatia, the legal surrender procedure is an urgent procedure which applies the time-limits set out by the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States. The extradition procedure is somewhat slower, taking into account several factors, such as means of communication, delivery, legal remedies etc. The average extradition time is 6 months.

To date, the Republic of Croatia has not applied the surrender procedure provided for in the Agreement on the surrender procedure between the EU Member States, Iceland and Norway.
In 2014 the United States of America sent an extradition request and the requested person was extradited to the United States of America from the Republic of Croatia for purposes of criminal proceedings for breaching confidentiality, integrity and the availability of computer data, programmes or systems and computer forgery.

7.6 Conclusions

- Croatia is not party to the MLA 2000 Convention;

- The contribution of Croatia to the international investigation on the ZEUS malware was active and very effective and demonstrates its operational capacity to cooperate with other countries;

- A clear message was conveyed by Croatian prosecutors that there is a need in Croatia to make appropriate arrangements for developing direct contacts between judicial authorities abroad;

- The prosecution service has produced a handbook for practitioners dealing with MLA: this can be seen as a good practice;

- There is a need also to improve the international legal framework (3rd countries/Russia);

- In the EMPACT CA the Croatian experts were very active, and they were the driver in one OAP cooperation with Slovenia. It is a very good example of proactive activity.

- No comprehensive/consolidated statistics in the area: this should be improved;

- No experience of mutual recognition instruments /except freezing orders.

8 TRAINING, AWARENESS RAISING AND PREVENTION

8.1 Specific training

As part of the training provided, the Judicial Academy organised two activities at the regional level in 2014 on the premises of the Regional Centre for Judicial Training on Cybercrime:

A two-day seminar was held in January 2014 entitled “Fighting Cybercrime and Child Pornography on the Internet” for 40 attendees in cooperation with the Technical Assistance and Information Exchange instrument (TAIEX) and the Academy of European Law (ERA). The aim of the seminar was to determine how international and European laws are applied in different MS and Candidate States in relation to cybercrime, as well as to assess the prospect of establishing efficient international cooperation in the suppression of cybercrime. The manner in which non-EU members faced the challenges of cybercrime was also discussed at the seminar.

A two-day seminar was held in October 2014 entitled "Cybercrime" for 29 attendees in cooperation with the Judicial Academy and the company INsig2, whose experts gave lectures pro bono. The following topics were discussed at the seminar: digital evidence and forensics, cybercrime, computers and networks, the Internet, mobile phones, electronic documents and the latest trends in cybercrime. Participants from the Regional Centre's user states participated in both seminars. The Judicial Academy aims to organise another regional seminar on the suppression of cybercrime by the end of 2015.

Although issues relating to cyber crime against children have been included in police education in previous years, in various training programmes and specialisations, as well as in the programmes of some courses at the Police Academy, only since 2012 has targeted specialist training for police officers in this field been carried out. From February 13, 2012 to October 24, 2013, as part of Component II of the IPA 2009 project "Capacity building in the field against sexual exploitation and sexual abuse of children and on police assistance to vulnerable crime victims", organised by the Police Academy and the MUP department which deals with juvenile delinquency and crime against families and young persons, 32 seminars were held (between 2 and 14 days in duration) for more than 800 participants - police officers, social workers, prosecutors and judges. These seminars were attended by a total of 330 police officers working on juvenile delinquency, economic crime and prevention.

In accordance with the obligations arising from the IPA 2009 "Capacity building in the field of combating sexual exploitation and sexual abuse of children and on police assistance to vulnerable crime victims" and the need to constantly refresh and upgrade police officers' knowledge and skills, course contents in the area of criminal offences related to sexual child abuse on the Internet and child pornography have been included in the existing programme of specialist training for police officers and youth investigators A specialised course on juvenile delinquency and crime against youth and families is held annually for 30 police officers.

In the second year of the Police Academy course, students are offered a module on Digital Evidence Forensics. It is about LEAs' methods and techniques for collecting, processing and storing data and information that can be found on electronic media such as computers, servers, Internet-based cloud systems, databases, mobile and GPS devices, memory cards, USB memory sticks and all other electronic carriers where it is possible to store the data (home appliances, CCTV etc.). Students are trained in identifying and securing the digital evidence which is the subject of the investigation. The role of the court expert in computer forensics is also explained. Students are trained in advanced Internet usage and web browsing, data mining files (images, meta-data), as well as all open source techniques and software which may be useful.

From November 2012 to date, there have been three such specialised courses, attended by 102 police officers of the criminal police. Within the overall timetable of the course, the contents of the IPA project have been implemented in a total of 76 teaching hours.

Special training programmes for young police officers and youth investigators have also been developed with a view to ongoing professional training through a specialised seminar on "The study of sexual crimes against children through the Internet" and "New technologies and electronic crime."

In addition to specialisation and professional training of police officers in the area of cyber crime against children, the Police Academy also organises seminars and other courses in the area of cyber crime.
In the last three years, as part of the specialist course on combating economic crime and corruption, lectures have been held on the topic of high-tech (computer) crime. From 2013 to 2014 these courses were held for a total of 60 professional trainees.

