Council of the
European Union

Brussels, 10 February 2017
(OR. en)

14585/1/16
REV 1 DCL 1

GENVAL 120
CYBER 133

DECLASSIFICATION

of document:	14585/1/16 REV 1 RESTREINT UE/EU RESTRICTED
dated:	31 January 2017
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Poland

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

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

Council of the
European Union

Brussels, 31 January 2017
(OR. en)

14585/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 120
CYBER 133

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 Poland

ANNEX

Table of Contents

1 EXECUTIVE SUMMARY

The visit was very well prepared by the Polish authorities and included meetings with the relevant actors with responsibilities in the field of preventing and combating cybercrime as well as in the implementation and operation of European policies. These included the Ministry of Interior and Administration, the Ministry of Digital Affairs, the Ministry of Justice, the National Police Headquarters, the Central Investigation Bureau of the Police, the National Security Bureau, the Government Centre for Security, the Prosecution General (currently the National Prosecution), the Polish Office of Electronic Communications, the General Inspector for Personal Data Protection, the Research and Academic Computer Network (NASK), the Internal Security Agency (CERT.GOV.PL) and the Nobody's Children Foundation, a non-governmental organisation.

During the on-site visit the Polish authorities did their utmost to provide the evaluation team with complete information and clarifications on legal and operational aspects of preventing and combating cybercrime, cross-border cooperation and cooperation with EU agencies, and cyber strategy. The courtesy and professionalism of the Polish authorities responsible for putting in place the evaluation visit, their permanent availability during the visit and their readiness to provide further information or clarifications should be highlighted.

The National Cyber Security Strategy of the Republic of Poland is decentralised. Poland does not have a single national cyber security strategy document but instead three main documents related to cyber security: *The Cyberspace Protection Policy of the Republic of Poland, the National Security Strategy of the Republic of Poland* and *the Doctrine of Cybersecurity of the Republic of Poland.* They cover the field of cyber security, cyber defence, cyber awareness, training issues and response to cyber attacks. Taken together with the defined priorities developed in Poland, the strategy provides a solid basis for fighting cybercrime.

The Ministry of Digital Affairs is a political and strategic coordinator for the cybersecurity in Poland. [1] A key challenge in terms of cybersecurity is to create an efficient system with a clear division of competences among the institutions dealing with cybersecurity and cybercrime, and to increase cooperation with companies operating in the field of cybersecurity.

As regards legislation, Poland has signed and ratified the Convention on Cybercrime and implemented the European Directives related to cybercrime in its national legislation. As in many other countries, no specific definition of cybercrime is provided by Polish legislation. At the practical level cybercrime comprises all offences against computer systems and computer data as well as crimes enabled by the use of a computer system. However, it was noticed that the lack of a single definition of cybercrime in legislation may make it difficult to measure all the incidents that fall within the category of cybercrime.

The system responsible for fighting cybercrime seems to be appropriately equipped and dimensioned. In the evaluators' view Poland has built up a robust structure to combat cybercrime and provide cybersecurity.

[1] According to the Law on division of the government administration in Poland.

The visit to and the illustration provided by the National Police highlighted the excellent organisational skills and capability to combat cybercrime as well as a structure aligned with the highest standards in terms of knowledge and expertise. At a central level, the Department for Fighting against Cybercrime was created within the Criminal Service Bureau and is responsible for initiating and co-ordinating Police activities in the area of cybercrime.[2] It also supports work carried out at the regional level where 18 units in total are operational (in each Voivodeship, in Warsaw Metropolitan Police Headquarters and in Central Investigation Bureau of the Police). These units are continuously being equipped with hardware and the police officers being trained to upgrade their qualifications. Although the Department is not actually in charge of each and every case, the support provided to the various regional commands in terms of technological investigations and forensic help makes the established system to combat cybercrime effective. Furthermore, they cooperate with the specialised law enforcement bodies such as the Central Investigation Bureau and the Internal Security Agency.

In general the police and prosecution deal with all kind of crimes, including cybercrime. The investigations are conducted by police officers from the investigations department. However, there is no special corresponding structure within the prosecution service for fighting against cybercrime in the field of operational work. Moreover, taking into consideration the crucial role played by judges and prosecutors, a certain lack of proactivity on their part in listing their own priorities in order to increase professional competences and to raise effectiveness in tackling cybercrime was noted.

[2] After the on-site visit the evaluation team was informed that the Bureau for Fighting Against Cybercrime has been created on 1 December 2016. The Bureau includes four departments i.e. General, Recognition, Operational, Support and Research. There are fifty two police officers and four civilians supposed to be on duty in the near future.

Even though the functioning of Poland's cyberspace protection system is decentralised, it works properly. Such a decentralised approach was also apparent from the existence of several Computer Emergency Response Teams (CERTs) and the governmental computer security incident response team (CERT.GOV.PL).

CERT.GOV.PL works within the structure of the Internal Security Agency and is responsible for enhancing the capability of public services to protect their own information systems. It is also the second level of the National Response System on computer incidents in cyberspace and, as such, the "last resource" for other CERTs or entities dealing with a serious cyber incident. In the case of incidents with a wide-ranging impact, CERT.GOV.PL is to coordinate the response to the attack.

CERT POLSKA, on the other hand, plays the role of a *de facto* national CERT. It was established in the structure of the Polish Research and Academic Computer Network (NASK). It is autonomous from the public administration and it provides a good example of public/private co-operation. Its tasks include responding to threats and incidents in the .pl domain space, providing services for banks and other third parties outside public administration, and security research, creating tools and information systems to protect the country's cyberspace. There are several other CERTs acting in Poland (e.g. MIL-CERT, PIONIERCERT, etc.). That is why formal designation of a national CERT could facilitate coordination of their efforts.

Despite this scattered landscape, NASK and the Internal Security Agency produce very good reports on the cyber situation in the country. They describe the level of the national security systems including the critical ICT infrastructure and the performance of services and institutions responsible for security in Poland.

Strong cooperation with the private sector, in particular in countering child abuse, and with the banking sector, which is strategic and fundamental, should be noted. The cooperation between the Polish police and the Polish Banks Association is an example of very good cooperation between the law enforcement authorities and the private sector. Another impressive example of this kind of collaboration is the work developed by the Nobody's Children Foundation, a non-governmental organisation working with abused children and their families in order to avoid re-victimisation. Special interviewing rooms allow the interviewing of the victims in the physical presence of the judge, the investigator and the prosecutor and at the same time in the hearing of the defence. This means that the victim does not have to be present in court during the trial.

The protection of Polish citizens and companies in cyberspace is strengthened by a number of awareness raising and prevention initiatives conducted by many entities, such as the Ministry of Digital Affairs, the Police, NGOs, academia, etc. However, it seems that there is no general overview of particular actions and their target audiences. Poland also lacks a dedicated budget for awareness raising and prevention campaigns.

An impressive capacity was displayed by the Police Academy and the National School of Judiciary and Public Prosecution regarding training of practitioners. There are many events organised internally or with external partners to raise knowledge among those in charge of fighting cybercrime. Particularly important are joint training sessions organised for judges, prosecutors and police officers to share knowledge and experience. However, it seems that the training does not reach all prosecutors and judges in need of it. Despite the good quality of the work being carried out in this area by the National School of Judiciary and Public Prosecution, training activities are not compulsory.

Also of relevance is international cooperation, including the Eastern Partnership members, training for LEA and the participation in the EMPACT Europol programme (and many other initiatives). Poland cooperates with several EU agencies (Europol/EC3 – Poland is involved in three Focal Points: FP Terminal, FP Cyborg and FP Twins, Eurojust, ENISA), national LEAs (NCA, FBI, BKA) and the private sector (in area of card fraud, the Police cooperates with the Polish Bank Association based on a signed agreement, and it carries out scientific projects in cooperation with universities).

Taking all factors into account, the evaluation team appreciated the way the system works in Poland. The strategy implemented is clearly designed to prepare the country to counteract possible cyber attacks. Considering the significant effort made by the Polish authorities to secure critical infrastructure, governmental bodies and citizens, the opinion of the evaluators is clearly positive.

2 INTRODUCTION

Following the adoption of the Joint Action 97/827/JHA of 5 December 1997[3], 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 European polices on preventing and combating cybercrime.

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud. It should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[4] (transposition date: 18 December 2013), and Directive 2013/40/EU[5] on attacks against information systems (transposition date: 4 September 2015), are particularly relevant in this context.

Moreover, the Council Conclusions of June 2013 on the EU Cybersecurity Strategy[6] reiterate the objective of ratifying the Council of Europe Convention on Cybercrime (the Budapest Convention)[7] 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'. The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.[8]

3 Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997 pp. 7 - 9.
4 OJ L 335, 17.12.2011, p. 1.
5 OJ L 218, 14.8.2013, p. 8.
6 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.
7 CETS no. 185; opened for signature on 23 November 2001, entered into force on 1 July 2004.
8 CETS no. 189; opened for signature on 28 January2003, entered into force on 1 March 2006.

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

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

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

The experts charged with undertaking the evaluation in Poland were Mr Giorgos Karkas (Cyprus), Mr Gianluigi Umeteli (Italy) and Mr Henrik Olin (Sweden). Two observers were also present: Mr José Eduardo Guerra (Eurojust) and Ms Małgorzata Sobusiak-Fischnalle (Europol), together with Mr Steven Cras and Mr Sławomir Buczma from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Poland between 1 and 5 February 2016, and on detailed replies from Poland 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

The cyberspace protection system in Poland is decentralised. The competences related to security of cyberspace are divided between the institutions that pursue their tasks regarding cyber resilience, the prevention of cybercrime and cyber defence. The three main documents relating to cyber security in Poland are:

- *The Cyberspace Protection Policy of the Republic of Poland*

Poland's Council of Ministers adopted *The Cyberspace Protection Policy of the Republic of Poland* (the *Policy*)[9] on 25 June 2013. As regards cyber resilience, the *Policy* refers to *the Strategy Efficient State*[10], the development strategy for public and law enforcement institutions. The strategic objective of the *Policy* is to achieve an acceptable level of security of cyberspace of Poland. Due to the scope of this document which is limited to governmental administration, the minister competent for the information society is responsible for its implementation on behalf of the Council of Ministers.

- *The National Security Strategy of the Republic of Poland*

The National Security Strategy of the Republic of Poland (the *Strategy*) was adopted in 2014. It is a document of a strategic nature that refers to the area of cyber defence. The strategic objective for cyber security set out in the *Strategy* is to ensure the safety of Poland in cyberspace, which includes ensuring an adequate level of national security systems, especially state ICT critical infrastructure and infrastructure essential for the functioning of society and private businesses, including the financial, energy and health sectors.

[9] The above mentioned Policy is available in Polish and English on site: http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html.

[10] http://administracja.mac.gov.pl/adm/departament-administra/strategia-sprawne-panst/8085,Strategia-Sprawne-Panstwo-2020.html

- *The Doctrine of Cybersecurity of the Republic of Poland*

The National Security Bureau (BBN), which is a body providing aid and support to the President of the Republic of Poland in executing security and defence tasks, published a document titled *The Doctrine of Cybersecurity of the Republic of Poland*[11] on 22 January 2015. The document contains official views and findings on objectives, environmental assessments and the operating concept to ensure safe functioning of the state as a whole, its structure, individuals and legal entities – including businesses and other entities without legal personality – in cyberspace.

The Polish authorities intend to create a new system with a clear division of competences among the institutions dealing with cybersecurity and cybercrime and to increase the cooperation of companies operating in the field of cybersecurity. In April 2015 the *Action Plan to ensure safety of cyberspace* was adopted. One of the tasks indicated in the Action Plan is the development of draft guidelines for a national act establishing Poland's cybersecurity system. The Ministry of Digital Affairs is to play a leading role in this. These guidelines will indicate the optimal conception which will be used as a basis for developing a national cybersecurity system, including the powers and tasks assigned to the various institutions. The Ministry of Digital Affairs also commissioned a report entitled *The cybersecurity of Poland*, which was prepared by the experts from the NASK research institute. The report formulates a number of recommendations for establishing a coordinating institution that will ensure the proper functioning of the system at the strategic and legislative level, as well as coordination of operational actions.

[11] https://www.bbn.gov.pl/pl/wydarzenia/6336,Doktryna-cyberbezpieczenstwa-RP.html.

The report also includes recommendations for combating cybercrime, one of which is the preparation of a multiannual *National Programme on Fighting Against Cybercrime*, which will be similar to the recently adopted national program on fighting against terrorism. The recommendations point to the need to ensure that the national CSIRT has the opportunity to report cybercrime to the national police. Finally, the national CSIRT should be used to build competences (skills) of law enforcement bodies: not only the police, but also the public prosecutor's offices and the other judicial bodies.[12]

3.2 National priorities with regard to cybercrime

The *Cyberspace Protection Policy of the Republic of Poland* is a national strategic document within the field of cybersecurity. The *Policy* mainly address cyber resilience aspects of cyberspace protection and indirectly relates to cybercrime through educational and awareness-raising actions. The priorities of the *Policy* include activities in the area of risk assessment; safety of governmental portals; activities in the legislative area; procedural and organisational action through the implementation of best practices and standards in this area; activities in the area of education, training and awareness-raising in the field of security; and action in the field of technical solutions aimed at reducing the risk of threats from cyberspace of Poland.

[12] After the on-site visit the evaluation team was informed that the Ministry of Digital Affairs presented a draft of a new Cybersecurity Strategy in February 2016. The draft of the Strategy is currently under nationwide consultations. Taking into account recent adoption of the Directive on security of network and information systems, the Ministry of Digital Affairs is currently working on comprehensive legislation on National Cybersecurity System. The legislation inter alia is to create a system with clear division of competences among different institutions involved.

Priorities related to the issue of cybercrime were also included in the following government strategic programs adopted by the Council of Ministers:

- *The National Counter-Terrorism Programme for the years 2015-2019.* One of the priorities of this programme is to analyse the possibility of cooperation between public administration and the private sector on preventing the publication and dissemination of content of a terrorist and extremist nature in the media and implement any additional measures in this regard. This task also applies to messages posted on the Internet.
- *The Programme for preventing and combating economic crime for the years 2015-2020.* This includes work to develop tactics and standards for the control of certain aspects of economic crime, including crime related to the development of new technology (cybercrime).

Poland has developed some further programmes that relate to the prevention of crime in cyberspace:

- The *Safety+* programme by the Ministry of National Education for the 2015-2018 period;
- the national program entitled *Safe and friendly school* for the 2014-2020 period.

The programmes incorporate a number of goals and tasks and aim at stabilising the trends and decreasing the range and intensity of problems and difficult behaviours among children and young people. This should help to decrease the level of aggression and violence ad cyber violence, and improve pupils' skills for appropriate behaviour in cyberspace, especially in the area of the new media.

Police priorities in the field of prevention and combating cybercrime

The document titled Concept for police activity on social prevention for 2015-2018 identifies priorities for a creative and multi-institutional approach to social prevention which were recommended at the national level. From the perspective of the police's role in social crime prevention, the most important areas are: raising the level of protection for Polish citizens and companies in cyberspace, and prevention of violence in a broad sense, including peer group violence and cyber violence.

Furthermore, the Commander-in-Chief of the Police issued Priorities of the Chief Commander of the Police for 2016 – 2018, identifying combating crimes committed in cyberspace as one of the main priorities[13]. In order to make the police more effective in identifying and combating the greatest contemporary threats including cybercrime the following tasks were specified:

a) the Voivodeship Police Headquarters and Warsaw Metropolitan Police Headquarters will intensify their operational work on fighting cybercrime;
b) the National Police Headquarters will create a national system for the exchange and coordination of information to assist in the fight against cybercrime. For this purpose technological developments are planned in the departments appointed to combat cybercrime (e.g. through the creation of specialised laboratories for the analysis of IT hardware and software). There are also plans to improve the quality and effectiveness of police work by successively increasing the professional competence of officers and employees of the police, inter alia via specialised training on combating cybercrime.

Implementation of these priorities will involve:

a) introducing a system for obtaining and analysing data from open sources online;
b) constructing the system/hardware platform for research into malicious software such as malware;
c) providing the vertical cells to fight cybercrime with the hardware and software solutions they need to collect and secure of digital evidence;
d) implementing specialised training for officers of the 'cyber' department, conducted at the Police Academy in Szczytno.

[13] Available in Polish: http://isp.policja.pl/isp/aktualnosci/7813,7-priorytetow-Komendanta-Glownego-Policji.html.

Polish police participation in EMPACT

The payment card fraud priority under EMPACT (European Multidisciplinary Platform against Criminal Threats) is supported by the coordinator in the Department for Fighting against Economic Crime (Criminal Service Bureau of the National Police Headquarters). EMPACT Card Fraud operations are priorities, in particular:

- research on card fraud, card not present, AVC, money mules, asset recovery,
- extending operation Joint Action Days, operational meetings and working visits directly related to the conduct of investigations.

Poland is the project leader of the Action dedicated to providing assistance to countries from Eastern Partnership Programme to develop capabilities to counter cybercrime/payment fraud. The project includes training for LEA (law enforcement) with the Eastern Partnership countries and activities for those countries within the framework of the project to develop capacity and instruments for prevention and to explore the phenomenon of crime in the area of card payments. In addition, in the context of EMPACT Card Fraud, the Department for Fighting against Economic Crime participates in the operation 'Airline Ticket Fraud Action Day' organised within the framework of the Joint Action Days.

EMPACT Cyber attacks is a platform designed to improve cooperation between EU Member States, relevant institutions and agencies and partners from the private sector for the production and dissemination of antimalware and defence against network attacks on infrastructure referred to in the Operational Action Plan for 2016. The Department for Fighting against Cybercrime (Criminal Service Bureau of the National Police Headquarters) supports priority dedicated to the identification of links and provision of support among Member States with regard to the use of the EMAS (Europol Malware Analysis System) database – through providing, as far as possible, malware samples for analysis.

The head of the Department for Fighting against Cybercrime is the national contact point for the European Network of Law Enforcement Technology Services (ENLETS) in the area of technology support and exchange of information on new technologies and solutions, research, development, and projects by the Council of Europe.

In the field of combating Cybercrime Child Sexual Exploitation (CSE): the National Police participates in EMPACT CSE, which is focused on CSE and Child Abuse Material (CAM). The Polish police also uses the Europol Information System (EIS) in particular cases. Generally there are no special demands or procedures for cooperation with Europol in this field: it is conducted based on general rules which oblige both sides. Moreover, since September 2014 the National Police has implemented Europol's security policy by engagement in EMPACT CSE. This activity is focused on finding and combating organised criminal groups which are responsible for placing CAM on the internet and uncovering any connections between these groups.

3.3 Statistics on cybercrime

3.3.1 Main trends leading to cybercrime

Since 2003 the general number of crimes committed in Poland has continued to decrease. The crime rate in Poland is currently lower than the European average. However, the Polish authorities reported that cybercrime does not follow this trend. In recent years the prevalence of electronic devices as well as the number of users of various electronic services (mainly internet based) have risen significantly. This has generated new forms and ways of committing criminal offences. In their actions criminals take advantage of the still inadequate knowledge about cyber threats.

According to CERT POLSKA statistics there were 1 282 cyber incidents in 2014. The most common problems were:

- identity theft and phishing – 383 reports;
- abusive content – 370 reports;
- malicious code (malware) – 98 reports;
- information gathering (scanning, sniffing) – 98 reports;
- intrusions and intrusion attempts – 49 reports.

The main objective of perpetrators is to gain information on users (in most cases usernames and passwords for access to various online services). The most popular method of infecting users on Polish networks is malicious email attachments. Traditional phishing targets many different online sites. Besides more traditional targets, such as banks and financial services, popular targets include online gaming sites, social network profiles, email and e-shop accounts.

According to the *Report on the state of security in Poland 2014*, which is a summary of the performance of the services and institutions responsible for the state of security in Poland, cybercrime remains an area of operation for both individual criminals and organised crime groups, extremist communities and terrorist organisations. According to the Polish authorities, the most serious threats in cyberspace which must be tackled in the near future include:

- The growing number of computer crimes against the protection of information, property and public safety associated with the rapid development of information technology, and the extensive use of them in almost every sphere of life;
- the expected continuation of the cyber espionage campaigns against key critical infrastructure institutions and companies;
- the progressive increase over recent years in the position of equipment manufacturers in the global telecommunications market, including the Polish market, in respect of which there is a reasonable suspicion that the equipment is being used for intelligence purposes.