The High-Tech Crime Department is responsible for organising and providing cybercrime-related training for all police officers responsible for the suppression of cybercrime, as well as digital forensics. This training is generally provided by international organisations. In this connection, whenever possible Croatia participates in education given by ECTEG and University College Dublin (courses held in Avila, Spain once a year), CEPOL (various courses organised across the EU), EC3 conferences and seminars held at Europol HQ in The Hague, OLAF international LE training courses (Hercule II and Hercule III) currently being held in Zagreb on different forensic topics, as well as training given by police officers from the Spanish police given through the IPA 2011 project (in 2015).

Croatia has been an ECTEG member since April 2014 and regularly participates in the ECTEG meeting at the Europol HQ. In 2014 and 2015, Croatian police officers participated in the ECTEG training courses on Linux Forensics organised by the Spanish National Police training centre in Avila, Spain.

The organisation of training on cybercrime falls under the competence of the professional training and specialisation department of the Police Academy, which each year draws up plans for police training, on a proposal from the organisational units of the Ministry of the Interior, in accordance with their estimates and needs. However, different forms of training can be organised locally, but may have an international dimension in the form of conferences, expert meetings and working meetings, in the organisation of which the Police Academy is involved, when individual organisational units so request.

Police officers who so wish can follow CEPOL activities by attending webinars in English. For example, in 2014 they were able to participate in a webinar on "Cybercrime: Disclosure, Investigation and Prevention", which was held on 27 November 2014.

All courses are financed from the regular budget funds. It is difficult to give an exact figure for the cost of an individual seminar or training event because it depends not only on the number of participants but also on the location where the seminar is held, as well on which organisational unit (city) the attendees come from. For example, a specialist training course for police officers and youth investigators costs about HRK 350,000.00 and a specialist seminar on "Investigation of sexual crimes against children through the Internet" around 15,000.00.

The judicial training programme of the Judicial Academy is attended by judges and deputy prosecutors and some of them act as contacts for international cooperation in criminal matters, but currently no programmes have been developed exclusively for these judicial staff in the field of the suppression of cybercrime.

Since 2013, in cooperation with the US Embassy in the Republic of Croatia and the Police Academy of the Ministry of the Interior, a "Partnership for Education" project has been implemented, with the aim of strengthening international police cooperation. Each year, as part of the project, 5 modules have been carried out on different topics. The participants are the police officers and prosecutors from the region (Albania, Bosnia and Herzegovina, Montenegro, Croatia, Kosovo, Macedonia, Slovenia and Serbia), and the lecturers are experts from Croatia and the United States. Also, each year the project includes a foreign partner, and thus in 2013 the partner was Great Britain, in 2014 Austria and in 2015 France. These countries participate by contributing their experts on various subject areas. In 2013 a 5-day module was carried out on the subject of computer crime, and the lecturers were experts from Croatia and the United States (Purdue University). In 2014 a 5-day module was carried out on the subject of computer crime and electronic evidence: the lecturers were experts from the US Secret Service and the private sector (Global Investigations Citi Security & Investigative Services, Global Security and Investigations, CISSP, FIS Global incidents and EECTF Rome). In 2015 a 5-day module was carried out on the topic of computer and network intrusions: the lecturers were US Secret Service agents. In each module, 4 representatives of the abovementioned countries take part (3 police officers and one specialised prosecutor). The project aims to strengthen international police cooperation and to develop a regional network of police officers to combat all forms of crime with a focus on organised, computer crime and terrorism.

The Regional Pilot Centre (hereinafter: Centre) for Judicial Training on Cybercrime was set up as part of the IPA 2010 project “Regional Cooperation in the Fight against Cybercrime in South-East Europe”. The goal of the project was to strengthen the capacities of the judicial authorities and the Ministries of Internal Affairs of states in the western Balkans and Turkey in order to establish efficient cooperation in the suppression of cybercrime.

The pilot centre operates in Zagreb, as an organisational unit of the Judicial Academy, the institution responsible for training candidates for posts as judges and deputy prosecutors (attending the State School for Judicial Officials), trainees, judicial advisors and judicial officials.

The Police Academy, includes in its courses themes and modules relating to cybercrime. For instance, in the specialised graduate course in criminology (2nd year), attended annually by 50 part-time students, within the subject "Crime against children and minors", there are 5 hours of lectures covering the identification of victims and of perpetrators of crimes against children based on open sources and darknet sources. During the classes the students are also trained to use the website www.sigurnijiinternetnet.hr.

The Police Academy implements a higher education programme, 'Police Officer', in which police officers are trained to conduct their work on the basic level.