Moreover, analysing the specific nature of cybercrime, it can be assumed that they will include: identity theft, ICT security breaches, the use of malware for criminal purposes, the acquisition of ATM cards, and crypto-currency (money laundering). Furthermore, the financial sector is being targeted by cybercriminals more frequently, especially banks and their customers, e-payment, and e-shops. Criminals are becoming noticeably more professional, and organised crime groups are starting to play a key role. There have also been DDoS attacks and anonymous reports of explosive charges. It should be added that quick development of IT and the most commonly used social engineering techniques will contribute to increasing cybercrime.

3.3.2 Number of registered cases of cyber criminality

The data concerning cybercrime are gathered by various state services (the police, the public prosecution service and courts under the Ministry of Justice) and reflect different stages of investigation into cyber incidents.

Statistics from the office of the Prosecutor General (PG) reveal the number of criminal proceedings initiated, and information about their outcome.

Judicial statistics are separated from the law enforcement authorities' statistics. Data gathered by the Ministry of Justice (based on the courts' statistical reports) reflect the number of criminal cases in which an indictment was filed and the results of those cases (number of people sentenced and penalties imposed).

Statistical data about detected crime, including cybercrime, are collected and processed in the National Police Information System (NPIS). Data are collected based on crimes listed in the Penal Code (PC) and other acts containing penal provisions, and then registered in the NPIS, taking into consideration the different characteristics of each type of crime.

Information about crimes is reported after a police investigation ends and when the complete case is ready to be sent to the prosecution, after the Juvenile Court releases its decision on the initiation and completion of proceedings for a criminal offence, or after the police prepares its decision to discontinue the investigation and the case is entered into the register of crimes. It is only then that information is entered into the NPIS.

According to the Polish authorities, it is possible to generate a statement on the preliminary investigations into cybercrime only (in reference to a particular article of the PC) using the NPIS by taking into consideration the modus operandi, for example 'internet' or 'computer'. However, it should be noted that in part the crimes are defined by the articles, the content of which does not make it possible to determine whether they were committed in cyberspace or not, as specifying the context of the crime (e.g. 'network' or 'internet') is not mandatory when filling in forms in the NPIS, although it may be included under 'modus operandi').

In addition, computer hacking, the theft of computer data, computer eavesdropping and attacks on network devices are rarely reported, which increases the number of hidden crimes. The reasons for this situation include: low awareness among users, who are often unaware that they have become a victim of cybercrime; a reluctance to report crimes associated with the illegal possession of data on a personal computer (e.g. pirated software); or, in the case of companies from which computer data had been stolen, a desire to conceal this fact because they fear losing their reputation and customers.

The NPIS is not integrated with the non-police database.

The following statistics on the number of registered cases, investigations, prosecutions and final convictions were recorded in 2013-2015.

Table 1: Police data

Crimes declared and detected in selected legal categories between 2013 and 2015 based on modus operandi *							
	Legal basis (see Annex 1)	2013		2014		2015**	
		Crimes declared	Crimes detected	Crimes declared	Crimes detected	Crimes declared	Crimes detected
Penal Code	Art. 190a § 2	269	84	439	128	391	90
	Art. 200 § 1	10	8	7	6	26	24
	Art. 200a § 1	12	6	52	47	20	14
	Art. 200a § 2	88	78	57	45	176	159
	Art. 200b	1	0	3	2	1	0
	Art. 202 § 1	10	9	23	16	20	11
	Art. 202 § 2 (annulled)[14]	35	29	66	58	8	7
	Art. 202 § 3	1 823	1 793	2 160	2 136	272	254
	Art. 202 § 4	23	22	19	14	6	5
	Art. 202 § 4a	242	220	120	106	54	46
	Art. 202 § 4b	7	6	8	6	2	2
	Art. 256 § 1	83	7	205	27	132	50
	Art. 256 § 2	1	0	8	6	4	3
	Art. 267 § 1	1 070	335	1 274	198	1 171	177
	Art. 267 § 2	61	18	74	9	75	10
	Art. 267 § 3	31	5	28	8	31	3
	Art. 267 § 4	1	1	4	1	7	4

[14] Art. 202 § 2 stated that 'Whoever presents pornographic material to a minor under 15 years of age or makes available to him or her items of this nature or distributes pornographic material in such a way as to allow him or her acquaintance with such material shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to two years'. The article was annulled by an amendment to the Penal Code on 4 April 2014 (which, after *vacatio legis*, has been in force since 26 May 2014) and by the same amendment was transposed as a new article 200 § 3 with a change concerning the penalty: now it is up to three years of imprisonment.

	Art. 268 § 1	112	20	84	21	54	6
	Art. 268 § 2	43	9	38	7	18	2
	Art. 268a § 1	329	72	374	79	286	58
	Art. 268a § 2	3	2				
	Art. 269a	27	2	23	4	23	2
	Art. 269b § 1	28	7	34	10	29	2
	Art. 271 § 1	117	117	7	5	102	102
	Art. 271 § 2			1	1	1	1
	Art. 271 § 3	27	27	1	1	54	54
	Art. 286 § 1	30 784	23 844	35 987	27 008	31 735	23 537
	Art. 286 § 1 in conjunction with Art. 294 § 1	17	14	28	11	34	8
	Art. 286 § 2	2	0	3	1	5	1
	Art. 286 § 3	174	134	335	257	172	106
	Art. 287 § 1	1 312	316	1 638	195	1 760	261
	Art. 287 § 1 in conjunction with Art. 294 § 1	2	1	2	2	7	0
	Art. 287 § 2	6	0	2	0	3	1
	Art. 310 § 1	117	19	90	16	59	16
	Art. 310 § 2	8	4	6	3	14	1
	Art. 310 § 4	5	5	2	2	3	2

* The behaviour of the offender in relation to victims: contact. Other features of behaviour: making unlawful modifications to computer data; on-site use of special computer software; connecting to the network of the internet service provider; masquerading as an existing website in order to obtain data in an unauthorised manner (phishing); breaching or bypassing the security of a computer server; breaking into a computer system (hacking); making threats over the internet or by phone.

** The data for 2015 refer to the period 1 January-30 September.

Table 2: Data from the Ministry of Justice

Type of offence/provision (Art. in the PC)	Number of people convicted	
Year	2013	2014
Art. 200a (1)	2	3
Art. 200a (2)	13	24
Art. 202 (1)	1	-
Art. 202 (3)	55	38
Art. 202 (4a)	82	79
Art. 202 (4b)	3	1
Art. 267 (1)	47	44
Art. 268a	22	18
Art. 269a	4	1
Art. 269b (1)	1	1
Art. 270 (1)	6 482*	5 920*
Art. 271 (1)	491*	359*
Art. 287 (1)	42	48
Art. 287 (2)	1	4

* Total number of people convicted for a given offence with no specific reference to computer-related offences

An analysis of the scale of the phenomenon of card fraud (most common offences in the area of electronic payment instruments) has been made on the basis of data obtained from the Police Electronic Reporting System (SESPol) for the period 2013-2014.

Table 3: Offences related to payment cards (cards referred to in proceedings) in 2013-2014*

Type of offence/event		Credit cards		Debit cards (including cards issued by stores and petrol stations)	
Period		2013	2014	2013	2014
Counterfeit cards	card fraud (white plastic)	221	226	23	31
	card processed	4	64	5	5
Cards	stolen cards	7 792	8 044	8 106	7 582
	lost cards	679	895	734	698
Internet transactions		912	1199	55	97
Undelivered cards		5	1	1	16
Transactions on the basis of applications using false data		74	22	15	7
Card scams	card skimming at ATM	496	375	362	3 835
	skimming	425	355	41	120
Other (offence not listed, e.g. card not present)		182	468	68	225

* From SESPol.

Table 4: Offences related to payment cards (cards referred to in proceedings) in 2015 (1 January-30 September)*

Type of offence/event		Credit cards	Debit cards (including cards issued by stores and petrol stations)
Period		2015	2015
Counterfeit cards	card fraud (white plastic)	8	23
	card processed	6	5
Cards	stolen cards	2 512	8 106
	lost cards	270	734
Internet transactions		221	55
Undelivered cards		1	1
Transactions on the basis of applications using false data		13	15
Card scams	card skimming at ATM	180	362
	skimming	174	41
Other (offence not listed, e.g. card not present)		70	68

* From SESPol.

Despite the statistics, the evaluators noted no exchange of structured data from the police to prosecutors, or to courts so as to allow the history of the case to be traced. As a result, there are substantial difficulties in keeping track of statistics on cybercrime from start to finish. Therefore, in the evaluators' view, sharing statistics among law enforcement agencies and judicial authorities could be of great value for a follow-up mechanism as well as prioritisation of goals in combating this phenomenon.

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

The prevention of and fight against cybercrime is considered a part of the general activities of the public prosecution service and criminal courts. According to Polish budgetary law, the expenditure of those services is not associated with particular types of crimes, but is covered from appropriate parts of the budgets of those services.

The budget expenses plan for the police units is worked out in accordance with the 2010 *Minister for Finance ordinance on detailed incomes, expenses, revenues and expenditures and the foreign funds classification*. In the process of planning the budget for 2015, funds for material expenses were divided on the basis of a decision by the commanders of 'Voivodeship' (regional) police headquarters (third degree budget funds administrators) according to the priorities and needs of the police units under their command. That means that the police budget does not contain funds dedicated specially to preventing and fighting cybercrime. The only financial means dedicated to this purpose are found in the expenses plan of the IT and Communication Bureau of the NPH, as it performs tasks related to the protection of cyberspace containing the police infrastructure.

In 2014 the IT and Communication Bureau of the NPH spent PLN 2 132 217 (EUR 488 984) for that purpose; the planned expenses in 2015 amounted to PLN 4 925 300 (EUR 1 129 526).
The implementation of anti-cybercrime projects is also funded by the European Union and the Norwegian Financial Mechanism. The financial resources are spent on training Polish officers in a range of aspects relating to the fight against computer crimes.

During consultations concerning the National Programme – Internal Security Fund 2014-2020, one of the proposals submitted during the needs assessment process was to replace the existing operational base (SIO) and to establish an electronic training base. The aim of this project is to facilitate the quick and competent functioning of a modern and failure-free police operational base by training professional staff, replacing access stations, servers and software, and improving information exchange between the services involved in preventing and fighting crime and terrorism, including cybercrime.

3.5 Conclusions

- *The National Cyber Security Strategy* has been in place in Poland since 2014 and aims to ensure the country's cyberspace safety, particularly as regards public ICT critical infrastructure considered essential for the functioning of public services, such as energy and healthcare, as well as private businesses, including the financial sector. However, it is fragmented and supplemented by two other documents: the *Cyberspace Protection Policy of the Republic of Poland*, which sets out the guidelines to be followed by public and law enforcement authorities; and *The Doctrine of Cybersecurity of the Republic of Poland*, which contains objectives for the safe functioning of the State as a whole in cyberspace.

- Poland has clearly defined its national priorities with regards to handling cybercrime and cyber security. The priorities cover cyber defence, cyber security, cybercrime, awareness and training. Moreover, the police priorities are clearly described and cover operational aspects, training needs, hardware and software improvement, awareness and safety.

- In the opinion of the evaluators, the strategy and the defined priorities developed in Poland provide a solid basis for fighting cybercrime. However, the range of different documents relating to cyber security seems to make it difficult for the Ministry of Digital Affairs to coordinate the implementation of the strategy because it does not have the necessary powers. Therefore, in the evaluators' view Poland lacks a coordinating body between the entities actually involved in fighting cybercrime, and one predominant document establishing national cybersecurity strategy at the central level.

- Moreover, despite the information provided by the Polish authorities, the evaluators did not find enough relevant information regarding the involvement of the judiciary (judges and prosecutors) in the setting up of the country's cyber security strategy. Therefore, taking into consideration the crucial role played by judges and prosecutors, a certain lack of proactivity from their side in listing their own priorities has been noted by the evaluators. In the evaluators' view this proactivity could raise their professional competences and effectiveness while tackling cybercrime.

- Regulation of the public-private partnership (including NGOs and CERTs), as well as critical infrastructure operators with a framework establishing duties and rules, could help information flow and management.

- As regards statistics, the General Statistics Office of the Republic of Poland is responsible for the collection and dissemination of the statistics. There are many sources for the collection of statistics related to cybercrime and cyber security but the main sources of statistics are the National Police Information System (NPIS) and CERT POLSKA.

- The NPIS records the numbers of crimes declared, crimes detected and criminal investigations initiated and completed. CERT POLSKA records the number of incidents reported to them by the public or discovered by the organisation. Due to the fact that there is no unique definition of cybercrime laid down in the legislation, it seems to be very difficult to account for all the incidents that fall within the scope of cybercrime. Moreover, it seems that there is an overlap in the way the NPIS and CERT POLSKA collect statistics and this is due to the fact that incidents reported to CERT POLSKA may be a part of the declared incidents in the NPIS records.

- Statistics related to cybercrime are low. If the Penal Code provided for cyber-related crime as a specific criminal offence, it seems that the law enforcement structures involved in fighting cyber issues could be made stronger. Some statistics are missing due to the fact that there is no distinction between crimes that are committed using electronic means and those that are not, e.g. between traditional fraud and forgery and/or computer-related fraud and forgery. Therefore, the evaluators have some doubts as to whether there is the same understanding of cybercrime amongst all stakeholders involved in countering cybercrime.

- Since the link between reported crimes, prosecutions and convictions cannot be traced, there are substantial difficulties in keeping track of statistics on cybercrime from start to finish. A part of the solution could be to establish common definitions among law enforcement and judicial authorities.

- There is no dedicated budget within the police and/or government for raising awareness related to cybercrime and cyber security. However, there are funds available within the general police budget for this purpose. Moreover, it was noticed that there is effective cooperation between NGOs and the governmental sector on applying for and granting European funds to raise awareness in the field of cybercrime and cyber security. All the grant applications are filtered by the Ministry of Digital Affairs before being submitted.

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecutions and courts)

4.1.1 Internal structure

Criminal investigations are carried out in Poland under the responsibility of prosecutors.
There are no specific structures devoted to prosecuting cybercrime within the public prosecution service nor designated courts dealing only with this type of case. On the other hand, such structures have been created at regional level in the police.

However, at the level of the Prosecutor General's Office several prosecutors have been designated to provide coordination and support to lower tiers of the public prosecution service in cases involving cyber attacks (attacks against computer systems), hate crimes, and the sexual exploitation of children. Moreover, at regional level coordinating prosecutors have been appointed to deal with cases of sexual exploitation of children. Those prosecutors closely cooperate with police officers, providing advice in the most complex cases.

In the evaluators' view, the clear specialisation of the police was not matched by their counterparts in the prosecution service.

After the on-site visit the evaluation team was informed that in April 2016 a specialised cybercrime unit was set up within the Department for the Economic Crime of the National Prosecution Office. Appointment of cybercrime coordinators in all Regional Prosecution Offices followed in May 2016.

4.1.2 Capacity and obstacles for successful prosecution

The main obstacles to the prosecution of cybercrimes mentioned by the Polish authorities are as follows:

- Domestically: a lack of sufficient resources (both human and technical) and restrictions on gathering data subject to banking confidentiality.
- Internationally: long and complex MLA procedures, differences between legal regimes (existence of cyber safe havens), servers located in countries where there is no Polish or EU jurisdiction, the complex legal situation concerning data retention in the EU and third countries (e.g. different data retention periods), the lack of a legal database of devices used for skimming, the long waiting period for international legal assistance and forum shopping.

Moreover, unregistered prepaid phone cards, difficulties in identifying anonymous network (Tor) users and the fact that there is no obligation for service providers to respond to law enforcement requests free of charge were listed as the main obstacles in detecting and combating cybercrime.[15]

[15] Some of the issues expressed at the time of the on-site visit as obstacles seem to be resolved. The Counter-Terrorism Act of 10 June 2016, adopted after the on-site visit, demands from the users of prepaid cards to register sim cards. Subscribers being party to a contract for the provision of telecommunications services, including prepaid services, are required to provide the service provider with their data. If the subscriber is a natural person he/she is obliged to provide at least a name and social security number if the subscriber has it, or the name, series and number of ID. In case of a foreigner who is not a citizen of a Member State or the Swiss Confederation he/she is obliged to provide the passport number or the number of a residence card. Subscriber who is not a natural person is obliged to give a name and identification number (REGON/NIP) or number in the National Court Register or in the business register or other relevant register. Service provider is able to provide telecommunications services only after the verification of the above mentioned data provided by subscriber. Registration of the prepaid cards reduces the anonymity of perpetrators of various crimes helps to prevent crimes. Moreover, according to the amendment to the Police Act and certain acts of 15 January 2016, obligation to free of charge answering to Police has been extended from telecommunications companies also to entrepreneurs providing electronically services.

There is also no legislation on the possibility of monitoring encrypted communication networks.[16]

Furthermore, based on the *Act on providing services by electronic means*, some internet service providers do not provide data requested by the police free of charge. Additionally, global companies such as Google or Facebook have their own specific procedures and cooperation with them is not subject to domestic law. These companies do decide to provide data in specific cases but those cases do not correspond to all crimes penalised under Polish law. There are no common international regulations in this field.

In order to strengthen the capacity of prosecutors and judges, the Polish authorities plan to increase the number of courses on cybercrime organised by the National School of Judiciary and Public Prosecution and to include this topic in other training fora (on evidence law, victims' rights, etc.).

4.2 Law enforcement authorities

Preliminary investigations are conducted by police entities based in the 'Voivodeship' (regional) police headquarters.

At the central level, the Department for Fighting against Cybercrime (25 police officers) has been established within the Criminal Service Bureau of the NPH. Its main tasks include:

1) coordinating and initiating police activities to identify criminal threats on the internet;
2) developing cooperation with public-sector, private and academic entities to determine how to collect and exchange information about crime in cyberspace;
3) conducting technical consultations and cooperating with domestic and foreign entities to identify and implement the most modern solutions in the fight against crime committed in cyberspace;

[16] The Polish authorities informed after the on-site visit that monitoring encrypted communication networks is based on the general rules of surveillance, but access to the data depends on the technical possibilities, which are still evolving.

4) deploying and maintaining dedicated IT systems to perform tasks such as monitoring the internet to detect offences or illegal content, detecting users of an anonymous network, providing remote access to dedicated cells set up under the command of the provincial (capital) police;
5) preparing opinions on and changes to legislation in the field of IT security;
6) organising in-service training for police officers under the responsibility of the department.

The specific structure for combating cybercrime was established in October 2014 in each 'Voivodeship' (regional) police headquarters. Currently, 19 units are operational in the Voivodeship police headquarters and Warsaw Metropolitan Police Headquarters (including the Central Investigation Bureau of the Police and Department for Fighting against Cybercrime in the Criminal Bureau of NPH), with a total of 240 permanent staff members. These units are being continuously equipped with hardware and trained to improve the qualifications of the police officers. Their main tasks are: operational police work, forensics, international cooperation either directly or through the International Police Cooperation Bureau, cooperation with ICP, ICT, coordination tasks and implementation of new tools.

Within this structure, the Department for Fighting against Cybercrime is also the 24/7 contact point for police officers and citizens, and can be contacted by email or phone to pass on information about any kind of incident connected with the internet, computers, and other relevant issues. In the case of international requests, the International Cooperation Bureau of the NPH is mainly responsible for coordinating the tasks.

The Division of Fighting against Cybercrime (15 staff) has also been established within the Central Criminal Investigation Bureau of the Police. Their main task is to combat cybercrimes committed by organised criminal groups. The Cyber Division is equipped with a highly advanced laboratory that offers a wide variety of tools and solutions, including a Laminar Flow Cabinet (for safe data extraction from damaged electronic data carriers) and hardware for cracking passwords on encrypted files.

The Cyber Division consistently offers its support to the cybercrime units of the Voivodeship police headquarters as well as the Department for Fighting against Cybercrime of the National Police Headquarters.