Within its faculties, the lecturer Nikola Protrka teaches an elective course on Digital Forensic Evidence over one semester. The course covers criminal methods and techniques for collecting, processing and storing data and information that can be found on electronic media such as computers, servers, Internet-based cloud systems, databases, mobile and GPS devices, memory cards, USB memory sticks and all other electronic carriers where it is possible to store the data (home appliances, CCTV etc.). Students are trained in identifying and securing the digital evidence which is the subject of the investigation. Students are trained in advanced Internet use and web browsing, data mining files (images, meta-data), as well as all open-source resources.

Within its professional higher education study programme the Faculty of Electronic Engineering and Computing of Zagreb University features in its syllabus 'Software Engineering and Information Systems', 'Telecommunication and Informatics'. The Faculty of Organisation and Informatics of Varaždin University includes 'Security information services' in its syllabus.

As outlined above, Croatian authorities took part in a number of training activities in the field of cybercrime, both at national and international level. However, as was stated several times during the on-site visit, there is a clear need for systematic and joint education targeted at all authorities involved in the area, namely police, prosecutors and judges.

8.2 Awareness raising

As part of a national campaign, 'Living Life Free of Violence', Croatia continually raises public awareness in order to encourage the general public to report offences against children. This relates in particular to the campaign conducted in early 2010, which at the time it was launched was intended solely for victims of domestic violence; since 2013, however, Croatia has changed its target group and has expanded the goals of the national campaign to also encompass the prevention of all forms of violence against children, including sexual violence, promoting a culture of non-violence, non-discrimination and tolerance, and has teamed up with the Ministry of Science, Education and Sports in order to conduct the campaign in all schools within the territory of the Republic of Croatia.

The national CERT permanently disseminates information with a view to raising public awareness. To that end, information is disseminated via web pages as alerts and news, and several brochures have been printed and distributed in daily newspapers. The names of the brochures are as follows: 'How to be safer on the internet', 'How to conduct business on the internet more safely', 'Threats on Facebook' and 'How to maintain more privacy on Facebook'. Representatives of the National CERT often give public presentations in the form of conferences or national TV broadcasts.

The public and civil sectors have undertaken numerous activities and projects aiming to prevent online abuse, especially in schools. The 'Child Online Safety' project, which has been conducted in five different Croatian schools and is funded by the European Union, has resulted in the development of a school curriculum on safe internet use and the creation of more than 800 items of learning content for pupils, teachers and parents.

In the area of personal data protection, the Republic of Croatia has undertaken intensive measures by raising public awareness (via workshops, press conferences and expert lectures), in order to reduce cybercrime to a minimum.

8.3 Prevention

8.3.1 National legislation/policy and other measures

As stated above, countering cybercrime has been recognised in Croatia as one of the five priority areas which require the definition of strategic goals and which are specifically defined in the National Cyber Security Strategy adopted on 7 October 2015.

In addition, all four links in the (five) selected areas of cyber security, which are also defined in the Strategy, aim to support efforts to counter cybercrime.

The links in question are as follows: 1. Sensitive information protection, 2. Technical coordination in the treatment of security incidents, 3. International cooperation, and 4. Education, research, development and raising awareness of security in cyberspace.

One of the goals defined in the Draft Strategy for 'Technical coordination in the treatment of security incidents' is 'Regular implementation of measures for improving security through warnings and recommendations'.

In addition, in 'Education, research, development and raising awareness of security in cyberspace', the Draft Strategy and the action plan for the implementation thereof define a number of activities aimed at systematic education and professional knowledge acquisition in the area of cyber security, raising security awareness among internet users and the implementation of certain measures on the part of operators, with a view to preventing security incidents (e.g. publishing recommendations on the minimum security requirements for users of public and commercial wireless networks).

Prevention also constitutes an integral part of police activities. The Ministry of the Interior's Annual Work Plan for 2015 highlights the prevention of all forms of crime. The Prevention Service is a specialised department within the General Police Director`s Office and coordinates all prevention activities within the police, on both a national and a regional level.

The information security act does not identify specific measures relating to prevention and security awareness; however, in order to reduce the number of cyber incidents, the National CERT provides the following services to its constituency on the basis of best practices:

- publishing news and alerts relating to information security
- publishing white papers and brochures
- occasional TV and broadcasts
- publishing information about software vulnerabilities
- providing a vulnerability scan to commercial and non-commercial institutions on demand
- providing a regular vulnerability scan to the CARNet constituency.

The public and civil sectors have undertaken numerous activities and projects aiming to prevent online abuse, especially in schools. The 'Child Online Safety' project, which has been conducted in five different Croatian schools and is funded by the European Union, has resulted in the development of a school curriculum on safe internet use and the creation of more than 800 items of learning content for pupils, teachers and parents.

In the area of personal data protection, the Republic of Croatia has undertaken intensive measures by raising public awareness (via workshops, press conferences and expert lectures) in order to reduce cybercrime to a minimum.

THE RED BUTTON APPLICATION FOR REPORTING CRIME ON THE INTERNET

https://redbutton.mup.hr/

This application allows anyone to report crime, incidents on the internet and criminal activities on the internet and is intended for all citizens, but is especially suitable for children and enables the reporting of internet content which children suspect is illegal and which refers to various forms of exploitation or abuse of children. The application is not intended to act as a substitute for reporting a crime directly to a police station or calling the police emergency number, so there is a special disclaimer: '*In case of emergency, please call the police number 192 immediately or notify an adult whom you trust and ask him/her to call the police or come to the nearest police department or police station and ask for police assistance. We are able to read your message only from Monday to Friday from 8.30 to 15.30. Due to legal restrictions, we are able to receive and respond to complaints received from Croatia only*'.

CROATIAN NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

http://www.cert.hr/en/start

The National CERT has issued four brochures:

1. 'Safer Business on the internet' - http://www.cert.hr/sites/default/files/sigurnije_poslovanje_na_internetu.pdf

2. 'Safer on the internet' - http://www.cert.hr/sites/default/files/sigurnije%20na%20internetu.pdf

3. 'Protect your privacy on Facebook' http://www.cert.hr/sites/default/files/Facebook%20brosura%20v2%20(2012).pdf

4. 'Dangers of Facebook' http://www.cert.hr/sites/default/files/Opasnosti%20Facebooka.pdf

SAFER INTERNET CENTRE / CENTAR ZA SIGURNIJI INTERNET

http://www.saferinternet.hr/ or http://www.sigurnijiinternet.hr/

OBJECTIVES OF THE SAFER INTERNET CENTRE

The application of new technologies in everyday life, learning, teaching and work greatly facilitates work and learning, but requires the continuous education of technology users, especially as regards the possible risks and dangers which the connection of networks may present to both adults and children. The establishment of the Safer Internet Centre brings together the activities of various organisations in Croatia currently dealing with that issue from different perspectives - psychological, pedagogical, computing, information, legal and sociological. This gives users (children, parents, teachers, educators and other internet users) a single point of access to information and educational materials that cover all these aspects of child safety on the internet, and allows them to report the possible violation of online child safety. Informational and educational materials drafted by that centre in cooperation with its partners cover the following topics:

- The protection of personal data and privacy
- Online collaboration and communication
- Online learning and research
- Safely searching internet content
- Making friends, socialising with friends and online fun.

The aim of the Centre is also to encourage the institutionalised introduction of computer and information security in the educational system, e.g. as part of the curriculum for primary and secondary schools. The centre is open to partnerships with all stakeholders dealing with a safer online environment for children. The Centre also already cooperates with certain international organisations dealing with this issue and intends to deepen and expand that cooperation. An important goal of the Centre is to promote computer and information security and awareness of the importance of child safety in an online environment as a prerequisite for healthy and successful development and growth.

The Safer Internet Centre is governed by guidelines issued by the European Union for the Safer Internet project. By organising various events, panel discussions, public lectures, workshops, presentations and lectures, it will ensure the fulfilment of the Centre's main objectives, and raise public awareness about the importance of safety on the internet. The Centre operates through strategic partners, members of the Centre and the project sponsors.

Strategic partners of the Safer Internet Centre include the following:

- the Agency for Personal Data Protection
- the Agency for Education
- the Croatian Academic and Research Network and National CERT
- HAKOM - Croatian Agency for Post and Electronic Communications
- the Ministry of Social Affairs and Youth
- the Ministry of the Interior
- the Ministry of Public Administration
- the Ministry of Science, Education and Sports
- Gornji Bukovec elementary school
- the Child Protection Clinic in Zagreb
- the Polytechnic of Zagreb
- the Teachers' Association 'Partners in Learning'
- XV. Gymnasium Zagreb.

TEACHERS' ASSOCIATION 'PARTNERS IN LEARNING'
National campaign 'Safer Internet for Children and Young People 2013'

The 'Partners in Learning' Association has in recent years organised a series of activities around the theme of 'A Safer Internet for Children and Young People', and has represented Croatia as the Safer Internet Committee in INSAFE. Last year's campaign responded to a large number of teachers and students whose works are presented in a multimedia exhibition and methodical manual entitled 'How to teach children about safer, more appropriate and responsible behaviour on the internet'. The activities involved around 5 000 participants directly and more than 50 000 indirectly. As a result of those activities, the Croatian national campaign 2013 was declared the best Safer Internet Committee in 99 countries. The theme of the national campaign was 'Online rights and responsibilities'.

The police officers for prevention, in coordination with the police officers for youth at local level, are implementing various prevention programmes in their local community with numerous partners and civil society organisations in order to prevent various forms of sexual abuse of children via the internet and social networks (projects entitled 'Living Life Free of Violence', 'I have a choice', 'Together we can do more', etc.).

In 2011, as part of the Council of Europe campaign to stop sexual violence against children, the Ministry of the Interior launched a project with a wide range of prevention activities at local and regional level entitled 'Kiko and the Hand'. In some police departments certain activities are still in progress. The main activities are both educational and informative in terms of the workshops and lectures for children, parents and professionals as well as police officers. In addition to the training activities, thematic press conferences, public debates, round-table discussions, performances for children, public promotional events of the campaign, TV and radio shows and the like have also been carried out. Besides promoting the Convention and its objectives, such activities aim to raise public awareness of the subject and to encourage the reporting of such events, as well as to inform the general public about where and how to request the necessary assistance. The campaign uses standard promotional materials (leaflets, posters and videos) bearing the logo 'Kiko and the Hand'.