Additionally, crimes such as paedophilia, the sexual exploitation of children and child pornography, as well as credit card crimes, are dealt with by different units within the NPH (Criminal Service Bureau)and Voivodeship (regional) police headquarters.

There are special units in the Communication and IT Bureau of the NPH that focus on cyber attack and cyberspace. There is also a special position in the field of cyberspace security: the *plenipotentiary for cyberspace security*, who mainly deals with the coordination of activities within the infrastructure of the police network according to Decision No 415/2014 of the National Police Headquarters.

The police cooperate with the Internal Security Agency and the Military Counterintelligence Service in the field of operational work. Additionally, the Border Guard cooperates with the police and other institutions in order to prevent and combat cybercrime.

The police also conduct ongoing monitoring of the internet, with particular emphasis on criminogenic areas, and undertake initiatives to improve the awareness and safety of internet users. The police also cooperate with telecom operators, internet service providers, research institutions and experts in the field of combating cybercrime from other countries. Moreover, the Department for Fighting against Cybercrime cooperates at national and international level with state institutions and the private and public sector to obtain information on the methods and forms of crimes committed in cyberspace.

4.3 Other authorities/institutions/public-private partnership

Poland has a decentralised system for protecting cyberspace. Competences related to security in cyberspace are divided between, among others, the Ministry of Digital Affairs, the Ministry of the Interior, the Ministry of National Defence, the Ministry of Justice, the Government Centre for Security, the Polish Office of Electronic Communications, the Inspector General for Personal Data Protection, the Ministry of Development, the Ministry of Foreign Affairs, the Internal Security Agency, the police, the Foreign Intelligence Agency, the Military Counterintelligence Service and the National Bank of Poland, as well as CERT POLSKA, which is part of the structure of the Polish Research and Academic Computer Network (NASK).

In addition, Poland has public and private teams for responding to computer incidents (CSIRTs) covering, among other things, the government administration, the military administration and the police, as well as teams established by telecommunications operators and the scientific and research communities. The above institutions work on tasks relating to cyber security, the prevention of cybercrime, and cyber defence.

Ministry of Digital Affairs (MDA)

The *MDA* is responsible for:

- the political and strategic coordination of cyberspace for cybersecurity in Poland;
- the provision of minimum ICT security requirements in the public administration
- the provision of minimum requirements for public registers and the exchange of electronic information, as well as minimum requirements for ICT systems (based on the 2005 Act on the computerisation of activities of entities performing public tasks as well as the 2012 Regulation of the Council of Ministers on the national interoperability frameworks);

- supervision of the Office of Electronic Communications, to which telecommunication operators report the most important cyber incidents on telecommunication networks (according to the 2004 Act on telecommunications law);
- supervision of NASK as the research institute and operator for data transmission networks and National Cybersecurity Centre, which is part of the institute.

Internal Security Agency (ISA)

The *ISA*'s activities in relation to threats in cyberspace focus on:

– coordination in responding to incidents threatening the security of ICT systems or networks used by state bodies (task of CERT.GOV.PL);
– developing public administration capabilities to protect ICT resources;
– supervising an early warning system for hazards on the public administration networks (ARAKIS-GOV);
– combating cyber-terrorism (unlawful attacks or the threat of an attack on computers, networks or information systems as a result of the activities of terrorist groups or foreign intelligence services).

The Governmental Computer Security Incident Response Team (CERT.GOV.PL)

Established on 1 February 2008 within the ISA, *CERT.GOV.PL* ensures and develops the capability of public administration units to protect themselves against cyber threats, in particular attacks against infrastructure involving IT systems and networks the destruction or disruption of which may considerably threaten the lives and health of people, national heritage or the environment, or lead to considerable financial loss or disturb the operations of the public authorities. In accordance with the *Policy*, CERT.GOV.PL plays the main CERT role in the area of government administration. It publishes annual reports on the state of cyber security of Poland.

CERTs

There is no single computer security incident response team, but many CERTs dealing with the issue broadly defined as ICT security. Apart from CERT.GOV.PL, there is also a Departmental Management Centre for Security Services and Networks within the Ministry of National Defence committed to the prevention of incidents that could affect the defence of Poland and the teams set up by the telecommunications environment, including CERT OPL and PIONIERCERT, as well as CERT POLSKA (CERT.pl), which functioned at the time of the on-site visit within the framework of the Research and Academic Computer Network (NASK).[17] In parallel, the Departmental Security Management Centre for Networks and ICT Services plays a similar role within the military.

NASK

NASK is a research institute and data transmission network operator used to be supervised by the Ministry of Science and Higher Education. According to the new regulation adopted by the Council of Ministers, NASK has been supervised by the Ministry of Digital Affairs since 1 January 2016. The aim of the research conducted by NASK is to develop solutions that increase the efficiency, reliability and security of IT networks. NASK also conducts activities related to increasing internet security and responding to incidents that infringe network security. CERT POLSKA is responsible for this, and another team – Dyżurnet.pl – adopts reports concerning illegal matters on the internet and forwards them to the police. NASK offers innovative IT solutions for business customers, government and science. CERT POLSKA was established in 1997 as the first CERT team in the country. CERT POLSKA operates within the structure of NASK, the national top level domain registrar. CERT POLSKA *de facto* performs the role of a national CERT (and as such is listed in ENISA documents).

[17] After the on-site visit the evaluation team was informed that the National Cyber Security Centre (NC Cyber) was established within the framework of the Research and Academic Computer Network (NASK), part of which is CERT.POLSKA. The main task of NC Cyber is to collect information about incidents from critical sectors and cooperate with Police Department in the field of cybercrime.

The police carry out scientific projects in cooperation with the private sector (researchers in the field of the implementation of the software and tools to combat cybercrime at AGH University of Science and Technical University of Warsaw Poland Homeland Security Platform. Examples of police cooperation with the private sector:

- The Police Academy in Szczytno is a member of a consortium in an FP7 project: Comprehensive approach to cyber roadmap coordination and development (CAMINO) – 2014-2016 O ROB 0003 03 001
- Police officers were members of the consortium in the CIPS/ISEC project: Creation of a Polish Centre of Excellence for Research on Cybercrime - 2013-2014 HOME / 2012 / ISEC / INT / 4000003858.

Within the framework of cooperation with the private sector responsible for security in the newly established programming devices, it is planned for the police force to take part in the creation of new technologies for the financial sector. Checks to ensure that IT solutions are crime-proof will be carried out in conjunction with the PBA.
It is also worth mentioning the cooperation with the Polish Bank Association (PBA) and with the Nobody's Children Foundation (please refer to chapters 6.2.3, 6.3.2 and 8.2).

4.4 Cooperation and coordination at national level

4.4.1 Legal or policy obligations

On the basis of *The Cyberspace Protection Policy of the Republic of Poland*, the Minister of Digital Affairs, on behalf of the Council of Ministers, serves as a coordinator for the protection of cyberspace for government administration offices at the strategic and political level. An Action Plan on cyberspace security in Poland was agreed and adopted by the Governmental Committee for Digitalisation on 13 April 2015. The Action Plan is currently being implemented and contains

recommendations regarding cyberspace security for the entire governmental administration. The strategic objective of the *Policy* is to achieve an acceptable level of safety in cyberspace. It should be clarified that the term 'acceptable' is used in the sense of risk management standards, because the *Policy* is based on this approach. The actions and measures to be taken in order to achieve this goal are the result of cyber security risk evaluations carried out by relevant public bodies.

The main task of Governmental Computer Security Incident Response Team (CERT.GOV.PL), which is as a part of Internal Security Agency, is to perform operational tasks related the security of information systems of public bodies. Its chief task is to ensure and develop the capability of public administrative bodies to protect themselves against cyber threats, in particular against attacks aimed at the ICT infrastructure. The CERT.GOV.PL mainly manages cyber incidents within the public sector and its actions include coordination of the incident response process, resolving and analysing incidents, and coordination of responses to security breaches. In the case of incidents that are wide-ranging in their effects or action, the team coordinates and responds to the incident and also exchanges the information with the institutions directly affected by the cyber attack. Moreover, the team uses experience gained from previous incidents, prepares warnings with technical information and prepares recommendations regarding further action and transfer it to the government administration units. This is a process that aim avoiding/reducing possibility of appearing similar attacks on other institutions.

Utmost importance is attached to CERT POLSKA, whose tasks include responding to threats and incidents in the Polish Internet domain (.pl), publishing annual reports about cyber threats and creating tools and information systems to increase the country's cybersecurity potential, e.g. an early warning system, and a knowledge and information exchange platform known as ARAKIS.

In 2015, on the basis of Commander-in-Chief of the Police's decision, a team to respond to Computer Incidents (POL-CERT) was based at the NPH.

The Team performs the tasks associated with the coordination of the process of response to computer incidents in police teleinformatic systems and networks. In order to streamline the flow of information about events in the Voivodeship (regional) Police Headquarters as well as police in colleges, contact points dealing with cyber issues were established. In future team that responds to computer incidents POL-CERT will constitute the element of the Polish system of reacting to computer incidents in cyberspace.

4.4.2 Resources allocated to improve cooperation

At the moment the Polish police are in the process of equipping newly created units for combating cybercrime. It is intended to create modern tools which will improve the work and which will help to identify cybercrime offences committed in the new medium - the Internet. Units combating cybercrimes have specialised software and tools which make it possible to disclose and secure electronic evidence.

The hardware and software used in the fight against cybercrime, in particular in the field of computer forensics, are among the licensed tools used by law enforcement agencies around the world. In 2016 it was planned to build a hardware platform for the study of malware, which significantly accelerate police action in investigating this type of crime and make it more effective.

4.5 Conclusions

- The Ministry of Justice is responsible for the administration of prosecution and judiciary. There are no dedicated judges who deal exclusively with cybercrime cases. However, in practical terms, judges who are familiar with cybercrime issues are usually appointed to deal with this kind of case, at least the serious ones.

- At the prosecution level, there are no specialised units to deal with cybercrime. However, at the Prosecutor General's Office, a group of designated prosecutors was set up. Its mission is to co-ordinate and support investigations carried out at the regional level involving cybercrime, hate crimes and the sexual abuse of children. After the on-site visit the evaluation team was informed that in April 2016 a specialised cybercrime unit was set up within the Department for the Economic Crime of the National Prosecution Office. Appointment of cybercrime coordinators in all Regional Prosecution Offices followed in May 2016.

- The police effectively come under the Ministry of the Interior and give the impression of being a well-structured organisation with a clear mandate and clear responsibilities. There is a specialised unit within the National Police Headquarters, the Department for Fighting against Cybercrime, dealing with child pornographic material, cyber-attacks and online fraud cases. This Department consists of 25 well trained officers whose responsibilities include monitoring and advising the regional police investigators who deal with cybercrime cases. The Department for Fighting against Cybercrime provides support to cybercrime units at the Voivodeship/regional level of the police.

- In addition, at the regional level (Voivodeships) specialised units for fighting cybercrime were established with an average number of 10 officers per unit. This creates the capacity for investigations to be conducted into crimes such as paedophilia, the sexual exploitation of children and child pornography by different units: at the central level by the Central Criminal Investigation Bureau or at the regional level by the Voivodeship Police Headquarters. When necessary, the Polish police cooperate operationally with the Internal Security Agency and the Military Counterintelligence Service. The internal structure of the police and the designation of specialised police officers to deal with cybercrime cases seem to be examples of best practice.

- Moreover, at the Police Headquarters level there is a dedicated team consisting of 15 well trained officers, the Central Criminal Investigation Bureau of the Police, who are responsible at operational level for assisting the investigation with their expertise in the field of computer forensics and live data investigation and forensics.

- Since preliminary investigations are conducted by the police, the whole existing structure for fighting cybercrime is based on the police's technical and human resources. This fact, combined with the lack of technical capacity and appropriate training for judges and prosecutors, raises the question of whether the scrutiny of judges and prosecutors over the police investigations is effective and consistent. Therefore, in the evaluators' view, there is a need for specialised prosecutors with knowledge of cybercrime at the regional level to support colleagues at the district level in conducting or supervising investigations. Moreover, training for prosecutors should be put in place and courses should be attended on a regular and mandatory basis.

- A number of other authorities and organisations take part in the prevention of and fight against cybercrime. The interaction and cooperation between public and private sectors in Poland seems to be effective and productive. NASK and the Bank Cybersecurity Centre (set up by the Polish Bank Association) provide good examples of collaboration between public administration and civil society.

- On the other hand, it was noticed at the time of the on-site visit that there was no national CERT acting as a central point of coordination, cooperation, information sharing and statistical registration of cyber security incidents. The main CERTs in the Republic of Poland are: CERT.GOV.PL, which is responsible for the government's ICT and CERT POLSKA, operated by NASK, which functions as an academic entity; POL-CERT is for the police, MIL-CERT is for the military, and for entities such as Alior Bank with CSIRT. In the evaluators' view, the current structure gives the impression that there is a need for the creation of a single point of contact. Therefore, appointing a national CERT with coordinating powers for other CERTs could strengthen the resilience of the Polish cyber security system.[18]

- The protection of cyberspace is taken seriously by Polish administrative and governmental authorities. However, this very decentralised approach (several different entities are involved in this matter, from a few ministries to the Military Counterintelligence Service, from the National Bank of Poland to NASK), may result in a certain lack of co-ordination. Therefore, in the evaluators' view, coordination of the various authorities involved in the fight against cybercrime should be enhanced. As a consequence, designating one body with the powers to give instructions to the authorities in charge of cybersecurity and carrying them out could be of great value.

[18] After the on-site visit the evaluation team was informed that NC Cyber and its part CERT POLSKA is acting as a national CERT – central point of coordination, cooperation, information sharing and statistical registration. In a new cybersecurity law, which is currently under preparation, NC Cyber is expected to be designated as the national CERT.

- On the other hand, annual reports prepared by NASK and the Internal Security Agency (CERT.GOV.PL) paint a clear picture of the cyber situation in Poland. They cover the overall situation in Poland pertaining to the public administration and the private sector as well as incidents affecting citizens. In the evaluators' view, it is advisable to measure the progress of cyber criminality based on diversified resources exercised by governmental and non-governmental bodies such as carried out on an annual basis in Poland.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on Cybercrime

Poland is a party to Council of Europe's Convention on Cybercrime, which entered into force on 1st of June 2015.

5.1.2 Description of national legislation

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

Poland has transposed Council Framework Decision 2005/222/JHA on attacks against information systems as well as Directive 2013/40/EU on attacks against information systems. The Polish authorities reported that since all requirements of this Directive were fulfilled by the existing provisions of the Polish law its transposition did not cause difficulties.

There is extensive legislation in place in Polish law regarding cybercrime[19]. The following acts are criminalised in the Polish Penal Code (PC): illegal access to information systems (Article 267), illegal system interference (Article 269a), illegal data interference (Article 268a), illegal interception of computer data (Article 267), misuse of devices (Article 269b), computer -related forgery (Articles 270 and 271), fraud (Article 287), computer-related identity offences (falls under the definition of forgery or fraud), sending or controlling the sending of spam (Act on services provided through ICTs). There is no definition of cybercrime in the Penal Code.

[19] Due to the large number of pages involved, its description has not been included in the report. For more information see Annex D.

The Penal Code (PC) does not provide any catalogue of aggravating or mitigating circumstances influencing the court's decision. However, certain provisions of the Code indicate circumstances which the court must take into consideration while assessing the social harm caused by the offence committed, deciding upon the guilt of the offender and imposing a penalty. Furthermore, it should be noted that the general rules set out in Article 53 of the Penal Code (directives for imposing penalties) apply to all criminal offences.

The law stipulates that an attempt to commit these offences is also punishable. Incitement and aiding and abetting are also criminalised under the Polish law.

The level of social harm associated with an offence is based inter alia on the results and on the way in which the offence was committed. Minor character of an offence will result in lesser judgment.

Legal entities can be held liable for the offences set out in Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography and Directive 2013/40/EU on attacks against information systems, as well as in the Convention on cybercrime. Regulations regarding this liability are provided in the 2002 *Act on liability of collective entities for criminal offences subject to penalties*. This Act lays down rules of liability of collective entities for criminal offences, and sets out a catalogue of those offences (that includes all of the offences related to the provisions of the Budapest Convention) and sanctions imposed on legal entities.

Pursuant to Articles 7 and 9 of the above -mentioned Act, with respect to the collective entity, the court might impose a fine of PLN 1000 to 5 000 000 (EUR 250-1 250 000), but not higher than 3% of the revenue in the financial year in which the offence was committed resulting in the liability of the collective entity and application of other measures explicitly mentioned therein.

There are several criminal offences and minor offences related to cybercrime (or use of ICT) defined in various acts. The most important are:

- regarding personal data*: Act on the protection of personal data,* which sets out the definitions of several offences related to the gathering and processing of personal data, including the sanctions that may be imposed if proper security measures are lacking (recklessness in personal data management),
- regarding SPAM: *Act on providing services by electronic means*, which in Article 24(1) provides for a fine to be imposed in cases where electronic communications are used for direct marketing without the consent of the subscriber.

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

Poland has transposed in full Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography into national law and has ratified the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the so-called Lanzarote Convention). Poland has extensive legislation in place regarding, inter alia, computer-related production, distribution or possession of child pornography (Article 202) and computer-related solicitation ("grooming')' of children[20].

C. Online card fraud

In Polish law there are countermeasures against any fraudulent financial operations made online. The conduct described as "computer-related forgery" falls under the definition of forgery set out in Article 270(1) of the Penal Code (material forgery) and Article 271(1) (intellectual forgery).

[20] Due to the large number of pages involved, its description has not been included in the report. For more information see Annex D.

Article 270(1) provides that any person who forges, counterfeits or alters a document with the intention of using it as authentic, or who uses such a document as authentic, is liable to a fine, a restriction of liberty or imprisonment for between three months to five years.

Article 271(1) lays down that a public official, or another person authorised to issue a document, who certifies an untruth therein, in circumstances of legal significance, is liable to imprisonment for between three months and five years

This offences may be committed intentionally (a direct intent – the aim to use a forged document as if it was authentic – is required under Article 270 (1) of the Penal Code). Attempt to commit the aforementioned offences is punishable. The term "document" (used in Articles 270 and 271 of the Code) is defined in Art. 115 (14) as an object or record on a computer data carrier to which is attached a specified right, or which, in connection with the subject of its content, constitutes evidence of a right, a legal relationship or a circumstance that may have legal significance.

Article 287(1) of the Penal Code states that a person who, in order to gain material benefits, affects automatic the processing or transmitting information, or changes or deletes a record or introduces a new record on an electronic information carrier without being authorised to do so, is subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years. This offence may only be committed intentionally (a direct intent – the aim of gaining material benefits is required). The conducts described as "computer-related identity offences" fall under the definition of forgery or fraud.

5.2 Procedural issues

5.2.1 Investigative Techniques

Searching for, and collecting data from the information system/computer

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

The search, collection and preservation of electronic data is performed on the basis of general provisions of the Code of Criminal Procedure (CCP) regarding collection and preservation of evidence.

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

Real-time interception/collection of the content of the communication (regardless of its of its nature: telephone talk, e-mail, sms or other) is possible, but is considered a special investigative technique, and therefore requires a court order. Only in urgent cases (when there is a risk that evidence will be lost) may the Police take such action, and at the same time they must request a court's authorisation. Evidence gathered without such an authorisation cannot be used in criminal proceedings and must be destroyed.

The above restrictions do not apply to actions related to traffic data. Under Article 218 of the CCP, the public prosecutor or the court is entitled to obtain traffic data from telecommunications and transport companies. This includes the so - called billings (lists of connections, their time and duration) as well as information about the location of a telecommunications device.

Preservation of computer data

During the criminal proceedings, the data secured during the investigation are kept until the court proceedings conclude. The data can be stored on their original carriers (computer discs) or (what is most common) a digital/forensic copy of the data can be made.

Order for stored traffic/content data

Pursuant to Article 218a of the CCP the public prosecutor or a court may order any telecommunication services provider to store (preserve) all data regarding services provided, including content data. The preservation period must not exceed 90 days.

Cybercrime investigations are conducted according to the same procedure as with other crimes. Pursuant to Article 236a of the CCP the provisions on stop and search apply accordingly to the holder and the user of equipment containing computer data or computer system, in terms of the data stored in the device or system, or in the media at his disposal or use, in particular in correspondence sent via email.