8.3.2 Public/Private Partnership (PPP)

Croatia does not use public/private partnership in a formal way (contracts etc.) in terms of preventing and combating cybercrime. However, there are some joint campaigns, public releases, operative meetings and educational activities.

8.4 Conclusions

- In Croatia, as in most Member States, there is a general need to improve the education of newcomers as well as to enhance the training of experienced practitioners in the field of cybercrime; police training seems to focus mainly on forensic activities and would need to be reinforced, even in the field of internet investigations;

- During the on-site visit, the team was informed that there is an ongoing project for creating a basic training package dedicated to 'first responders', i.e. local police officers, in order to respond properly to cybercrime cases; such a project should be strongly encouraged;

- The Regional Pilot Centre for Judicial Training on Cybercrime, set up as part of the IPA 2010 project 'Regional Cooperation in the Fight against Cybercrime in South-East Europe', still operates in Zagreb, as an organisational unit of the national Judicial Academy; it should continue to be supported and indeed encouraged as a good example of regional cooperation in the field of training;

- The on-site visit made it clear that the systematic and joint training of police, prosecutors and judges is vital, in order to ensure that every stakeholder in the system has a correct understanding of the role and needs of other interveners and of how to detect, obtain and use e-evidence.

9 FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions by Croatia

It should be noted that the Republic of Croatia was among the first states to ratify the Council of Europe Convention on Cybercrime and that the Secretariat of T-CY assessed that the Republic of Croatia complies with the provisions of the Convention on Cybercrime with regard to standardisation and enforcement. Croatia also actively cooperates with other parties to that Convention within the T-CY.

November 2010 saw the launch of a joint project of the EU and the Council of Europe, 'CyberCrime@IPA - regional cooperation in the fight against cybercrime', which ended in June 2013; apart from the Republic of Croatia, the project's beneficiaries were Albania, Bosnia and Herzegovina, Montenegro, Kosovo, Macedonia, Serbia and Turkey. During the initial phase, a detailed report was drawn up on the state of crime for each country project beneficiary, and formed the basis for improving upon the current state of affairs. Upon completion of the project, a new assessment of the state of cybercrime was made, thereby establishing that significant improvements had been made in all areas of the project, especially in bilateral and multilateral relations in the region. In addition, it was established that the project had resulted in a better understanding of the issue of cybercrime as a threat to society, that to that end a number of measures ought to be introduced at national, regional and international level, including the establishment of a strategy for combating cybercrime, and that it is necessary to invest additional resources in the professional training of police officers. Consequently, on 15 February 2013, a Strategic Priorities Declaration on cybercrime was issued.

On 28 June 2012 a new Regulation concerning the Internal Organisation of the MoI came into force, calling for the establishment of a High-tech Crime Department within the National Police Office for the Suppression of Corruption and Organised Crime (NPOSCOC). In addition, forensic experts for digital evidence were introduced within the Forensic Centre. On a regional level there are specially trained police officers in Services/Departments/Divisions of economic crime in each Police Administration, who are responsible for cybercrime issues and IPR violations. Furthermore, certain offences in the area of cybercrime (under the Convention on Cyber Crime) cover other organisational units: Child pornography on a computer system or network - General Crime Department, the Division of Juvenile Delinquency; Computer Fraud - Organised Crime Department; Racial and other Discrimination - counter terrorism. As a NATO member, Croatia is developing the military and the civilian component of defence against threats from cybercrime – the MOI is involved in the work of multidisciplinary bodies whose objective is to ensure an effective national response to the threat of cybercrime.

Furthermore, the National Cyber Security Strategy, together with an Action Plan, has been drawn up in conjunction with all the bodies responsible for cybersecurity in Croatia.

Croatia has implemented the IPA 2011 project - 'Strengthening the capacities of the Ministry of the Interior to combat Cybercrime', which was implemented jointly by the Spanish Ministry of the Interior and the Austrian Federal Ministry of the Interior. The purpose of the project was to strengthen the capacities of the Croatian Ministry of the Interior to effectively combat cybercrime at national and international levels, in line with the related EU policies and strategies. Project activities were organised around two main components. The first component intended to enhance the activities of the MoI's Forensic Science Centre through the implementation of a long-term training scheme and a Train-the-trainers programme on topics relating to forensic cybercrime investigation. The second component focused on new tools and techniques used in cybercrime investigations with the aim of strengthening the capacities of the Croatian Criminal Police Directorate in fighting cybercrime at national, regional, European and international levels.

Nevertheless, within the MoI there is still a lack of capacity and limited resources especially in terms of the number of police officers and level of financial support. Closer integration of law enforcement agencies and other stakeholders is also necessary.

Computer fraud is the most common cybercrime offence. The State Attorney's offices issued over 96 indictments for that offence in 2014. The establishment of the Regional Centre is undoubtedly an excellent idea and an example of good practice. It is up to the states involved to step up efforts in order for the practice to take root.

The public and civil sectors have undertaken numerous activities and projects aiming to prevent online abuse, especially in schools. The 'Child Online Safety' project, which has been conducted in five different Croatian schools and was funded by the European Union, has resulted in the development of a school curriculum on safe internet use and the creation of more than 800 items of learning content for pupils, teachers and parents.

In the area of personal data protection, the Republic of Croatia has undertaken intensive measures by raising public awareness (via workshops, press conferences and expert lectures) in order to reduce cybercrime to a minimum.

Within the 2015 Operational Action Plan (OAP) of the EMPACT Priority G 'Cybercrime Attacks', strategic goal 5 was identified 'to contribute to the establishment of a coordinated multidisciplinary mechanism for response in the event of a serious cyber-attack with a cross-border dimension with well-defined roles, responsibilities and procedures'. The project team, consisting of HR, SI, DE, PT, IE, EUROPOL, EUROJUST, DG HOME and EUCTF, is taking part in Operational activity 5.1 'to draft guidelines and/or operational procedures for improving operational national contact points (NCP) for the exchange of information in accordance with Article 13 of Directive 2013/40/EU on attacks against information systems'.

This action is currently the only action designed to implement strategic goal no. 5. Operational national contact points (NCP) for the exchange of information in accordance with Article 13 of Directive 2013/40/EU on attacks against information systems are designed to respond promptly to request(s) from other Member State(s) in terms of data retention, suspect location or information required in order to carry out a criminal investigation into cyber-attacks. The swift exchange of information is an important component of the coordinated multidisciplinary mechanism for response in the event of a serious cyber-attack with a cross-border dimension with well-defined roles, responsibilities and procedures.

The cross-border dimension is the main characteristic of cyber-attacks. Offenders originate in one country, the server through which the crime is being committed is located in a different country and victims are usually located in various countries throughout the world. In order to fight cybercrimes committed by OCGs effectively, cooperation between countries must take place in real time as the crime happens. Enhanced cooperation between the Member States in terms of evidence and data preservation and collection should ensure the success of cyber-crime investigations with a cross-border dimension. The guidelines and/or operational procedures for improving operational national contact points (NCP) for the exchange of information will be the result of the action. The guidelines and/or operational procedures should be implemented in the daily operations of the Member States` NCPs. The number of the NCPs adopting guidelines and/or operational procedures should be regarded as a measurement of success. Croatia is the Action Leader and cooperates with the Member States to ensure the smooth exchange of information between the MS.

As examples of good practice, the Croatian authorities have identified the 'Cyber Coalition' within NATO, involvement in EMPACT, FP Cyborg, and cooperation on operation BUG BYTE etc. Participation in international operations is a very valuable experience for us and provides a good opportunity to monitor the national capacity to face the challenges presented by major cybercrime operations and projects.

Examples of good practice in the area of prevention undoubtedly include the organisation of events that raise awareness among the general population and experts. In response to this, Croatia has performed several botnet mitigation actions and stopped malware spreading in its constituency.

The Croatian authorities have said that there is a need for sufficient financial, human and technical recourses to enable effective measures to combat cybercrime. The legislation has to keep up with the new and rapidly growing technologies that often produce new forms of cyber threats. Prevention activities should be intensified as well as cooperation among all stakeholders in Cybersecurity.

The better and faster exchange and sharing of information (e.g. Malware Analysis), formalising coordination and information exchange among Government CERT Teams of EU Member States.

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

Croatia should conduct a follow-up to the recommendations contained in this report 18 months after the evaluation and report to the Working Party on General Affairs, including Evaluations (GENVAL) on the progress made.

The evaluation team deemed it appropriate to make a number of suggestions for the attention of the Croatian authorities. Furthermore, based on the various best practices, related recommendations to the EU, its institutions and agencies, and to Europol in particular, are also put forward.

9.2.1 Recommendations to Croatia

1. Croatia is encouraged to fully implement the National Cyber Security Strategy and its associated Action Plan;

2. Croatia should develop a mechanism to provide detailed, standardised and comprehensive statistics on investigations, prosecutions and convictions relating to cybercrime at national level and also in relation to international cooperation; in particular, Croatia should finalise and implement the results of the IPA 2010 Project for the development of an International Legal Assistance (ILA) IT System regarding the collection of statistical data on mutual legal assistance and judicial cooperation which involve criminal offences in relation to cybercrime and make it fully operational;

3. Croatia should significantly strengthen its human and technical resources in order to combat cybercrime, in particular within the investigative and forensic police services;

4. Croatia should be encouraged to improve coordination between the various stakeholders involved in the fight against cybercrime at national level;