Due to the dynamic development of methods, techniques and tools for committing cybercrime it is difficult to create a catalogue of good practices in the area of investigative techniques. All activities carried out by the police officers are based on their own experience and exchange of information. Another source of information is the training organised for the officers of the "cyber" department e.g. by the Police Academy in Szczytno. The course specialises in training officers how to obtain information from the internet to enable them to combat computer crime. There is also a specialist course for police officers performing tasks related to the fight against cybercrime. Another source of "good practices" is the training in computer forensics offered by companies distributing specialized equipment for protection, data acquisition and analysis. Subsequently, under the European Police Exchange Programmes organised by the European Police College (CEPOL)

officers have the opportunity to enrich and exchange their experience of the methods, techniques and tools needed to fight cybercrime effectively. Meetings of contact points within the EC3 provide an opportunity to discuss common issues and improve the exchange of information. In addition, within the framework of interaction with the public and private sectors in the exchange of information police officers gain experience and knowledge regarding new techniques used cybercrime perpetrators.

Additionally, a brochure aimed at police cybercrime units with information on good practices when it comes to properly securing the electronic evidence, has been released by the Department for Fighting against Cybercrime.

The Prosecutor General prepared the methodology for the prosecution of hate crimes, paedophilia and child pornography, which also covers its cyber aspect.

5.2.2 Forensics and Encryption

The CCP does not cover the concepts such as "electronic or remote expertise inquiry". However, Article 193(1) of the CCP stipulates as follows: "If the determination of material facts having an essential bearing upon there solution of the case requires some special knowledge, the court shall consult an expert or experts".

Military

The Ministry of National Defence (MND) considers encrypted network communication (and the problem of monitoring such communication) and encrypted devices to be a problem. It stated that as regards encrypted network communication, there is a need for proxies that can decrypt and re-encrypt the traffic in order to analyse it to detect possible threats (this approach requires appropriate legal regulations and strong justification).

MND claims there are no significant problems with cooperation in this area. The National Cryptology Centre was established in 2013. Decryption is not carried out in cooperation with private companies. Moreover, the digital forensics of encrypted devices was highlighted as the area in which it has not yet been possible to deal with the problem of encryption effectively. Traffic filtering and user awareness improvement have been implemented in the Internet access network.

Police

The Central Forensic Laboratory of the Police has the task of examining encrypted digital devices in the form of hard disk drives and volumes recovered from the memory of seized digital devices. During these examinations the IT experts attempt to break the cryptographic protection using special software running on the computer cluster consisting of computers available in the Central Laboratory's IT Unit. Currently, the biggest problem in cryptography relates to the limited possibility (too little processing power) to break cryptographic protection in cases when the perpetrators use long and complicated passwords.

5.2.3 e-Evidence

Terms such as computer data, information/computer system/network are used in various provisions of Polish criminal law, including in definitions of criminal offences. However, no legal definitions of the above-mentioned terms are provided, nor is there a definition of electronic evidence. This results from a tradition of defining in law only those terms that have a meaning other than that in natural language.

Although there is no legal definition of e-evidence in Polish law at the moment, it is understood by practitioners as information stored on electronic media. Defined thus electronic evidence is admissible in a criminal trial and subject to the opinion of the court like any other evidence, i.e. on the principle of free assessment of evidence. The procedure with e-evidence is the same as that for other forensic evidence.

As a general rule, Article 7 of Penal Code provides that the authorities in charge of the proceedings (prosecutors, courts) form their convictions on the basis of evidence gathered and appraised at their own discretion, with due consideration given to the principles of sound reasoning and life experience (principle of free appraisal of evidence.). Moreover, Article168a of the CCP provides that evidence acquired in an unlawful way (by the commission of an offence) is not admissible (gathered, used or taken into consideration by prosecutors or courts).

Those principles apply also to e-evidence (while there are no admissibility rules that would apply specifically to this type of evidence), as they do to evidence gathered outside Poland (by means of legal assistance).

Polish law takes a fairly broad and flexible approach to evidence gathered outside Poland. Article 587 of the CCP provides that such evidence (all reports from hearings, interrogations, and examinations of accused persons, witnesses or experts made at the request of a Polish court or public prosecutor, or reports based on other evidentiary procedures carried out by the courts or public prosecutors of foreign states or authorities acting under their supervision) may be presented (used) at the trial. Such evidence must be dismissed if the manner of conducting the procedure (obtaining the evidence) was contrary to the principles of Polish legal system. However, in line with the case law of the Polish Supreme Court, the mere fact that the procedural safeguards (that apply to gathering of some types of e-evidence) in Poland are stricter does not *per se* lead to dismissal of such evidence.

The Central Forensic Laboratory of the Police, whose duties include the examination of computer hardware and analysis of the data saved on various digital devices (such as hard disk drives, USB Flash Drives, DVDs etc.). The forensic IT experts recover/disclose only those data that are indicated in the request for examination.

5.3 Protection of Human Rights/Fundamental Freedoms

Fundamental rights and liberties are protected by the Polish legal order for both the offline and online world. They are provided for in the following legal acts:

a) *The Constitution of the Republic of Poland* that guarantees the right to privacy, the protection of personal data, freedom of expression, as well as the right of all citizens to search for and share information. The Polish Constitution also contains guarantees governing the observance of civil rights and liberties while conducting criminal procedures, including those in the area of cybercrime.

b) The 1997 Act on the protection of personal data[21], which contains quite rigorous regulations indicating when and how personal data may be processed. Article 8 of that act, provides for appointment of an Inspector General for Personal Data Protection with responsibility for, inter alia, issuing administrative decisions and handling complaints with regard to the enforcement provisions on the protection of personal data and keeping a register of data sets. The Inspector General also gives his opinion on legal acts concerning the protection of personal data.

c) The Telecommunications Act, which deals with the protection of privacy in the context of cybercrime, along with acts regulating the activities of particular services. They determine which bodies may access the personal data of subscribers processed by telecommunication service providers and how such access is to be obtained.

[21] Official Journal from 2014, No 1182 t. as amended.

d) The 2002 Act on providing services by electronic means[22] that followed Directive 2000/31/EC and introduced the protection of what are known as Internet intermediaries against legal responsibility for content generated, exchanged and posted on the Internet by users. The exclusions of liability make it possible to provide such electronic services that allow the users to freely express their thoughts and opinions on the Internet and, at the same time, the notice and takedown procedure makes it possible to efficiently remove content violating the general law as it applies to the Internet.

Moreover, all public authorities (such as the police, prosecutors and judges) must act on the basis of, and within the limits of, the law. Therefore, any actions on the part of public authorities which may interfere with constitutionally guaranteed rights and freedoms require explicit a legal basis in an Act of Parliament.

The right to privacy, the protection of personal data and freedom of expression are considered constitutional rights and freedoms. Therefore, restrictions on them can only be imposed when necessary: they must not violate their essence, and they must take the form of an Act of Parliament.
It is considered appropriate to entrust the prevention and investigation of crimes, as well as the prosecution of perpetrators, to certain state services with special powers/investigative techniques. The grounds for using such techniques are the severity of the crime and the need for action (when there are no other less intrusive measures). The use of special investigative techniques remains under the supervision of the courts.

[22] Official Journal 2013.1422 consolidated text.

The Act on the Police sets out the basic tasks of the police, which include:

- protection of lives and health of people and property against unlawful attacks;
- criminal prevention and cooperation in this field with state agencies, local governments and social organizations;
- detection of offences and prosecution of their perpetrators;
- collection, processing and transmission of criminal information;

In order to carry out its statutory tasks the Police is allowed, inter alia, to:

- use the personal data, including in electronic form, obtained by other bodies, departments and state institutions in conducting operational intelligence, and process them within the meaning of the Act on the protection of personal data, without the knowledge or consent of the data subject;
- search persons and premises in the manner and cases referred to in the Code of Criminal Procedure (CCP) and other laws; perform a personal inspection, inspect the contents of luggage and cargo in ports and stations as well as on forms of land, air and water transport where there is a justified suspicion of a criminal offence;
- conduct surveillance of and record events taking place in public, and (when acting within the framework of its operational and administrative activities) and the sound accompanying such events.

In certain cases (serious crimes, which include cyber sabotage), if other measures have proved ineffective or are unsuitable, the police may use a special investigative tools including operational control and communication interception. Use of these techniques requires a district court order, delivered at the written request of the Commander-in-Chief of the Police, made after obtaining the written consent of the Prosecutor General, or at the written request of the commander of the provincial police, with the written consent of the district prosecutor. In urgent cases, when evidence may be lost, a court order may be issued ex post, but not longer than 5 days after the operational control or communication interception was started.

The *Public Prosecution Act* and the CCP determine the competences and duties of the prosecution service, including supervision of preparatory proceedings in criminal matters and of the legality of initiating and carrying out operational activities by law enforcement to the extent provided in the statutes governing the organisation of these bodies and the scope of their activities. It should be noted that every request to use operational control and communication interception requires the consent of the relevant prosecutor.

5.4 Jurisdiction

5.4.1 Principles applying to the investigation of cybercrime

Rules on jurisdiction in criminal matters are set out in Article 5 and Articles 109-113 of the Penal Code. Those provisions apply to offences defined in the Penal Code itself, as well as to any other criminal offences defined by Polish law. Polish criminal jurisdiction applies to every offender (regardless of his/her nationality) who commits a prohibited act in Poland, or on a Polish vessel or aircraft, unless Poland is party to an international agreement stating otherwise (Article 5 of the PC). Under Article 111 of the Penal Code, jurisdiction over offences committed outside Polish territory is subject to the condition of dual criminality. However, that limitation does not apply to offences:

- specified in Article 112 of the Penal Code (an offence against: the internal or external security of the Poland; Polish offices or public officials, Poland's material economic interests, the offence of false testimony made before a Polish office, or an offence from which a material benefit was gained, even if indirectly, in Poland);
- laid down in the international agreements to which Poland is a party.

Since Poland is the party to the Convention on Cybercrime, the Additional Protocol thereto and the Lanzarote Convention, the requirement of dual criminality does not apply to offences which are defined therein and which correspond to the offences laid down in EU legislation concerning cybercrime.

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

The Polish authorities have not dealt with any cases which would involve conflicts of jurisdiction. However, there have been a number of cases in which foreign nationals were identified as perpetrators of cybercrime acts.

Polish substantive and procedural law contain rules on the personal and territorial application of Polish criminal law and legal instruments for international cooperation, including the transfer of proceedings, extradition and surrender, that are fully in line with applicable European regulations, specifically Framework Decision 2009/948/JHA of 30 November 2009 on the prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings. Therefore, any conflicts of jurisdiction could be resolved in accordance with national legislation and the rights of the authorities of the other Member States.

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

Polish authorities have not so far experienced problems related to the manner in which data are stored in what is termed “cloud computing”. However, according to the Polish authorities, this phenomenon may lead to serious problems in the future as cloud solutions are becoming more popular, resulting in more data important for the investigation of criminal offences being stored outside Polish and other EU Member State jurisdiction.

It should be mentioned that most of the procedures used to acquire such data are lengthy and inefficient, one factor being that key providers are located outside EU.

5.4.4 Polish perceptions with regard to the legal framework to combat cybercrime

Having signed the Convention on Cybercrime, the Additional Protocol thereto, and the Lanzarote Convention, Poland harmonised its national legislation in relation to both core cybercrime and offences that are often committed with the use of ICTs. However, national laws of the EU Member States still vary, as do those of non-member states.

In the opinion of the Polish authorities, the efficient investigation of cybercrime and the identification of offenders depend on the availability of data kept by mobile service providers and internet service providers (especially traffic and subscriber data). There is a need for European legislation that specifies in greater detail what data is defined as traffic, user, and personal (IP address, username, password, etc.) data. There is also a room for some regulation with regard to cooperation with third-countries, with a particular focus on those where the most important ICT companies have their headquarters.

5.5 Conclusions

- Poland is a party to the Council of Europe Convention on Cybercrime that entered into force on 1 July 2015. Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems were also transposed into Polish law.

- Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and the sexual exploitation of children and child pornography has been fully implemented.

- General rules on the prerequisites for punishment and on the elements of a criminal act (intent, recklessness, attempt, etc.), as well as liability (including incitement and aiding and abetting), are laid down in the Polish Penal Code and are applicable to cybercrime. However, as in other Member States Poland does not have a unique definition of cybercrime. In the evaluators' view, this lack of a unique definition may lead to unclear statistical registration and representation of cybercrime.

- Legal entities can be held liable for all the offences related to the provisions of the Budapest Convention and for the offences set out in EU Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and Directive 2013/40/EU on attacks against information systems.

- In relation to investigative techniques, there are a number of possibilities like special operations, monitoring and wiretapping that seem to be effective for the investigation of cybercrime. From a procedural point of view, Polish law allows for the most important investigative techniques and measures specific to this area of criminality. However, remote search and seizure is not provided for by Polish law e.g. in the case of LEA hacking online of a suspected computer instead of physically obtaining. In the evaluators' view, legislation permitting such an operation could be considered, notwithstanding the rights of a suspect.

- The ruling of the European Court of Justice invalidating the Data Retention Directive (Directive 2006/24/EC) affected some provisions of the Telecommunication Law which had to be amended. The public prosecutor or judge may order telecommunication services providers to preserve data relating to the services provided, including content data. The preservation period must not exceed 90 days.

- There are no specific rules regarding admissibility and assessment of e-evidence. E-evidence, like most traditional evidence, is admissible in court and is evaluated by the judge in accordance with the principle of free assessment of evidence. No difficulties or problems were mentioned regarding e-evidence obtained abroad.

- The Polish authorities reported difficulties with encrypted communications, encrypted storage devices and cloud -based hosting. However, there is a dedicated forensic laboratory within the Central Criminal Investigation Bureau which has an advanced decryption capability. Cloud hosting and storage is mostly a legal issue of jurisdiction and ownership.

- Moreover, the Police Central Forensic Laboratory is equipped with advanced material containing a wide variety of tools and solutions, including safe data extraction from damaged electronic data carriers or hardware specifically set for cracking encrypted files or devices. In the opinion of the evaluators, the expertise of the Police Central Forensic Laboratory could be shared with the other police field offices in the national territory, improving the skills of the officer and guaranteeing a first response in emergencies or where swift analysis is required in urgent cases or investigations.

- The principle of territoriality is the main rule for establishing Polish jurisdiction over a criminal offence. Polish law is applicable to crimes committed in Poland (and on board Polish maritime vessels and aircraft). For offences committed outside Polish territory, jurisdiction is subject to the condition of dual criminality, unless the vital interests of the country are at stake or it emerges from obligations laid down in international instruments. Since Poland is a party to Council of Europe Convention on Cybercrime, to its Additional Protocol, and to the Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, the requirement of dual criminality does not apply to offences in these areas.

- In the evaluators' view conflicts of jurisdiction are a problem of great relevance in most advanced cybercrime cases. Poland seems to address and handle these problems in a pragmatic way. Eurojust should be used in this case to solve the problem. However, the Polish authorities have not dealt, so far, with any cases which would involve conflicts of jurisdiction regarding cybercrime as, for instance, when two or more Member States can investigate and prosecute the same perpetrator for cybercrime offences committed outside their respective territories, or when criminal acts committed in the cloud are involved.

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

In 2014 the Internal Security Agency recorded 7 498 incidents. The following categories of incident occurred most often: botnet (4 681 incidents), wrong configuration of device (2 213 incidents), scanning (132 incidents), social engineering (119 incidents), web application errors (101 incidents).The reports on the cyber security threat landscape and cyber incidents in the Polish Internet domain are prepared by CERT POLSKA[23].

6.1.2 Mechanism for responding to cyber attacks

The Cyberspace Protection Policy of the Republic of Poland provides for a three-level National Response System for Computer Security Incidents in cyberspace:

1) Level I – the level of coordination – the minister responsible for informatisation;

2) Level II – computer incident response;

a) the Governmental Computer Security Incident Response Team CERT.GOV.PL;

b) Departmental Centre for Security Management of ICT Networks and Services performing tasks in the military sphere;

3) Level III – the level of implementation – administrators responsible for individual ICT systems operating in cyberspace.

The operational tasks of cyberspace protection are also performed by public and private teams established by telecommunication operators and scientific-research communities.

[23] http://www.cert.pl/PDF/Report_CP_2014.pdf

The main responsibility of the Governmental Computer Security Incident Response Team (CERT.GOV.PL) is to perform operational tasks related to the security of information systems of public bodies. Its chief task is to ensure and develop the capability of public administration units to protect themselves against cyber threats, in particular against attacks aimed at the ICT infrastructure. The CERT.GOV.PL mainly manages the cyber incidents within the public sector and its actions include coordination of the incident response process, resolving and analysing incidents, as well as the coordination of responses security breaches. The CERT.GOV.PL publishes announcements concerning security threats and notifications security bulletins and annual reports on cyber security in public bodies.

Utmost importance is attached to CERT POLSKA operating within the structure of NASK:

- responding to threats and incidents in the Polish Internet domain (.pl);
- publication of annual reports about cyber threats;
- creating tools and information systems to increase the potential of cybersecurity in the country: an early warning system, and a knowledge and information exchange platform ARAKIS,
- n6 platform, the information exchange system NISHA,
- specialist training and the organization of the SECURE conference.

According to *the Cyber Safety Policy of Poland*, CERT.GOV.PL is the second level of the National Response System on computer incidents in Polish cyberspace. In the case of incidents that are wide-ranging in their effects or activities, the team's task is to coordinate and respond to the incident and also exchange information between institutions directly affected by the cyber attack. Moreover, the team uses experience gained from previous incidents, prepares warnings with technical information and recommendations regarding further action and passes them on to government administrative bodies. The aim here is to prevent or reduce possibility of other institutions suffering similar attacks.

CERT.GOV.PL is responsible for dealing with incidents that affect government agencies. There are also agreements with IT operators as regarding voluntary reporting. This gives the team has opportunity to cooperate when responding to incidents that appear in institutions' data networks. Should there be an incident which is beyond the team capacities, CERT.GOV.PL cooperates with all other Polish Cyber Incident Response Teams such as CERT POLSKA or MIL-CERT.
In 2015, on the basis of Commander-in-Chief of the Police's decision, the team that responds to computer incidents (POL-CERT) was based at the National Police Headquarters. The Team performs the tasks associated with the coordination of the response to computer incidents in police teleinformatics systems and networks. In order to streamline the flow of information about events in Voivodeship (regional) Police Headquarters as well as in police colleges, the contact points dealing with cyber issues were established. In future POL-CERT will constitute the element of the Polish system of reacting to computer incidents in the cyberspace.

Critical Infrastructure (CI) operators are involved in the process of reducing the risks of cyber-attacks and mitigating their impact by protecting assets of its own critical infrastructure and through cooperation with public administration. Critical Infrastructure operators in particular prepare and implement critical infrastructure protection plans. Furthermore, CI operators plan and implement their own back-up systems supporting this infrastructure and support its full continuity. The requirements and measures for ensuring cyber security and information exchange are set out in the *National Critical Infrastructure Protection Programme*[24]. The solutions adopted are reviewed in the process of consultation and approval of plans for the CI protection. Within the framework of its activities, agreements with CI operators willing to cooperate with the CERT.GOV.POL's team have been signed.

[24] http://rcb.gov.pl/?page_id=210

Additionally, under the 2007 *Crisis Management Act,* to obtain information about a possible critical situation following a terrorist incident that threatens critical infrastructure, the Head of the Internal Security Agency may advise entities which suffered from those threats. That Act impacts directly on CERT.GOV.PL activity.

Critical infrastructure operators from the public and private sectors are obliged, on the basis of § 7 of the 2010 *Regulation of the Council of Ministers on the National Critical Infrastructure Protection Programme*[25] and the records of the programme itself, to provide information about the risks to the critical infrastructure and the threats to the security of the State and citizens resulting from the disruption of the functioning of critical infrastructure. There is an obligation to exchange information about any circumstance or event which might affect the safety of the critical infrastructure, including cyber-attacks. The procedure for the exchange of information with crisis management centres and other public administration bodies on threats to critical infrastructure is one of the requirements of Critical Infrastructure Protection Plans- § 2 (3) of section 5 of the *Regulation of the Council of Ministers of April 30, 2010 on Critical Infrastructure Protection Plans*[26] and must be included in these plans, together with an indication of the means of communication.