5. Croatia should improve both the general and specific advanced training in cybercrime for police officers, judges and prosecutors at all levels, in particular by establishing the exchange of information and best practices between all the authorities involved through joint educational activities;

6. Croatia should continue to support, as best it can, the very useful regional training activities of the Regional Pilot Centre for training judicial officials on combating cybercrime, established in Zagreb;

7. According to the National Cyber Security Strategy, which aims to 'continuously improve the national legislative framework, taking into account international obligations', Croatia should further analyse its legislation and practice, in particular as regards the introduction of new investigative techniques, and in order to reflect new trends in cybercrime (such as virtual currencies);

8. Croatia should consider creating a network of focal points for prosecutors specially trained in the field of cybercrime at all levels of the prosecution service in order to support the dissemination of information and best practices in the field of cybercrime; official contact points should also be established for Courts;

9. Croatia should promote direct contacts between judicial authorities in international cooperation in cybercrime;

10. Croatia should consider developing a user-friendly handbook of best practices for local police officers as first responders and other non-specialised police officers;

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

The Member States and the European Union institutions should:

11. Explore the possibility of creating common statistical denominators in the field of cybercrime, including harmonised methodology, methods for data collection and evaluation at European Union level;

12. Encourage the organisation, at EU level, of operationally-oriented trainings on the whole life-cycle of cybercrime, whereby the speakers and participants involved are police officers, prosecutors and judges and, where appropriate, practitioners from the private sector;

13. Consider ways of improving external cooperation in the field of cybercrime with third countries, and in particular major neighbours and partners;

The European Commission should:

14. Take a more active part in the seventh round of mutual evaluations on Cybercrime;

15. Consider ways of supporting, in particular through appropriate co-funding, the very useful activities of the Regional Pilot Centre for training judicial officials on combating cybercrime in Zagreb, Croatia;

16. Consider the possibility of providing the Member States' competent authorities with the technical means necessary for tackling cybercrime, and in particular providing funds for the acquisition of high-tech hardware and software for the better identification and extraction of e-evidence; one added value of this is that it would enable the Member States' authorities to work and cooperate with comparable e-evidence.

9.2.3 Recommendations to Eurojust/Europol/ENISA and to EJTN

17. The European Judicial Training Network should establish regular joint training programmes for police officers, prosecutors and judges in the field of cybercrime; this would again be done in coordination and cooperation with Eurojust and Europol;

18. Europol and Eurojust should pursue and enhance, as far as possible, their active contribution to the seventh round of mutual evaluations in all Member States;

19. Europol should continue to encourage close cooperation between Member States' law enforcement services in the technical field, using dedicated workshops or meetings in specifically defined tasks (Botnets, Bitcoins, laundry mule money, malware threats, etc.);

20. Eurojust should continue to provide support for Member States in the area of combating cybercrime within its mandate, in particular by means of coordination meetings, as well as by supporting the exchange of best practices.

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

Tuesday 29 September 2015

Ministry of the Interior – General Police Directorate

Visit to High-tech Crime Department

- Welcome
- Organisation and Operations of the High-tech Crime Department
- Case Study – ZeuS Banking Malware
- Overview – National 24/7 Contact Point for Urgent Requests
- Overview – Croatian Participation to EMPACT Cyber Attacks
- Overview – Child Sexual Abuse Online and Child Pornography
- Overview – Online Card Fraud

Visit to Zagreb Regional unit of the National Police Office for the Suppression of Corruption and Organised Crime

- Practical operations – Search and Seizure of Computer Data

Visit to the Centre for Forensic Science, Research and Expertise "Ivan Vučetić"

- Overview – Computer Forensic Examinations

Wednesday 30 September 2015

Visit to State Attorney's Office of the Republic of Croatia

- Presentation of the State Attorney's Office work in cybercrime matters

Visit to National CERT Office

- Introduction to National CERT, its role and operations
  - Legal framework
  - Internal organisation and operations of National CERT
  - Overview of everyday CERT operations

- Introduction to cyber threat intelligence and incident statistics

- International and domestic cooperation:
  - Current cyber defence projects
  -cooperation on EU and NATO cyber defence exercises
  -brief demonstration of National CERT internal and public services
  -overview of National CERT infrastructure

Thursday 1 October 2015

Visit to Ministry of Justice

- Presentation of the national legislation and the transposition/implementation of the EU legislation:
  - Sector for Criminal Law
  - Sector for Mutual Legal Assistance and Judicial Cooperation in Criminal Matters
- Court practice – Municipal court

Visit to the Office of the National Security Council

- Overview of the Organisation, Roles and Activities of the Office
- The New National Cyber Security Strategy
  - Internal Proceedings
  - Approach and Methodology
  - Goals and Implementation
- Discussion

End of the Visit

-/-

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 29 September 2015

Venue: **High-tech Crime Department**

Person interviewed/met	Organisation represented/Function
Ms Darko Žižek	Criminal Police Directorate/ Deputy Head
Ms Kristina Posavec	High-tech Crime Department/Head
Mr Renato Grgurić	High-tech Crime Department /Police officer
Mr Ivan Mijatović	High-tech Crime Department /Police officer
Mr Danko Salopek	Juvenile Delinquency and Crimes against Children Department/Police officer
Mr Željko Brkić	Organised Crime Unit/Police officer

Venue: **Zagreb Regional unit of the National Police Office for the Suppression of Corruption and Organised Crime**

Person interviewed/met	Organisation represented/Function
Mr Zoran Filipović	Zagreb Regional Unit of the National Police Office for the Suppression of Corruption and Organised Crime/Head
Mr Dragan Marić	Zagreb Regional Unit of the National Police Office for the Suppression of Corruption and Organised Crime/Crime Analysis officer
Mr Robert Pešt	Zagreb Regional Unit of the National Police Office for the Suppression of Corruption and Organised Crime/ Crime Analysis officer

Venue: **Centre for Forensic Science, Research and Expertise "Ivan Vučetić"**

Person interviewed/met	Organisation represented/Function
Mr Saša Krnjašić	Centre for Forensic Science, Research and Expertise "Ivan Vučetić" *I* Computer Forensic Expert

Meetings on 30 September 2015

Venue: **State Attorney's Office of the Republic of Croatia**

Person interviewed/met	Organisation represented/Function
Mr Dubravko Palijaš	Chief State Attorney's Office/ Deputy

Venue: **National CERT Office**

Person interviewed/met	Organisation represented/Function
Mr Darko Perhoč	National CERT/Head of National CERT
Mr Tibor Kulcar	National CERT/Computer Security Expert

Meetings on 1 October 2015

Venue: **Ministry of Justice**

Person interviewed/met	Organisation represented/Function
Mrs Sanja Nola	Assistant Minister for Criminal Law and Probation
Mrs Ana Kordej	Head of the Sector for Criminal Law
Mr Dinko Kovačević	Head of the Service for Criminal Law Regulations
Mr Hrvoje Bozić	Senior advisor - specialist in the Service for Criminal Law Regulations

Mr Mislav Matić	Senior administrative advisor in the Department for Regulations of Criminal Procedural Law, Juvenile Law and the Execution of Criminal Sanctions
Mr Bojan Ernjakovic	Senior expert advisor in the Department for Extradition and Mutual Legal Assistance in Criminal Matters
Mrs Cornelija Ivanušić	Judge of the Municipal Court in Velika Gorica
Mrs Dasla Leppee Pažanin	Head of the Service for European Affairs in the Directorate for European Affairs, International and Judicial cooperation

Venue: **The Office of the National Security Council**

Person interviewed/met	**Organisation represented/Function**
Mr Aleksandar Klaić	Assistant Director for Information Assurance
Mr Vinko Kuculo	Senior Advisor in Department for Planning and Oversight of Information Assurance

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN CROATIAN OR OTHER ORIGINAL LANGUAGE	FULL NAME IN CROATIAN OR ORIGINAL LANGUAGE	ENGLISH
CEPOL			European Police College
CERT			Computer Emergency Response Team
CMS			Case Management System
CoE			Council of Europe
CSA			Child Sexual Exploitation
ECJ			Court of Justice of the European Union
EC3			European Cybercrime Centre
EGTEC			European Cybercrime Training and Education Group
EJN			European Judicial Network
EJTN			European Judicial Training Network
EMPACT			European Multidisciplinary Platform Against Criminal Threats
ENISA			European Union Agency for Network and Information Security
EUCTF			European Union Cybercrime Task Force

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN CROATIAN OR OTHER ORIGINAL LANGUAGE	FULL NAME IN CROATIAN OR ORIGINAL LANGUAGE	ENGLISH
EUROJUST			European Unit Judicial Cooperation Unit
EUROPOL			European Police Office
FBI			United States Federal Bureau of Investigations
GENVAL			Working Party on General Matters including Evaluations
ICSE			Interpol's International Child Sexual Exploitation Database
ICT			Information and Communications Technology
INTERPOL			International Criminal Police Organization
IOCTA			Internet Organised Crime Threat Assessment
IOT			Internet of Things
IP			Internet Protocol
IPR			Intellectual Property Rights
IT			Information Technology
J-CAT			Joint Cybercrime Action Task Force
JIT			Joint Investigation Team
JHA			Justice and Home Affairs
LEA			Law Enforcement Authorities
MLA			Mutual Legal Assistance

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN CROATIAN OR OTHER ORIGINAL LANGUAGE	FULL NAME IN CROATIAN OR ORIGINAL LANGUAGE	ENGLISH
MLAT			Mutual Legal Assistance Treaty
MoJ			Ministry of Justice
NAW			Nordic Arrest Warrant
NGO			Non-Governmental Organisation
PPP			Public/Private Partnership
SCADA			Supervisory Control and Data Acquisition
SPACE			EC3's restricted virtual platform
SPOC			Single Point of Contact
TOR			The Onion Router
VPN			Virtual Private Network
VPS			Virtual Private Server