As far as CERT.GOV.PL is concerned, the team implements tasks related to the public administrative bodies. Within team's activity framework, agreements have been signed between the International Security Agency and others who are willing to take part in the ARAKIS-GOV and ARAKIS 2.0 GOV projects and with critical infrastructure operators who are willing to exchange information on incidents. Moreover, CERT.GOV.PL cooperates with Microsoft Co. in the field of professional training for teleinformation systems administrators who work for the public administration.

[25] Official Journal from 2010, No 83, item 541
[26] Official Journal from 2010, No 83, item 542

The main problem identified by the team CERT.GOV.PL, is the lack of a legal act controlling the response to cyber incidents in the range of activities presented. There are no legal instruments that make it obligatory for institutions to report on undertaken activities in case information is forwarded to them by CERT.GOV.PL.

6.2 Actions against child pornography and sexual abuse online

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

The police have databases containing, inter alia, the identity of the perpetrators. The police do not have a database specially dedicated to victim identification. This situation is the result of legal regulations in Polish law, one being the *Act on the protection of personal data*. It also results from the lack of legislation allowing law enforcement authorities to establish and use a database strictly dedicated to victim identification.

It was noticed during the on-site visit that the police have no dedicated hash values database to facilitate the investigation and identification of child sexual exploitation victims.

The Polish police use all possible legal ways to delete child abuse content from the Internet. They do so mostly by using the „notice & takedown" procedure, frequently in the framework of international police and cooperation. Moreover, the child abuse images seized in a particular case (i.e. during the execution of a search warrant) are also deleted after the case is closed and the judicial procedure completed. There are no special procedures that are dedicated specifically to children – victims of sexual abuse whose images are distributed on the Internet. However, these victims can be provided with assistance on regular basis to avoid mental and physical harm as well as re-victimisation (the same as assistance provided to victims of child sexual exploitation).

During the on-site visit, the evaluation team visited the NGO Nobody´s Children Foundation. Its main task is to help children, inter alia, if they fall victim to child sexual abuse or domestic violence. The premises of the Foundation consist of specially designed rooms where children are interviewed by the competent authorities. The interviews of young victims in co-operation with Nobody´s Children Foundation, and the subsequent use of the video recordings of the interviews during court proceedings, is in the opinion of the evaluators an example of best practice that enables re-victimisation to be avoided.

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

A special educational campaign *GADKI* ("Underwear Rule" www.gadki.fdn.pl) was created as a Polish version of the Council of Europe's „1 in 5" Campaign. It implements the commitment entered into by Poland following the ratification of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Its goal is to educate parents on how to provide their children, in a simple and natural way, with the information which can protect them from sexual abuse and to raise the children's awareness that they make decisions about their body and that they can always say "no" if the action violates their intimate area.

Moreover, the evaluation team was informed by the Ministry of Justice of a bill being drafted to create a legal basis to establish a register of sexual offenders, specifically those convicted of sexual crimes against children.

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

An annual agreement between the Commander-in-Chief of the Police and the President of *Nobody's Children Foundation* was signed on June 7, 2014 and extended for another year in June 2015. The aim of this agreement, which is a part of international campaign "Don't look away", is to prevent and combat the sexual abuse of children in travel and tourism. The said document provided the basis for increasing the efficiency of police work by creating a special website (www.stopseksturystyce.fdn.pl), where anyone can find the application form for reporting (anonymously or officially) information about cases of sex tourism or other suspicious behaviour possibly connected with the sexual abuse of children.

Furthermore, all these reports are checked by the relevant police units, either at national or regional level (depending on where a specific report or the information is directed) which specialise in combating CSE. Once in possession of the information, criminal investigators can verify it and then take appropriate operational and investigative measures.

The campaign, lasting more than two years, attracted the media, travel companies and Internet users. The relevant website was visited more than 7 500 times. 750 officers and police civilian staff have been trained in the framework of the Polish child sexual abuse project that was referred to above. Hotel staff, tourism students, as well as travel agents, also participated in this training. The police, the Nobody's Children Foundation, and ECPAT International have been the main organisers of the project from the very beginning. The Ministry of the Interior and Administration, the Ministry of Sport and Tourism, the Human Rights Defender and the Ombudsman for Children are honorary patrons of the project.

The following preventive actions were undertaken to keep children away from illegal content on the Internet:

Dyżurnet.pl hotline

Since 2004 NASK has had the Dyżurnet.pl team which, as part of the Safer Internet Programme (currently, CEF - Connecting Europe Facility), deals with reports received from Internet users about illegal or harmful content (in particular CAM). This contact point, acting within NASK, is part of the Polish Safer Internet Centre set up by NASK and the Nobody's Children Foundation. Dyżurnet.pl is a member of the INHOPE association that brings together similar teams from all over Europe as well as from outside Europe.

The team cooperates with the providers of content, the police and similar teams all over the world, and the type of cooperation in tackling the dissemination of harmful or illegal content resembles the work of the CSIRT teams. There is close cooperation between Dyżurnet.pl and CERT POLSKA regarding consultations on the technological aspect of the problem.

The police have established a partnership with the "Dyżurnet.pl" hotline which involves the reporting of indecent images and content found on the Internet, including CAM, to a special police unit (Department for Combating Cybercrime). Moreover, the Nobody's Children Foundation runs a hotline dedicated to children and adults who want to report a child abuse crime or a suspicious situation which can lead to such a crime. Reports on these situations are forwarded to the police so that they can take proper legal action, if needed. The hotline is run in cooperation with the police.

Educational activities

Since 2013 the Ministry of Digital Affairs has been carrying out activities aimed at protecting children and teenagers against inappropriate content on the Internet. The biggest emphasis is put on educational activities increasing awareness of hazards coming from the Internet as well as skills in the safe use of the Internet. These actions are addressed to various groups of recipients, mainly to children and teenagers, but they also cover teachers and parents. The implementation of these actions, as a public task, is delegated to non-governmental organisations on the basis of Article 13(1) of the *Act on public benefit and volunteer work* that are selected by way of a competition. So far, the Ministry of Digital Affairs has financed 11 projects in this area. Subsidies for non-governmental organizations for activities aimed at protecting children and teenagers on the Internet in 2013 amounted to 447 000 PLN (112 055 EUR) in 2014 – 838 925 PLN (210 304 EUR) and in 2015 – 1 000 000 PLN (250 683 EUR).

Three projects of this type were planned for implementation in 2015. These projects include training for approx. 6,000 pupils aged 6-12, approx. 4,500 pupils aged 13-18 years and approx. 2,000 teachers, educators and parents. A standard for online security for educational institutions was developed with the participation of cyber security experts (NASK and the Janusz Korczak Pedagogical University in Warsaw) as part of the financed projects. The standard includes graphic diagrams with procedures for intervention, for instance in the following cases: cyber violence, grooming, encountering illegal content, sexting, acts forbidden by law, excessive use of modern technologies as well as how to respond to computer hazards and incidents. A preventive model was also presented - recommendations for the preparation of a safe and effective Internet infrastructure for schools or other educational institutions.

The Minister of National Education lays down the direction of state educational policy every year. The aim is to improve safety in schools. In the school year 2014/2015, the priority remains the prevention of aggression and violence in schools. Establishing the priorities means that throughout the school year the headmaster and teachers should pay special attention to this issue, and institutions that support schools, such as psychological and pedagogical centres, teacher training centres or pedagogical libraries should support headmasters in the implementation of those activities, e.g. they should prepare information and education materials or offer training for teachers.

Moreover, the work on the second edition of the government programme "Sa*fe and friendly school*" for the years 2014-2016 is in progress. The main objective of the programme is to increase the effectiveness of education and prevention actions and to create a friendly and safe school environment. The issues covered include:

1) Prevention of aggression and violence, including cyberbullying;
2) Prevention of addiction to computer games, the internet and gambling;
3) Developing students' skills, teaching them how to behave properly in the environment of new media;
4) Preparing teachers to teach classes on cyberbullying.

Under the "*Safe and friendly school*" government programme a helpline has been opened. The helpline is for students, parents, teachers and people who cooperate with schools.

1) Number 116 111 and online help are available for students. Open for ten hours a day, 7 days a week, excluding public holidays;
2) Another phone number - 800 100 100 - and online help have been made available to parents, teachers and other professionals for six hours a day from Monday to Friday, excluding public holidays;
3) The websites www.116111.pl and www.800100100.pl will offer free telephone and online support.

The websites are an inseparable part of the telephone help and they include an information and education package. That the help given is of high quality is ensured by constant monitoring of the consultants' work by supervisors during duty hours and by holding briefings of the team of consultants on duty before and after duty hours each time, as well as by monthly supervisions. The organization submits monthly reports on interviews and interventions.

Police actions

"CyberPol" is a programme based on cooperation between the police and NASK and is aimed at sharing knowledge and experiences on measures taken in relation to the activities of children and adolescents on the Internet, combating cybercrime and raising awareness of people using the network. The main task of the "CyberPol" is to combat cybercrime and increase the safety of children and young people in the network.

The Ministry of the Interior and Administration has launched a hotline, website and e-mail. This makes it possible to instantly report illegal and harmful Internet content that threatens children and young people.

Cooperation between the National Police Headquarters and the Nobody's Children Foundation, the Research and Academic Computer Network, the Children's Ombudsman and the Orange Foundation as part of the European Commission Safer Internet Programme, led to the creation of the "*Child on-line*" campaign. An important part of this campaign, apart from media activities, is the wide range of educational material offered. This was prepared by the Nobody's Children Foundation and is aimed at children, adolescents, their parents and the professionals.
In this campaign an innovative course called "*Child on-line*" was created. It shows various aspects of the sexual abuse of children on the Internet and other forms of threat to young Internet users (www.dzieckowsieci.pl). The campaign is conducted under the patronage of the Police National Headquarters, the Ministry of Education, the Government Plenipotentiary for Equal Treatment and Office of Electronic Communications.

Activities have been supported by the companies ArcaBit, Virtual Poland, VA Strategic Communications and several media partners, and are aimed at promoting the possibilities offered by the Polish project Helpline.org.pl, which has been operating since February 2007. Helpline.org.pl consultants help on-line or by telephone in situations when a child's or an adolescent's safety on-line is in danger.

Every year the police conduct or participate in national, regional and local campaigns and initiatives concerning the safe use of the Internet and threats that children and juveniles may face in Internet, including situations connected with the various forms of CSE or CAM. More information on projects, programmes and social campaigns which concern the preventive measures taken in this field may also be found at the URL address http://fdn.pl/en/social-campaigns.

"Live streaming" or "real time web-based child pornographic performance" is not yet a growing trend in Poland, according to the police assessment. However, the police are aware that these criminal phenomena may be a serious problem in the future.

So far only a few cases of commercial "live-streaming" have occurred in Poland, most of them involving a situation where Polish offenders tried to watch live child pornographic performances hosted abroad (e.g. the Philippines), offering an amount of money in exchange. The other type of crime occurring in Poland concerns situations in which children perform sexual acts on the webcam with no commercial gain or profit during the chats with the adult offender(s). Both of the above-mentioned criminal activities are prohibited. Under the Polish Penal Code "live streaming" or as it is described "participation in the presentation of pornographic materials with participation of minors" is punishable (Article 202 § 4a and 4c) and the penalty is up to two years' imprisonment. Moreover, the offender's conduct is also seen as part of child – grooming which is also punishable under Article 200a of the Code.

6.2.4 Actors and measures countering websites containing or disseminating child pornography

Polish regulations on blocking of access, removal of content, and taking down of web pages are based on standards set out in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). The 2002 *Act on providing services by electronic means* states that the electronic service provider is liable for illegal content if this provider has received reliable information about the illegal character of this content. Therefore, to avoid such liability, ESPs block or remove such content. An important role in this regard is played by NGOs, which inform the ESPs.

The dissemination of CAM is prohibited under Article 202(3) of the Penal Code. Therefore, where CAM hosted in Poland is detected, the police take all necessary steps to identify the individual responsible for uploading such materials and remove illegal content from the internet. If a hotline receives information about child abuse content, it informs the police (usually the NPH's Department for Fighting against Cybercrime of the) which next deals with the case.

When the child abuse content is detected (no matter who found it on the Internet) the police, on receiving the information, contact the relevant ISP or ESP for the purpose of identifying of the individual who uploaded it, seizing the material (if possible) and then removing the content. Then, once the perpetrator has been identified, legal and procedural steps against that person are taken.

Polish law does not allow the use of techniques which block access to the website, even if it contains CAM. The police remove detected child abuse content but they are not allowed to block access to the web pages and websites containing such materials. In such cases the procedure of "notice & takedown" applies. According to statistics presented in hotline reports, this procedure is quite successful and the CAM is quickly removed from the Internet[27].

There is no specific procedure for blocking access/removing on-line content, but there are different was in which CAM detected on the Internet can be reported: mostly online in special format (if sent to a dedicated hotline or by hotline to the police) or as an e-mail but also by letter or as from time to time as information given orally.

Various different filtering tools are available in Poland. Many of them are provided free of charge by NGOs, internet security companies, and some of the ISPs (mainly telecoms). However, ISP/ESP are not obliged to use or to offer such tools to their customers.

There is no single authority responsible for tackling illegal on-line content. Depending on the nature of such content (its illegal character) the decision on its removal (if the ESP/ISP has already not removed/blocked such content) may be issued by criminal or civil court.

Every citizen, institution or organisation in Poland is obliged to inform the police about crime that has been committed. That is why the police receive reports about the detection of CAM, including the web pages/websites containing such materials, from various actors: fellow nationals, NGOs, public institutions and other LEAs.

[27] More information (in English) at the URL: https://dyzurnet.pl/en/multimedia.html.

The principle of the liability of service providers for providing electronic services are defined in the *Act on providing services by electronic means,* which implements Directive 2000/31/EC on e-commerce:

- Article 12 relates to the exclusion of liability of a service provider in case of so-called mere conduit or the provision of access to a telecommunication network. The exclusion of liability also covers automatic and short-term indirect storage of transferred data if this action is aimed only at conducting the transfer;
- Article 13 determines the grounds for the exclusion of liability in the case of a service known as caching. This means automatic and short-term indirect storage of data in order to accelerate repeated access to it. The service provider is not responsible for the stored data if it does not modify the data, if it uses recognised and IT techniques usually applied for determining the technical parameters for access to data and their updating and does not inhibit the use of recognized and usually applied IT techniques for the collection of information on using the collected data;

- Article 14 relates to the exclusion of liability for so-called hosting. The service provider is not responsible for the stored data if he does not know about its illegal nature. When the service provider receives an official notice or obtains credible information about the illegal nature of the data or related activities and prevents access to this data, the service provider will not be responsible for damage caused to the service user as a result of preventing the access to the data (the notice and takedown procedure).

Under Article 15, service providers are not obliged to verify (monitor, control, analyse) data transferred, stored or shared by them in relation to services specified in Article 12-14. This is especially significant in the case of hosting where one of the grounds for the exclusion of liability is the service provider's knowledge of the illegal nature of stored data.

On the basis of the provisions of the *Act on providing services by electronic means* it is acceptable to block access or to remove content if the published content is of an illegal nature and the service provider is notified of that fact. For this purpose, the service provider should obtain a so-called credible message. It may be sent by anyone - both the injured party and a third party not connected with the stored data. It is possible to obtain a credible message from the service provider itself, e.g. as a result of becoming familiar with the users' comments on an administered Internet forum. The service provider may also be notified by a public authority, which sends the official notice, as it is called, to the service provider.

Where child abuse content hosted abroad is detected, the police inform the relevant LEA in the country concerned and provide it with all materials and evidence collected. As regards international channels of police cooperation in such matters, the police use Europol (if the case concerns EU Member States or has links with the Europol – SIENA channel), and the Interpol and liaison officers of the respective countries. If CAM hosted abroad was detected by the hotline, it informs its counterpart hotline in the respective country if it exists. Then hotline informs Police.

6.3 Online card fraud

6.3.1 Online reporting

Citizens and private companies usually report online card fraud offences to the banks as complaints, and the banks, as the victims, then notify the law enforcement agencies.

According to the Polish authorities, the cooperation between the industry, banks, the private sector and law enforcement authorities in the field of prevention and fight against online card fraud is effective. They constantly making the authorisation of online transactions and customer authentication stricter. Banks and the private sector notify the police if they find any abuse of new payment tools. The police are not informed of the bank's strategy in the field of increasing non-cash payment security.

In accordance with the information on payment cards published by the National Bank of Poland (NBP) in March 2015, 5% of all payment cards used in Poland had only a magnetic stripe. The vast majority of payment cards had both a magnetic stripe and a microchip (94.6% of all payment cards). The total number of payment cards equipped with only a magnetic stripe is gradually decreasing. A microchip solution based on the EMV standard ensures completely safe cards usage.

Moreover, in accordance with *Assessment of the functioning of the Polish payment system* in the second half of 2014 published by the NBP (on the basis of the data obtained from banks), the volume and value of fraud transactions made with the payment cards in that period increased by 10,9% and 4,9% respectively. However, in accordance with the above-mentioned document this increase is mainly caused by growth in the numbers and value payment card transactions (the volume and value of fraudulent transactions in relation to all payment card transactions are still at the same level– fraudulent transactions represent only 0.003% of the volume and 0.006% of the total value of payment transactions made with the use of payment cards issued by the banks).

It should be noted that on 30th September 2013 a consultative body of the NBP published *Recommendations concerning contactless payment cards*. The recommendations contain rules on the issuing, servicing and acceptance of contactless payment cards. The recommendations are aimed at improving the procedures related to the issuance of this type of payment card. In accordance with report on the implementation of the Recommendations, published by the Polish Bank Association (PBA) in April 2014, all banks – payment cards issuers – were in compliance with the *Recommendations*. Only two banks noted that they would implement the Recommendations by the end of 2014. According to the Polish Financial Supervision Authority (FSA), in January 2015 both banks declared compliance with the Recommendations.

Moreover, the Payment Service Providers (PSP) undertake activities aimed at ensuring the security of payment transactions. Banks, in order to secure their ATMs, install anti-skimming card readers, which record fraud attempts. Simultaneously, the vast majority of ATMs are monitored by the cameras. In order to enhance the safety of card transactions, a special helpline ((+48) 828 828 828) was set up for those payment cards users who lost their cards. This solution makes it possible to block a lost card even if the user does not have the bank phone number. A key element of this system is the fully automated helpline IVR using speech recognition technology.

The proceeds of online card fraud are often laundered in countries other than the country of origin of the victim. The Polish Financial Intelligence Unit, responsible for combating money laundering and the financing of terrorism, focuses on enhancing cooperation with its foreign counterparts in order to determine whether the suspicious transactions under investigation are associated with the laundering of the proceedings of online card fraud.

Poland belongs to the AWF SOC FP TERMINAL. Cooperation improves the exchange of information in the course of casework. The national coordinator of the AWF SOC FP TERMINAL work file is a designated police officer in the Department for Fighting against Economic Crime (Criminal Service Bureau of the NPH).

6.3.2 Role of the private sector

In area of card fraud, the police cooperate with the Polish Bank Association (PBA). Cooperation with banks (exchange of information, mutual training) is based on the agreement. This cooperation has evolved over the years: it has successfully initiated and organised work aimed at preventing the commission of banking crimes, including crimes involving the illegal use of payment cards. The active participation of the representatives of the PBA in events organised by the Criminal Service Bureau of the NPH (dedicated to training to deal with this kind of crime) has contributed to a significant widening of the knowledge and skills of police officers in dealing with the above issues. Furthermore, in the framework of mutual cooperation an algorithm for law enforcement with regard to the detection of card fraud was developed with representatives of the PBA and the security department involved in fighting card crime. The aim of this strategy is to facilitate criminal proceedings in the field of card fraud. This subject was divided into 4 areas in order to achieve this objective: reporting the theft of a payment card, credit card disclosure by an unauthorized person or through a search of the circumstances enabling the commission of an offence, on suspicion it was committed at the point of transaction, and if data was copied from a credit card.

6.4. Conclusions

- The Cyberspace Protection Policy of the Republic of Poland establishes a three-level National Response System for Computer Security Incidents in cyberspace: the first level of coordination at the ministerial level; the second level computer incident response and the third level of implementation refers to administrators responsible for individual ICT systems operating in cyberspace.

- The main task of the CERT.GOV.PL is to provide cyber security at the governmental level (second level). It manages the cyber incidents within the public sector and its actions include coordination of the incident response process, resolving and analysing of incidents, coordination of responses to security breaches. Should an incident occur which exceeds the team competencies, CERT.GOV.PL cooperates with all other Polish Cyber Incident Response Teams such as CERT POLSKA or MIL-CERT.

- The CERT POLSKA, which is under the coordination of the Ministry of Digital Affairs, is a leading organisation in the collection and analysis of cyber attack incidents in Poland. Critical infrastructure are obliged to report cyber attack incidents to CERT POLSKA. It acts as a Centre of Excellence and has the ability to respond to threats, to develop early warning software systems and to provide dedicated training on cybercrime and cyber security. Moreover, it conducts research in the field of cyber security and collects and reports statistics on cyber attacks annually. CERT POLSKA continues to cooperate closely with CERT.GOV.PL and other CERTS for the purpose of fighting cyber-attacks.

- Poland has established structures to deal with online child sexual exploitation. There is effective cooperation with international entities such as Europol, Interpol and NCMEC as regards the collection and analysis of information related to child sexual exploitation. Moreover, initiatives and measures were taken to tackle the phenomenon of "child sex tourism". There are also a number of public campaigns and initiatives that were launched to raise public awareness (e.g. cyber violence, grooming, illegal content and sexting). However, there is no direct connection between the Fight Against Cybercrime section of the police and the ICSE database. After the on-site visit the evaluation team was informed that in 2016 actions were taken to re-establish a direct access to the ICSE database.[28]

[28] The evaluation team was informed that one dedicated police officer at the National Police Headquarters, does have currently direct access to ICSE database. This police officer is soon to train others to have access to ICSE database. The ICSE database is used by dedicated police staff on a daily basis in the frame of cases concerning sexual exploitation of children as well as for the purpose of joint international efforts in victims' and offenders' identification.

- It was noticed that there was no dedicated hash values database within the police to facilitate the investigation and identification of child sexual exploitation victims. In the opinion of the evaluators, the lack of a national register of child pornography files that identify unique files with hash-sums seems to be a great disadvantage. Such a register could save a lot of resources, which might be used to achieve greater success in the fight against cybercrime.

- Poland has managed to address effectively the re-victimisation of children by introducing specialised interviewing rooms that are running under a non-governmental organisation called the Nobody's Children's Foundation. The Foundation has impressive facilities specifically designed, furnished and decorated in such a way that interviews of children and teenagers in the context of investigations for sexual abuse can be carried out in a neutral and familiar atmosphere, without confrontation between victim and perpetrator. The Foundation also offers psychological, medical, and legal help to victims of these types of offence. In the opinion of the evaluators, the tasks performed by the Foundation and the professionalism it developed should be regarded as best practice. Moreover, the evaluators acknowledged that the draft legislation establishing a register of convicted paedophiles may further enhance the protection of victims.

- A phone line for supporting and counselling children in difficult situations is also provided by this NGO. The telephone helpline at the Nobody's Children Foundation is a big success, but due to financing problems it cannot be operated on a 24/24 basis. Since in the opinion of the evaluators the helpline plays an important and useful role for victims, consideration could be given to supporting the Foundation so that it works on a 24/24 basis.

- Moreover, it was noticed that there is an effective “notice and takedown” procedure in cooperation with the ISPs. It seems that data retention and co-operation with the Polish ISPs works from a practical perspective although some Member States suffer from lack of sufficient co-operation with the police and legal authorities. This appears not to be the situation in Poland.

- The police working with the Polish Bank Association offers an impressive and at the same time effective example. The police and Computer Emergency Response Teams are part of the advisory board of the Polish Bank Association, a fact that has led to effective information sharing and success in the fight against cyber attacks. This kind of cooperation with the financial sector creates a win - win situation for both sides which, in the opinion of the evaluators, should be regarded as an example of best practice.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

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

Polish prosecutors were positive about cooperation with Eurojust. In most cases such contacts were used to identify competent authorities, to clarify formal requirements or to speed up the processing of requests.

Poland takes part in two Analysis Work Files: AWF SOC (Serious Organised Crime) and AWF CT (Counterterrorism). Poland is involved in three FPs which have been helping to combat cybercrime: FP Terminal, FP Cyborg and FP Twins. National coordinators of each FP were appointed to maintain the high standards of coordination of exchanged information in Poland, based on the 2014 Decision by the Chief Commander of the Police on establishing national experts to carrying out tasks of Europol AWFs.

In connection with the combating of credit card crime Poland participates in the AWF SOC FP TERMINAL. Cooperation in this area essentially takes the form of exchanges of information in the course of casework at national level (contributions, requests) and at international level (replies to requests, taking part in actions or operations). The national coordinator of the work file AWF SOC FP TERMINAL is a designated officer of the Department for Fighting against Economic Crime (Criminal Service Bureau of the NPH). This type of crime is also tackled at regional level. Each Voivodeship (regional) Police Headquarters has an 'Economic' division which appoints a coordinator in the field to combat this kind of crime.

In September 2015, the Department for Fighting against Cybercrime was appointed to participate in EMPACT cyber-attacks. Moreover, the Department for Fighting against Cybercrime is also a member of Europol's AWF SOC FP Cyborg. However, due to the fact that Poland is a new member of the above-mentioned initiatives (FP Cyborg and EMPACT cyber-attacks) it does not have much experience of cooperation in concrete cases, but the Department for Fighting against Cybercrime aims to improve cooperation with Europol in the area of combating cybercrime.

At the moment the Police cooperates very closely with FP Twins at Europol (as a member of this Focal Point) in several cases where the participation of Europol is needed, and also cooperates in international operations led or coordinated by Europol such as 'Downfall II', 'Daylight', 'Depletion', 'Lima Rhodes', etc.

In addition, Poland participates in the planned operations, e.g. the 'Airline Ticket Fraud Action Day'. The operation is organised once a year and its purpose is to prevent crime associated with buying airline tickets online using illegally copied data from payment cards. The operation also involves representatives of the largest airlines in the world, including LOT Polish Airlines.
Since 2013, Poland has been a board member of the European Union Cybercrime Task Force (EUCTF) composed of the Heads of the designated National Cybercrime Units throughout the EU Member States and Europol. The EUCTF is an inter-agency group formed to allow the heads of Cybercrime Units, Europol, the European Commission, CEPOL and EUROJUST, with the participation of INTERPOL, Norway, Switzerland and Iceland as observers, to discuss the strategic and operational issues related to cybercrime investigations and prosecutions within the EU and beyond.

Furthermore, in September 2014 Europol launched the Joint Cybercrime Action Taskforce (J-CAT) within its European Cybercrime Centre. The members of J-CAT were all co-located at Europol's headquarters and jointly involved in major cybercrime investigations and operations. The Criminal Service Bureau and the Central Investigation Bureau of the Police have already declared their willingness to join this project.

The Eastern Partnership project led by Poland became part of Operation Action Plan 2016. Poland is actively cooperating with EC3 (FP Terminal) to engage with the Eastern Partnership countries on combating payment card fraud.

As regards cooperation with the European Union Agency for Network and Information Security (ENISA), NASK and CERT POLSKA closely cooperate with the Agency in the form of engagement in its management bodies and working groups, developing expertise and guidelines ordered by ENISA. It was possible to obtain the opinion of ENISA in accordance with Article 14.2 (d) of Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the ENISA and repealing Regulation (EC) No 460/2004; the member of the board of ENISA representing the Polish Government is an employee of NASK.

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

Polish experience shows that Eurojust involvement usually results in a shorter time for processing requests.

The assessment of cooperation with Europol is also positive. The good practice and information on tools which support the work of police officers who are dealing with cybercrime cases are also provided by Europol. During the working meetings which take place within the EUCTF (European Union Cybercrime Task Force) group operating within EC3 at Europol, information is provided on the latest threats of cybercrime.

With regard to combating CSE and CAM, the very good cooperation with Europol's analytical work file AWF SOC – FP Twins was underlined. Due to the fact that CSE (in many different kinds of this phenomenon) has a trans-border character, the international cooperation of LEAs is crucial to combat this area of crime. Therefore, based on Polish Police experience and results of investigations and operational actions conducted together, the assistance of Europol, and FP Twins in particular, in combating sexual abuse of children and child abuse images is highly appreciated.

7.1.3 Operational performance of JITs and cyber patrols

In 2015 Poland established a JIT with Sweden on fraud online. The Police has not yet participated in operational phases of large-scale international operations directed against CSE and CAM (including monitoring of specific areas of the internet i.e. paedo bulletin boards in TOR network).

7.2 Cooperation between the Polish authorities and Interpol

According to the Polish authorities, cooperation with Interpol is good - and in the field of victim identification, even excellent.

The Police cooperates closely with Interpol in the area of identification of CSE victims, especially in the use of the ICSE database. Using Interpol channel the Police receives from and provides to other countries operational/intelligence information and evidence of CSE and CAM crimes for the purpose of taking any relevant actions which are deemed necessary (in both EU Member States and third countries).

At the moment the Police has access to ICSE through direct contact with relevant Interpol officers and obtains access to the database through I – 24/7 channel. So far, based on information and materials from ICSE which were sent this way, the Police have managed to carry out successful/positive identification of victims and offenders both in Poland and abroad.

However, given the increasing number of cases regarding crimes against children conducted by the police, the National Police Headquarters has recently undertaken actions aimed at obtaining direct access to the ICSE database for the National Police Headquarters and the selected Voivodeship (regional) Police Headquarters. Currently, the Criminal Service Bureau of the NPH makes surveys to establish how many individual accesses to ICSE are needed by criminal officers at the national and regional level. The next step will be to organise training for the future users of ICSE.

7.3 Cooperation with third States

For the purpose of cooperation with third countries in the area of combating CSE and CAM the Interpol channel is mostly used. However, the Police also uses the Europol channel to cooperate with third countries that have signed an operational agreement of cooperation with Europol (inter alia Australia, Canada, USA or Colombia). Nonetheless, the Interpol channel for communication and cooperation with the above-mentioned third countries is used more often. Sometimes the Police also use the Polish liaison officers network, especially in contacts with Belarus, Russia and Ukraine.

According to the Polish authorities, cooperation with third countries through Europol is useful. However, the fully-fledged assessment may be carried out individually based on the circumstances of the specific operation or investigation. As an example, coordination or leadership of operations with the USA was mentioned as an important role of Europol.

There have been requests for judicial assistance to third countries (India, Thailand and the USA). All the cases concerned crimes in which a computer or IT system was used as a tool or a target in particular in online card fraud. Requests were sent through the Prosecutor General's Office, with the aid of Europol or Eurojust.

Polish prosecutors sent MLA requests in cybercrime-related cases to Singapore and Indonesia. Execution of those requests took 11 and 18 months respectively.

7.4 Cooperation with the private sector

The Police cooperates with private entities, mostly located in the USA in cases involving criminal activity: child abuse on-line, distribution of child abuse materials on the internet, etc. In such cases the Police cooperated or tried to cooperate directly with these companies, due to the fact that there are no Polish-sited branches of the relevant entities such as Facebook, Yahoo and Google. Usually, the Police cooperated at operational/intelligence level by sending a specific request and very often received the reply that without MLA/letters rogatory or court warrant, the entity was not able to provide the requested information. These situations had a strong impact on ongoing investigations and sometimes even led to a specific case being closed.

7.5 Tools of international cooperation

7.5.1 Mutual Legal Assistance

Mutual legal assistance in general (MLA, transfer of proceedings, transfer of the execution of sentence as well as extradition) is regulated by the Code of Criminal Procedure and its provisions are applicable according to the principle of subsidiarity - only if there is no international legal instrument or if the provisions of such instrument do not regulate specific issues. It results from the basic constitutional principle of the precedence of ratified conventions over national law, which is valid also for MLA in criminal matters. There are no specific provisions in Polish legislation on MLA for cybercrime, as general provisions on MLA are applicable.

Cooperation with the Member States of the European Union

Judicial cooperation with the competent authorities in the EU is regulated by Chapters 62a-67 of the CPP which incorporate all adopted instruments of mutual recognition in criminal matters and relevant procedural provisions regarding mutual legal assistance, and transfer of proceedings. The main goal of its provisions is to enable smoother and faster cooperation as well as the simplification and acceleration of procedures. Therefore, in connection with relevant multilateral instruments (such as the Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the EU, and the Schengen Convention), it enables direct communication between judicial authorities of EU Member States.

In 2014 Polish authorities received 781 MLA requests from the EU Member States and sent 564 requests. Most of the requests regarding cybercrime, both sent and received, concerned internet-related crimes (computer fraud, fraudulent emails) and attacks on computer systems (most often the use of malware to obtain access to banking systems). Several requests concerned CAM, copyright infringements and hate crime (racist and xenophobic hate speech).

All requests received were dealt with in a period of one to three months, with an average processing time of less than 30 days in the case of urgent requests. Execution of requests sent by Polish authorities took on average between three and 12 months, and up to 18 months in particularly complex cases.

Cooperation with third counties

General rules for MLA with third countries are set out in the CPP and regulations on rules of procedure of the public prosecution service and courts. According to those acts, depending on the provisions of bi- or multilateral agreements, mutual legal assistance requests are transmitted directly (between competent domestic or central judicial authorities) or through the diplomatic channel (through the Ministry of Foreign Affairs).

Bilateral or multilateral arrangements were frequently used to send/execute MLA requests in cases related to cybercrime. The greatest difficulty is that it takes on average two to three times longer for the competent authorities of third countries to execute the requests of the competent Polish authorities than is the case for cooperation within the EU.

Requests for international legal assistance most often concern: finding (identifying) and interrogating computer users with the specified IP, preserving and displaying documents or other data carriers and copies thereof, identifying and interrogating bank account holders (especially the beneficiaries of amounts resulting from phishing), interrogating a witness or questioning a suspect, and obtaining criminal records.

Assistance is possible at all stages of proceedings and for all investigative or procedural measures (interrogation, service of documents, obtaining bank information, expert evaluation, tracing of telecommunications, identification of users of telecommunications, interception and recording of telecommunications and other forms of communication, interception of emails, search and seizure, confiscation, etc.). Tracing of telecommunications and identification of users of telecommunications are the most common reasons for MLA requests with respect to cybercrime. MLA requests have to be used quite often since many cybercrimes (not only cyber attacks) are committed by foreign nationals or involve the use of foreign IT infrastructure.

Every year the public prosecution service sends over 300 requests for legal assistance, and receives around 100 such requests. Most of those requests concern various types of internet fraud (mainly false internet auctions), malware and phishing. The average time of processing incoming requests is one to three months. Obtaining a response from other States usually takes between four to 12 months, with a significantly longer waiting period in the case of non-EU States.

The practitioners met raised concerns regarding cooperation with some Member States, for example those systematically refusing the cooperation in the case of offences where the damage is less than a specific amount of money.

7.5.2 Mutual recognition instruments

It is not possible to provide the requested data on mutual recognition instruments since the type of crime is not specified in the related statistics.

7.5.3 Surrender/Extradition

EAW

Pursuant to Article 607b(1) of the CCP requesting a surrender of a person on the basis of an EAW in the case of offences punishable under Polish law by deprivation of liberty for a minimum period of at least one year. This applies to cybercrime offences, as the penalties provided in relevant provisions of the PC exceed this minimum.

When surrendering a person there is no minimum requirement regarding penalty and a double criminality principle will not be verified if a warrant was issued for a criminal offence punishable under the law of the requesting Member State by deprivation of liberty for a maximum period of at least three years, and if such a criminal offence is classified under the law of that State as, inter alia, a computer-related crime.

The maximum penalties for computer-related offences are all above one year of imprisonment, therefore according to Polish law all computer-related criminal offences fall within the scope of the EAW list and are extraditable.

On average about 10 EAWs are sent each year in cases related to cybercrime, and about four EAWs are received. Execution of the EAWs takes between 12 days and three months.

EAWs are issued (upon a Public Prosecutor's motion or ex officio) by regional courts and transmitted directly between judicial authorities or, if the place of residence of the person concerned is unknown, to the central unit of the Police.

Extradition

With regard to the minimum penalty, the Polish law (Article 604.2 of the CCP) requires that in the event of extradition a prison sentence of one year or more be imposed for the offence under the law of the requesting State (with reference to the maximum penalty for the relevant offences).

Extradition requests are issued by Public Prosecutors or courts, and transmitted to the competent authority in the third county via the Ministry of Justice or diplomatic channels.

Both EAWs and extradition requests are executed by the Public Prosecution service, with the final decision on surrendering a person taken by the regional court (in the case of extradition this is followed by a decision of the Minister for Justice).

7.6 Conclusions

- Poland cooperates with several EU agencies such as Europol/EC3, Eurojust and ENISA. Prosecutors dealing with cybercrime are well aware of both the role and the added value of Eurojust, whose support is requested whenever needed. Moreover, there is effective cooperation by CERT POLSKA with ENISA in the field of cyber attacks.

- The police is in close cooperation with Europol/EC3. They follow the policy cycle by taking part in EMPACT Child Sexual Exploitation, EMPACT Cyber Attacks and EMPACT Card Fraud. Poland is a member of three EC3/Europol Focal Points: FP Twins, participating in the FP Twins supported operations, experts meetings and training; FP Terminal, actively participating in the Action Day on Airline Fraud with several arrests at the airport in Warsaw, and FP Cyborg, participating in Operation Onynimous.

- In 2015 Poland set up a Joint Investigation Team with Sweden against a global OCG active in the area of cyber-enabled fraud. The Eastern Partnership project led by Poland became part of Operational Action Plan 2016. Poland is actively cooperating with EC3 (FP Terminal) to engage with the Eastern Partnership countries in combating Payment Card Fraud. Poland joined EMPACT PCF in 2016.

- Since 2013 Poland has been a Board member of the European Union Cybercrime Task Force (EUCTF) composed of the Heads of the designated National Cybercrime Units throughout the EU Member States and Europol. The EUCTF is an inter-agency group formed to allow the heads of Cybercrime Units, Europol, the European Commission, CEPOL and EUROJUST, with the participation of INTERPOL, Norway, Switzerland and Iceland as observers, to discuss the strategic and operational issues related to cybercrime investigations and prosecutions within the EU and beyond. Poland partially contributed to the annual iOCTA (Internet Organised Crime Threat Assessment) report in the years 2014 and 2015. More input is expected in 2016 and the following years.

- The Polish authorities gained some experience while cooperating with private entities from third States, mostly located in the USA and involving criminal activity such as: child abuse online, distribution of child abuse materials on the Internet, etc. In those cases the police tried to receive data directly from private companies such as Facebook, Yahoo and Google). However, these bodies claimed that without an MLA/letters rogatory or court warrant, they were not able to provide the requested information. Taking into account this experience, in the evaluators' view the EU should examine the possibility of entering into an agreement with service providers like Facebook, Yahoo and Google regarding the provision of data needed in the fight against cybercrime.

- The MLA request procedure is used in order to obtain electronic evidence from other Member States and third countries. The average timeframe for answering a request is between 1-3 months. In the opinion of the evaluators, the MLA procedure seems to be the most effective way to obtain electronic evidence for prosecution purposes although it is sometimes too slow and this adversely affects the investigations.

8 TRAINING, AWARENESS-RAISING AND PREVENTION

8.1 Specific training

Judicial training

The National School of Judiciary and Public Prosecution regularly organises training for the judicial and prosecution service on cybercrime. Since 2009 the School has organised the following course:

- 'Methodology of conducting criminal proceedings in cases including IT systems use' (2009 and 2010),
- 'Investigation and IT systems – electronic evidence in criminal proceedings' (2010),
- 'Practical aspects of criminal proceedings based on the Law on Copyright and Related Rights' (2011; among the topics discussed were cooperation with administrators of internet auction services and the role of IT experts in the course of proceedings),
- 'Criminological reconstruction of a crime. Latest criminology developments in disclosing and securing trace material on crime scene' (2011; discussion related especially to securing electronic data carriers and computer equipment),
- 'Criminal responsibility and provision of medical services. Crimes committed via information networks' (2013).

Moreover, in 2015, nine courses on organised transnational crime were held within the project 'Training for judicial and prosecution service on combating and preventing transnational and organised crime'. This training is also continued in 2016.

In addition, every year newly appointed judges and assessors participate in dedicated training on crimes committed by using computers and IT systems. A training module for 140 judges, prosecutors, assessors and assistants on computer crime is scheduled in 2016. The following topics will be discussed:

- cybercrime,
- securing substantive information on evidence, in particular IT data, with regard to bank crimes, sexual offences online and cyber attacks,
- using e-evidence in criminal proceedings,
- admissibility of e-evidence,
- functioning of the TOR anonymity network and possibilities of detecting criminals using this network,
- methodology of criminal proceedings in cases regarding online and computer fraud, including crimes committed by spreading computer viruses.

Furthermore, the Criminal Service Bureau of the NPH in agreement with NASK provided courses in the area of electronic evidence and techniques of combating cybercrime for judges, prosecutors and police officers.

Police training

The Police provides training in the field of cybercrime: 'Computer Crime - obtaining information from the Internet'. This training has been conducted regularly in the Police Academy in Szczytno since 2005. It is designed for police officers who deal with computer crime and cybercrime. The aim of the course is to broaden the knowledge of police officers in the criminal service in the field of computer crime and obtaining information from the internet, with the aim of improving the preparatory proceedings in cases of computer crime. The topics covered are characteristics of computer crime, computer environment, services in computer networks or procedures to be followed in cases of computer crime. Each year the course, which lasts five days and includes 45 hours of training, is repeated several times.

Within the framework of the central Police training system, the Police organise a specialist course on internet-based data collection for police officers who combat cybercrime. Participation in the course is based on the following criteria:

- police officers should deal with cybercrime - internet-based data collection
- police officers should be directly involved in combating cybercrime in criminal and economic units/departments,
- police officers should have basic computer skills (knowledge of PC-class computer with MS Windows software)
- knowledge of Polish penal law on cybercrime.

The course lasts for five days. In 2014, 25 such courses were organised and 304 police officers were trained. In 2015, 25 courses were planned and 299 police officers were to be trained. On the basis of the decisions taken in the National Police Headquarters in 2015, a team was appointed to develop a course programme for specialised police performing tasks related to combating cybercrime.

In the area of combating CSE and CAM, the police aims to organise 3-4 courses annually for police officers across the country, including officers who deal with international police cooperation. However, there are no courses in the area of CSE and CAM strictly geared to international police cooperation officers. Moreover, the Police experts who specialise in the above-mentioned crime area meet at least once or twice a year to gain new experience, information about current trends and threats as well as to share best practices and case studies.

The range of CERT.GOV.PL Team activities include organised courses and awareness-raising campaigns. The Internal Security Agency in cooperation with Microsoft organised training for administrators of public administration tele-information systems under the IT Safety SCP (Security Cooperation Program). 176 participants took part in that training.

The Ministry of Interior and Administration and the NPH in cooperation with NASK started the 'CyberPol' project in 2015. The main goal is raising the competence of LEAs in cybercrime subjects. 210 policemen are taking part in training at three levels of knowledge (30 policemen from cybercrime units/departments attended a 2-day course provided by CERT POLSKA). Safer Internet (a project run by NASK and Nobody's Children Foundation) provides courses and conferences for LEAs as well as electronic material about children's safety on the internet and with regard to new technologies.

As part of the professional forensic science technicians' training, classes in 'Selected issues of ICT' are held (using content for computer investigators). In the course of their training police officers involved in the fight against economic criminality take part in 'Computer Crime' classes.

The Police Academy in Szczytno conducts the following studies on subjects in the curriculum (at the basic level): *Methodology of investigations into cases with illegal content* and *Acquisition and examination of electronic evidence from computer media.* The Police Academy in Szczytno and the Police Training Centre in Legionowo are responsible for providing training in cyber forensics.

The Cybercrime Research Centre at the Faculty of Law and Administration of the Nicolaus Copernicus University

The *Cybercrime Research Centre* at the Faculty of Law and Administration of the Nicolaus Copernicus University was established and started its activities on 1 October 2013. It carries out research and provides training and education in the field of preventing and fighting cybercrime. The Centre organises annual conferences (web attacks conference) and facilitates cooperation and an exchange of views and experiences between various stakeholders (ISP/ESP, law enforcement, judges, scientists).

Centre for Analytical Intelligence and Excellence to Combat Cybercrime

The *Centre for Analytical Intelligence and Excellence to Combat Cybercrime* was established in the Police Academy in Szczytno in 2015. Cooperation agreements have been signed with a number of private and public entities. The scope of activities of the Centre is as follows:

- training and professional development of the uniformed services;
- development of the methodology of training and professional uniformed services;
- scientific research and development work on the broader issues of cybercrime;
- preparation of reports, publications and educational materials related to the issues of cybercrime;
- organisation of lectures, occasional meetings and conferences and scientific seminars and special projects;
- mutual working meetings to identify areas of cooperation that may be used in scientific and educational work;
- consultations in solving problems relating to combating cybercrime.

The National Cryptology Centre

The National Cryptology Centre, operating within the structures of the Ministry of National Defence, has signed an agreement with three leading public universities (Wroclaw University of Technology, University of Warsaw, Warsaw University of Technology). In accordance with the agreement, the universities launched studies in Computer Security. Additionally, the universities will establish research cooperation with regard to cybersecurity (common research projects, common research laboratories). Warsaw University of Technology has established a Cybersecurity Division (http://cybsec.pl/).

Academia, due to its educational mission, plays an important role in the education process, especially with regard to students and some areas of professional education (e.g. postgraduate studies). Due to its autonomy regarding both private and public universities, it can independently shape its curricula. Therefore, it is not feasible for the Ministry of Science and Higher Education to impose cybercrime-related courses as an obligation. However, it has been noted that cybercrime-related courses are nowadays more frequently organised. Some examples of studies with the cybersecurity specialisation, apart those at the three universities mentioned above, are: WAT – Military University of Technology in Warsaw, Radom Academy of Economics, WSB – The University in Dąbrowa Górnicza, WSPiA – School of Law and Public Administration in Rzeszow. Other universities offer postgraduate studies related to cybersecurity. Some examples are: Warsaw University of Technology, AGH University of Science and Technology, The West Pomeranian Business School, University of Security in Poznan, School of Computer Science and Economics in Krakow, Wroclaw University of Economics, Rzeszow University of Technology, AMW – Polish Naval Academy in Gdynia. The examples of a fairly broad offer of postgraduate studies in cybersecurity show that there is a growing demand for ICT security specialists in Poland.

Moreover, as part of ongoing post-graduate studies in the Police Academy in Szczytno, classes are held on the modules of "Fundamentals of acquisition and testing of digital evidence from computer media" and "Cybercrime". As part of the degree studies I and II in the Police Academy in Szczytno, classes are held on the following subjects: 'Methodology of investigations into cases of illegal content', 'Acquisition and examination of electronic evidence from computer media', 'Crime in cyberspace', 'Fighting crime in cyberspace'.

The Police Academy in Szczytno organises the following annual international scientific-practical conferences:

- Technical aspects of ICT Crime – since 1998 (with 250-300 participants); after each conference a monograph on 'ICT crime' is issued,
- Electronic Payment Instruments Abuse – in the years 2000-2013 (with 200-300 participants),
- Criminal Analysts Symposium with workshops; GIS Day – since 2002 (with 150-200 participants),
- International Internet IPR Law Enforcement Conference – since 2014 (with 150-200 participants); after each conference a monograph on 'Internet infringement of intellectual property' is issued,
- Preventing and combating cybercrime – since 2015 (with 100 participants) in cooperation with AON – National Defence University in Warsaw, WAT – Military University of Technology in Warsaw, AMW – Polish Naval Academy in Gdynia.

In addition to regular courses, one-off courses are organised within CEPOL. Police officers involved in the fight against cybercrime, including lecturers from this field, often participate in training organised by CEPOL, ECTEG, Europol / EC3. Officers from CEPOL ECTEG, Europol are invited to various training programmes or seminars and conferences on combating cybercrime.

CEPOL

1. Stationary activities (courses, seminars, conferences) organised by the EU Member States; several police officers attended four cybercrime activities in 2014 and a number of cybercrime activities in 2015. In 2016 five planned activities are to be carried out. Poland has applied for and been awarded a grant with regard to the course First Responders and Cyber Forensics.

2. Online courses (webinars)

In 2014 three cybercrime webinars were organised, in which 31 Polish participants took part. In 2015 seven activities were organised. The exact number of Polish participants is not known due to the IT system constraints, but Poland maintained its involvement. For 2016 too three webinars are planned. Moreover, it is possible to ask for such an activity to be organised on an ad hoc basis, if necessary.

3. Exchange programme

In 2014 two Polish participants took part in the exchange programme in the area of cybercrime (exchange between the Voivodeship Police HQ in Łódź and Georgia and between the Voivodeship Police HQ in Poznań and Kosovo). In 2015 there were five such programmes (Central Police Bureau of Investigations - exchange with Spain, Customs Service - with Georgia, Voivodeship Police HQ in Kraków - with Bulgaria and two participants from the Bureau of Criminal Service, NPH, exchange with Slovakia). The subject of cybercrime will also be covered by the exchange programme in 2016.

4. E-learning modules.

Furthermore, CEPOL also developed an e-learning module on combating cybercrime.

EUROPOL

In 2015 EC3/Europol/EUCTF/ECTEG training was available in the form of courses, seminars and conferences, such as:

- 11th meeting of the European Union Cybercrime Task Force (EUCTF) 2015, 26 - 27 March 2015 (The Hague, Netherlands), one participant from Poland;
- Cybercrime Payment Card Fraud Conference, 8-9 April 2015 (The Hague, Netherlands), one participant from Poland;
- '1st Europol Training Course on Payment Card Fraud Forensics', 13-17 July 2015 (Avila, Spain), one participant from Poland

- Child Sexual Exploitation Experts Seminar, 1-3 June 2015 (The Hague, Netherlands), one participant from Poland;
- 3rd Meeting of the Forensic Experts Forum, 8-9 June 2015 (The Hague, Netherlands), one participant from Poland;
- EMPACT Cybercrime CSE meeting, 21 September 2015 (The Hague, Netherlands), one participant from Poland.
- 'Analytical Vienna 2015' Conference 21 - 23 September 2015 in Vienna (Austria), three participants from Poland;
- Solution of electronic violence and cybercriminality conference, 15-16 October 2015 (Jihlava, Czech Republic), two participants from Poland,
- European Cybercrime Training & Education Group meeting, 10-11 November 2015 (The Hague, Netherlands), one participant from Poland.

Four policemen took part in ECTEG pilot courses (Python Programming for Investigators (5–9 October 2015, Dublin); Malware for Investigators (30 November– 4 December 2015, Dublin); Live Data Forensics (19–23 October 2015, Apeldoorn and 7–11 December 2015, Wiesbaden).

Development of technologies in the field of ICT has an impact on the daily lives of citizens and increases the activity of criminals. It resulted in the establishment of 'cybercrime' divisions in the Voivodeship Police Headquarters in the second half of 2014. This led to an increase in the demand for training of police officers.

Apart from centrally organised training, the Police also organise local training, which is a responsibility of Chiefs of the Voivodeship (regional) Police Headquarters (Warsaw Metropolitan Police HQ) and financed by their Departments of Finance.

Courses on the prevention of and fight against cybercrime are led by the Regional Police Headquarters, the National Police Headquarters and the Police Training Centre in Legionowo.

The Police Training Centre in Legionowo conducts classes during a specialised course on obtaining information from the internet for police officers combating cybercrime. During that course police officers acquire knowledge and skills in the area of 'Cybercrime'. The annual cost of the course in 2014 was PLN 34 000 (EUR 7 824) and PLN 25 000 (EUR 5 753) in 2015.

Examples of financing training/education with EU Funds and the Norwegian Financial Mechanism

1. Voivodeship Police Headquarters in Lublin

Year 2015 - European Commission's Specific Programme 'Prevention of and Fight Against Crime' ISEC project 'International cooperation of EU law enforcement agencies concerning fight against cybercrime' – PLN 1 168 232(EUR 268 825)

2. Voivodeship Police Headquarters in Łódź

Year 2014 – Voivodeship Operational Programme - 2007-2013 project 'Modern technologies in fight against crime - equipping police operational services of the Łódzkie Voivodeship'. The cost of training within this programme: PLN 130 000(EUR 29 915) (including PLN 19 500 (EUR 4 487) state budget, PLN 110 500 (EUR 25 427) EU budget).

Year 2015 – Norwegian Financial Mechanism 2009-2014 project 'Safe Europe without borders' (training including use of IT in investigations, data recovery, hacking etc.) – PLN 1 165 000 (EUR 268 081) (including: PLN 175 000 (EUR 40 269 state budget, PLN 990 000 (EUR 227 811) EU budget).

3. Metropolitan Police Command in Warsaw

Year 2014 – Norwegian Financial Mechanism 2009-2014 – Improving police competence in prevention of and fight against cross-border and organised crime, including human trafficking and migration of criminal groups, by creating an educational platform using e-learning and distance learning – PLN 55 975 (EUR 12 881) (including PLN 8 396 (EUR 1932 state budget, PLN 47 579 (EUR 10 948 EU budget).

Year 2015 - Norwegian Financial Mechanism 2009-2014 - Improving police competence in prevention of and fight against cross-border and organised crime, including human trafficking and migration of criminal groups, by creating an educational platform using e-learning and distance learning – PLN 731 000 (EUR 168 212) (including PLN 110 000 (EUR 25 312) state budget, PLN 621 000 (EUR 142 900) EU budget).

8.2 Awareness-raising

Ministry of Digital Affairs

As part of the coordination function, the Ministry of Digital Affairs (MDA) is developing and disseminating a network of plenipotentiaries for cyberspace security planned in the strategic document Policy. At the moment, the network has approximately 150 representatives appointed in various government administration offices. So far, the MDA has organised six specialist training courses addressed to representatives and intends to organise subsequent ones. The Ministry of Digital Affairs has prepared a dedicated portal for plenipotentiaries with updated information on cyberspace security. Additionally, the MDA co-organised the CYBERGOV 2015 conference on IT security in the public sector that was held on 18 June 2015.

The Policy provides for conducting a social campaign of an educational-preventive nature focused on raising awareness of the safe use of the internet among children, teenagers, parents and teachers. Within this area the MDA organised competitions for carrying out the public task on the basis of the Act on public benefit and volunteer work, resulting in numerous educational materials, for instance, on the safe use of electronic services.

As part of the dissemination of important information regarding the network and information security, the Ministry of Digital Affairs also initiated the preparation of a document entitled Recommendations for representatives for the security of cyberspace of the Republic of Poland that was adopted by the Governmental Committee for Digitalisation. The MDA is cooperating with the Polish member of ENISA's Management Board, and the materials obtained and the Agency's guidelines are currently being distributed among the representatives.

Actions aimed at raising awareness as well as educational actions regarding the safe use of electronic services are also undertaken by other national authorities, public administration authorities, commercial chambers and research institutes, as well as by private entities, including telecommunication companies and banks. The Operational Programme 'Digital Poland 2014-2020' provides an opportunity to raise the level of citizens' awareness regarding the safe use of the internet and electronically provided services, as well as their knowledge about available tools.

The Police

Police preventive measures aimed at educating society in conscious and responsible use of the internet is contributing to the reduction of threats. Increasing police activity in this area helps to prevent social risks with particular emphasis on accepted priorities.

Public awareness is also raised through the media, using internet publications posted on the website: policja.gov.pl. Information posted there refers to protective action against cyber attacks and how to take preventive measures in this field. Not only information campaigns such as: '*Stop Afterburner*' and '*Stop cyberbullying*' are being organised, but also relevant chats at schools, etc.

Moreover, the officers from the Division for Fighting Against Cybercrime of the Metropolitan Police Headquarters in Warsaw, during their cooperation with educational institutions from Warsaw, conducted 10 meetings with teachers, parents, middle-school students and high-school students. The subject of the training was the prevention, identification and combating of cybercrime. Due to the need for such training in educational institutions, the Division for Fighting Against Cybercrime of the Metropolitan Police Headquarters in Warsaw intends to organise another seven workshops in 2016.

Research and Academic Computer Network

The Police and NASK conducted an information campaign '*Cyberpol*' on the safety of children on the internet, to raise their awareness of the risk of using the internet. Police officers from the prevention, criminal and cyber departments were trained in this field.

NASK organises many security conferences, including SECURE 2015 which is the most significant cybersecurity conference in Poland. Many other events, including as part of EU projects, have been organised in the past. Additionally, NASK (CERT POLSKA) is a partner of the EU FP7 CyberROAD project, which aims to map a cybercrime and cyberterrorism agenda. NASK also takes part in the European Cybersecurity Month (October) event supported by ENISA. This includes publishing online security quizzes and HackMe challenges.

Schools

In order to improve pupils' and students' knowledge of cybersecurity, police officers take part in conducting talks in primary and high schools. In cooperation with the private and public sector, including NASK and Nobody's Children, '*Internet Safer Day*' is organised every year. During this day, seminars for teachers and young people are held on the subject. Audiovisual training materials are also distributed which could be used during school activities and for children's education in future.

The core curriculum of general education in individual types of schools includes Information Technology (IT) classes. Students learn about the dangers resulting from the development of information technology and common access to information; the dangers connected with being addicted to the computer; ethical and legal issues connected with the protection of intellectual property and data protection and the threat of computer crime but also computer crime, confidentiality and security and data and information protection in computers and computer networks. An important task of Polish schools is to prepare students to live in an information society. Apart from obligatory IT classes, teachers of other subjects prepare students to search for, organise and use information from different sources with the use of IT.

Nobody's Children Foundation

NASK together with other partners, e.g. the Nobody's Children Foundation, conducted various awareness-raising projects, especially targeting the young generation. The Nobody's Children Foundation conducted the following projects:

- Education project Necio.pl, which is targeting children aged 4-5 years and their parents. The project's main component is www.necio.pl, a website with child-friendly animation, games and songs explaining to children the rules of online safety and the basics of computer use;
- BeSt application combines the functionalities of a web browser, search engine and parental control tool. It is dedicated to children aged 3-12. The application is based on a catalogue of child-friendly websites collected within the www.sieciaki.pl portal and currently contains hundreds of websites catalogued according to age and themes. The application will enable children to search and surf only on websites appropriate for their age group. The BeSt browser is available for download on: www.best.fdn.pl;
- 'Child on the Net' (http://dzieckowsieci.fdn.pl/) - awareness-raising of children, youngsters and their parents. It covers e.g. awareness-raising campaigns, events and information material for parents.

Another important project is Saferinternet.pl (http://saferinternet.pl/pl/) implemented by NASK and the Nobody's Children Foundation. Safer Internet Project was launched in 1999 and aims at promoting the safer use of the internet and new online technologies, particularly for children. The main objectives of the project are: fighting against illegal content, tackling unwanted and harmful content, raising awareness. The project comprises comprehensive activities promoting the safe and responsible use of new media by children and young people. Some examples: *Real friends or strangers?* - e-learning course for schools, *Watch your face* - Facebook campaign for teenagers, *Become a friend of your child* - educational materials for parents.

8.3 Prevention

8.3.1 National legislation/policy and other measures

On the basis of the regulation on the National Interoperability Framework, the minimum requirements for ICT systems are defined, including the methods to ensure security when exchanging information. In particular, the regulation states that entities performing public tasks are obliged to develop and implement (as well as to keep, monitor and develop) an information security management system. The aspect of information security management is developed in detail, as are, inter alia, plans for such actions as conducting periodical risk analyses and undertaking actions minimising this risk.

The preventive dimension is repeated in the Policy. The strategic objective of the Policy is to achieve an acceptable level of security of the State's cyberspace. This objective will be supported by the development of relevant organisational-legal frameworks as well as a system of effective coordination and exchange of information between the users of Polish cyberspace.

The Act on Police sets the legal basis for initiating and organising activities aimed at preventing offences and fostering cooperation in this field with other State bodies, local government and social organisations. There are also several other legal acts providing for specific legal steps, including the fight against cybercrime, such as the Penal Code, the 2001 Act on protection of databases, the 2002 Telecommunications Law Act, the 2007 Crisis Management Act and others.

Examples of preventive actions conducted by Police in partnership with other institutions:

- 'Be safe online' - educational texts, 'In the Network' (Capital Police headquarters in Warsaw, Nobody's Children Foundation, Microsoft)
- 'Cybernetic jungle' (Regional Police headquarters in Szczecin, Education Office);
- 'I am serving. I respect' (Regional Police headquarters in Gorzow Wielkopolski, Provincial Methodological Centre);
- 'Safety in the web' – contest (Regional Police headquarters in Bialystok);
- 'Stop Cyber Violence' Small Theatre Forms contest, short films (Regional Police headquarters in Gdańsk);
- 'Responsible Parents - Happy Children' - programmes 'Escape in cyberspace - the causes and consequences of addiction' (Regional Police headquarters in Olsztyn, Gold Zet Radio)
- 'University of Third Age' Cracow Police headquarters, and Psychology Science University,
- 'Teach, inform, prevent. Open schools - open Police Units' (Olsztyn Police HQ, Regional Court in Olsztyn, Mazurian Probation Office);
- 'In the Electronic Network of Violence' seminar for teachers (Katowice Police HQ)
- 'Surf Safely in the Internet Cloud' contest for presentation and information spot for parents and family members on the topic of effective and safe use of internet (Kielce HQ and Regional Centre for Teachers, Regional State Office);
- 'Legal and psychological aspects of cybercrime and addictions among children and youth' conference (Rzeszów Police HQ, local government).

In January 2015, the president of the Office of Electronic Communications published the Guide for safe use of electronic means of communication in cyberspace[29] to promote the safe use of electronic means of communication in cyberspace. It aims at revealing the threats posed to every user of cyberspace, the recommended precautions and most popular ways to protect their data and equipment. The guide contains important information about risk mechanisms, the consequences of effective cyber attacks and ways to safeguard facilities and computer systems. The guide also contains a set of information on the most important techniques for computer security, together with practical guidance on how to apply them.

In March 2015, another guide Protecting children from pornography available through Premium Rate services was released[30]. Premium Rate services such as SMS Premium Rate, MMS and Premium Rate Voice Special services are accessed via so-called 'Special numbers', usually four or five-digit SMS/MMS messages starting with the number 7 or the digit 9. Through the Premium Rate services the youngest users can obtain access to different types of content, including sexually explicit content and pornography. In addition, uncontrolled use of Premium services can result in very high telephone bills. The guide is designed to make young people aware of the risks of Premium Rate services.

8.3.2 Public Private Partnership (PPP)

The Police carry out scientific projects in cooperation with the private sector (researchers in the field of implementation of software and tools to combat cybercrime at the AGH University of Science and the Technical University of Warsaw, Polish Platform for Homeland Security). The projects concern the offline test data on the procedural place and programme for the analysis of criminal links.

Examples of police engagement in cooperation with the private sector:

29 https://www.uke.gov.pl/files/?id_plik=18438

30 https://www.uke.gov.pl/files/?id_plik=19323

- The Police Academy in Szczytno is a member of a consortium in an FP7 project: Comprehensive Approach to cyber roadMap coordINation and development (CAMINO) – 2014-2016 O ROB 0003 03 001
- Police officers were members of the consortium in the project CIPS/ISEC: Creation of Polish Centre of Excellence for Research on Cybercrime - 2013-2014 HOME / 2012 / ISEC / INT / 4000003858.

There are plans within the framework of cooperation with the private sector to ensure security in the newly established programming devices, and to take part as a police force in the creation of new technologies in the financial sector. Checks to ensure that an IT solution is crime–proof will be carried out with the PBA.

The Centre for Analytical Intelligence and Excellence to Combat Cybercrime, created on the basis of the Police Academy in Szczytno, works closely with important private companies in cyberspace, including Allegro.pl, PWPW, Fundacja Bezpieczna Cyberprzestrzeń, Matic, Scott Tiger S.A., Stow. Sygnał, ZPAV Warszawa, PwC, VSData and EY.

8.4 Conclusions

- The judiciary, prosecution service and police have a lot of training opportunities in the Tcybercrime field. The National School of Judiciary and Public Prosecution and the Police Academy in Szczytno offer a variety of dedicated courses to the judiciary, prosecution service and police. In addition, dedicated training courses are offered by the CERT POLSKA.

- The National School of Judiciary and Prosecution has organised training in the area of preventing and combating cybercrime since 2009. Despite the good quality of the work being done in this area by the National School of Judiciary and Public Prosecution, training activities are not compulsory. The evaluation team was informed that because of the workload judges and prosecutors find it difficult to attend training actions on a voluntary basis.

- Furthermore, there are no networks of prosecutors and/or judges working with cybercrime cases. Since the area of cybercrime and securing evidence in an IT environment is constantly evolving, an exchange of best practice among practitioners could be of great value.

- The Police Academy in Szczytno organises first, second degrees and postgraduate studies in the field of cybersecurity and combating cybercrime. It also develops specialised training for officers of cyber departments. It also provides training on cybercrime to police cadets. The police also use training opportunities offered by external sources such as Europol or CEPOL.

- Most of the courses offered by the Police Academy in Szczytno are compulsory for police officers. On the other hand the training for the judiciary and prosecution service is not mandatory. Therefore, in the evaluators' view, the possibility of establishing more mandatory training could be useful to raise the level of knowledge of representatives of the authorities dealing with cybercrime.

- Prevention and awareness in the field of cybercrime falls within the administration of different ministries in cooperation with NGOs, mostly based on European grants. All the awareness-raising proposals are filtered, before the final application, by the Ministry of Digital Affairs which is responsible for identifying which proposals are going to apply for grants. However, it seems that there is a need for coordination of awareness/prevention campaigns, not only as regards the persons to whom such campaigns are directed (so as to avoid, for example, that some children attend several courses, and others none), but also as regards content (so as to avoid differing/contradictory messages being given). Moreover, in the evaluators' view it would be useful to involve representatives of the judicial authorities in those campaigns.

- The police have a department dedicated to coordination of the whole set of preventive actions put in place by this law enforcement body. There is not, however, a specific budget allocated to preventive and/or awareness-raising actions.

9 FINAL REMARKS AND RECOMMENDATIONS

9.1 Suggestions from Poland

The Polish authorities take the view that the provision of sufficient financial, staffing and material resources, as well as suitable competence of all law enforcement authorities and courts (judges), are of critical importance to ensure that the fight against cybercrime is effective.

The legislation and procedures in this field have to comply with the fast development of ICT to allow for the monitoring of the cybercrime phenomena and for intensification of cooperation between all stakeholders participating in the fight against cybercrime.
Moreover, the unification of international rules on combating cybercrime and of the legal aspects concerning electronic evidence and its transfer is also important.

From the police perspective, it is important to expand the structure which deals with combating cybercrime together with new IT systems, to develop algorithm processing in cases related to cybercrime, cooperate with the public and private sector in order to increase the security of society, and to increase their knowledge and competence in this field. The police propose of the following actions which could be considered as good practices :

- informing the public about current updated software, including aspects of social engineering, for example information campaigns on the Police website about malware activity and practical guidance on the removal of a virus[31];
- exchange of information relating to law enforcement through national coordinators of the Analysis Work File (AWF); FP Terminal, FP Cyborg, FP Twins;

[31] http://www.policja.pl/pol/kgp/bsk/dokumenty/cyberprzestepczosc/79328,Uwaga-hakerzy-podszywaja-sie-pod-Policje.html. Additionally, information and issues connected with cybercrime and instructions for safe use of the internet are presented on http://www.policja.pl/pol/kgp/bsk/dokumenty/cyberprzestepczosc.

- direct cooperation between Europol contact points enabling access to information about current practices and identification of emerging problems;
- as part of the social awareness arising from the anti-piracy coalition, three organisations
- Association of Audio Video (ZPAV), the 'SIGNAL' Association and the Software Alliance (BSA) - support the activities of the police in the fight against infringements of intellectual property rights. The Police were awarded a 'gold badge' in appreciation of their contribution to combating crimes relating to copyright;
- cooperation and information exchange with the private sector enabling law enforcement authorities to receive information about current trends and risks in the use of new technologies by cyber criminals, and ways of infringing security;
- organisation of training and conferences with the participation of officers from 'Cyber' units of Regional Police Headquarters and the Central Investigation Bureau regional offices, as well as representatives of the private and banking sector, providing a good opportunity to acknowledge the existing procedures for requesting and providing information, presenting tools and solutions, and exchanging methods and techniques for efficiently fighting cybercrime;
- attending many specialist courses in IT forensics and data recovery.

It is worth considering the establishment of network and information security units for the civil sector, in addition to Computer Emergency Response Teams (CSIRTs), which collect data on threats and vulnerabilities and issue guidelines for IT security, as well as specialised units for cybercrime and cyber-defence.

The main challenges mentioned by the police are:

- Bitcoin;
- TOR network – hidden identity;
- Other means of anonymity – proxy servers etc.;
- International legislation – lack of unified legal systems in Member States;
- Security of data in the 'cloud'- user data can be offered on a voluntary basis because they are located outside Poland;
- Lack of qualified staff;
- Expensive training;
- Standardisation of a prevention programme.

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 Poland was able to satisfactorily review the system in Poland.

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

The evaluation team thought it fit to make a number of suggestions for the attention of the Polish authorities. Furthermore, based on the various good practices, some related recommendations are also made to the EU, its institutions and agencies, Europol in particular.

9.2.1 Recommendations to Poland

1. Poland should consider developing a mechanism to provide standardised statistics based on investigation, prosecution, convictions and reported incidents related to cybercrime; (cf. 3.3.2 and 3.5)
2. Poland should enhance coordination of the various authorities involved in cybersecurity and designate one body with the necessary powers to issue guidelines to authorities in charge of cybersecurity and put them into action; (cf. 4.3, 4.4.1 and 4.5)
3. Poland is encouraged to appoint a national CERT at central level which could undertake to coordinate actions with regard to the other CERTs (CERT.GOV.PL, CERT.PL, etc.); (cf. 4.3 and 4.5)
4. Poland should consider establishing a national database on child pornography based on hash values and other techniques in order to avoid having to manually assess each file and to facilitate identification of victims; (cf. 6.2.1 and 6.4)
5. Poland should consider establishing a network for prosecutors to exchange views and/or best practices in the field of cybercrime; (cf. 8.1 and 8.4)
6. Poland should assess the possibility of establishing more mandatory training for prosecutors and judges dealing with cybercrime; (cf. 8.1 and 8.4)
7. Poland is encouraged to establish coordination of the various awareness / prevention campaigns, which are currently carried out individually by the Ministry of Digital Affairs, the Ministry of Education, the Police and other entities; (cf. 8.2 and 8.4).

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

1. Member States should consider establishing or vesting their national CERTs with powers to collect and analyse cyber incidents targeted against public and private domains and the ability to respond to threats, develop early-warning software systems and provide dedicated training on cybercrime and cybersecurity, such as the actions performed by NASK (CERT POLSKA); (cf. 4.3, 4.4.1 and 4.5)
2. Member States are recommended to prepare annual reports of the cyber situation in their country as carried out by the Internal Security Agency and NASK in Poland; (cf. 4.3 and 4.5)
3. Member States should consider setting up specialised units within LEAs to combat cybercrime more effectively both at national and regional/local level as has been developed by the police in Poland; (cf. 4.2 and 4.5)
4. Member States are recommended to develop tools and measures aimed at protecting children and minors from re-victimisation, as performed by the Nobody's Children Foundation; (cf. 6.2.1 and 6.4)
5. Member States are recommended to use public-private partnerships to develop or strengthen cooperation with the financial sector while tackling cybercrime, as has been established with the Polish Bank Association in Poland; (cf. 6.3.2 and 6.4)
6. Member States are recommended to enhance their cooperation with neighbouring countries to strengthen their policy to fight cybercrime, as Poland has done with the Eastern Partnership countries; (cf. 7.1.1 and 7.6)
7. Member States should explore the feasibility of carrying out joint cybercrime training for police officers, prosecutors and judges, like the activity performed by the Police Academy in Szczytno in collaboration with the National School for Judiciary and Public Prosecution in Poland; (cf. 8.1 and 8.4)
8. The EU should work on solutions to improve and speed up the communication process between Member States and third countries, specifically with regard to exchange of operational information and to MLA requests; (cf. 7.3 and 7.6)
9. The EU should consider whether to conclude agreements with big private companies to facilitate cooperation in criminal matters (e.g. Facebook or Google); (cf. 7.4 and 7.6).

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

AGENDA		
DAY I	***01 FEB 2016***	
PM	Arrival of GENVAL experts in Warsaw	
17.30-18.30	Briefing with representatives of the Ministry of Interior and Administration	**Hotel bar**
DAY II	***02 FEB 2016***	
09.00 - 09.30	Transfer from the hotel to the Ministry of Digital Affairs	
09.30-11.00	National cyber security strategic and legislative framework – civilian sphere - Introduction by the Ministry of Digital Affairs - The Cyberspace Protection Policy of the Republic of Poland, actions planned in the future - Governmental Committee for Digitization, A Task Force for the security of cyberspace of the Republic of Poland – Ministry of Digital Affairs - National Critical Infrastructure Protection Programme – the Government Centre for Security - National Security Strategy of the Republic of Poland, the Doctrine of Cyber Security of the Republic of Poland – Ministry of Defense, the National Security Bureau - Questions and comments	**Ministry of Digital Affairs** 27 Królewska street Warsaw with representatives of: **-** the Government Centre for Security, - the National Security Bureau, - Ministry of Defense
11.00-11.15	***COFFEE BREAK***	
11.15-12.45	National cyber security strategic and legislative framework – civilian sphere - Act of February 17, 2005 on the computerization of the activities of entities performing public tasks, Regulation of the Council of Ministers of April 12, 2012 on the national interoperability frameworks – Ministry of Digital Affairs - Act of 16th July 2004 Telecommunications Law with corresponding regulations on security and integrity of telecommunications networks and services - the Polish Office of Electronic Communications - Act of August 29, 1997 on the protection of personal data - General Inspector for Personal Data Protection	**Ministry of Digital Affairs** with representatives of: - the Polish Office of Electronic Communications - General Inspector for Personal Data Protection

	- Act of July 18, 2002 on the electronic provision of services – Ministry of Digital Affairs - Questions and comments	
12.45-13.15	***LUNCH***	
13.15-14.45	Operational aspects of cybersecurity, education, prevention, raising awareness - Main cyber incidents in domain .pl - Research and Academic Computer Network (NASK) - Cyber incidents identified by governmental CERT.GOV.PL – the Internal Security Agency (CERT.GOV.PL) - Prevention measures performed by the plenipotentiaries for cyberspace security – Ministry of Digital Affairs - Educational projects on information security financed by Ministry of Digital Affairs - Questions and comments	**Ministry of Digital Affairs** with representatives of: - Research and Academic Computer Network (NASK), - the Internal Security Agency (CERT.GOV.PL)
DAY III	***03 FEB 2016***	
08.30–09.00	Transfer from hotel to the National Police Headquarters (NPH)	
09.00-09.15	Official welcome by the Commanders of the Polish Police	**The National Police Headquarters**
09.15- 9.45	Introduction to the issue of combating cybercrime, including Police structure, international cooperation and cooperation with private sector and NGOs - Department for Fighting against Cybercrime, Criminal Service Bureau	148/150 Puławska street Warsaw
9.45-10.15	Combating child abuse on-line and off-line: Polish Police perspective and experience including international cooperation – Department for Fighting against Human Trafficking, Criminal Service Bureau	
10.15–10.45	The new modus operandi in the field of card fraud – Department for Fighting against Economic Crime, Criminal Service Bureau	
10.45-11.15	The Polish Banks Association (PBA) cooperation with Polish Police – vice president of the PBA	
11.15-11.30	***COFFEE BREAK***	
11.30-12.00	International information exchange with Europol and Interpol in the field of cybercrime - International Police Cooperation Bureau of the NPH	

12.00-12.30	The role of the Computer Emergency Response Team POL - CERT in the system of cybersecurity of Poland - Bureau of Communication and Information of the NPH	
12.30-13:00	The Police activities in preventing cyber threats – Prevention and Road Traffic Bureau of NPH	
13.00–13.30	The Police Academy in Szczytno input in combating cybercrime	
13.30-14.30	***LUNCH***	
14.30-15.00	Current challenges in the field of cybercrime combating and prevention – Prevention and Road Traffic Bureau of the NPH, Department for Fighting against Cybercrime, Criminal Service Bureau Discussion/Questions	
15.00-15.30	Transfer to the premises of the Department for Combating Cybercrime Central Bureau of Investigation of the Police	
15.30-16.00	*TASKS AND EQUIPMENT OF THE DEPARTMENT FOR COMBATING CYBERCRIME CENTRAL BUREAU OF INVESTIGATION OF THE POLICE* Presentation of the equipment and their tasks	**Central Investigation Bureau of the Police** Taborowa street Warsaw
16.00-16.30	*THE COOPERATION BETWEEN POLICE AND NGOS* Transfer to the Nobody's Children Foundation	
16.30-17.00	Presentation of „friendly rooms" and information about cooperation between the Nobody's Children Foundation and law enforcement in the scope of protecting children from abuse and providing help for abused children	**Nobody's Children Foundation** 12 Mazowiecka street Warsaw
17.00 – 17.30	Transfer to hotel	

DAY IV	***04 FEB 2016***	
9.15 – 10.45	Judicial and legislative framework for prevention and combating cybercrime	**Ministry of Justice** 11 Aleje Ujazdowskie street Warsaw
10.45 – 11.00	***COFFEE BREAK***	
11.00 – 11.30	Overview of courts statistics on cybercrime	
11.30 – 12.30	International judicial cooperation in the field of cybercrime	
12.30 – 13.30	***LUNCH***	
13.30 – 14.00	Overview of prosecution statistics on cybercrime	**Ministry of Justice**
14.00 – 15.30	Role of the Prosecution Service in combating cybercrime – presentation of case studies	with the representatives of **the Prosecution General**
15.30-15.45	***COFFEE BREAK***	
15.45 – 16.15	Judicial training on prevention and combating cybercrime	
19.30-22.00	***DINNER***	
DAY V	***05 FEB 2016***	
9.30-10.00	Start up with coffee	**Ministry of Interior and Administration** 5 Batorego street Warsaw
10.00-11.30	Closed session for Genval experts and/or possibility for extra exchange of views, interviews, etc.	
11.30	Transfer to the airport	

Annex B: Persons interviewed/met

Meeting 2 February 2016

Venue: Ministry of Digital Affairs, Warsaw

Person	Function/Organisation represented
Paweł Wiszniewski	Expert, National Security Bureau
Maciej Pyznar	Head of Unit, Government Centre for Security
Jarosław Łuba	Counsellor of the Minister, Ministry of Digital Affairs
Magdalena Wrzosek	Expert, Ministry of Digital Affairs
Maciej Groń	Director, Ministry of Digital Affairs
Marek Jurkiewicz	Head of Unit, Office of Electronic Communications
Paweł Makowski	Deputy Director, Inspector General for Personal Data Protection
Piotr Kijewski	Head of CERT POLSKA, NASK
Monika Pieniek	Chief expert, Ministry of Digital Affairs
Łukasz Olszewski	Senior expert, Ministry of Interior and Administration

Meetings 3 February 2016

Venue: National Police Headquarters, Warsaw

Person	Function/Organisation represented
Lt Col. Andrzej Szymczyk	Deputy Chief Commander of the Police
Col. Natalia Rost	Director of the Criminal Service Bureau of the NPH
Col. Renata Skawińska	Commander of the Central Investigation Bureau of Police
Maj. Irmina Gołebiewska	Deputy Director of the International Police Cooperation Bureau of the NPH
Lt Col. Marcin Golizda – Bliziński	Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Lt. Ph.D. Aneta Trojanowska	Deputy Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Lt Col. Jerzy Kosiński	Police Academy in Szczytno

Person	Function/Organisation represented
Cpt. Jarosław Kończyk	Department for Fighting Against Human Trafficking, Criminal Service Bureau of the NPH
2d WO Marta Krakowian	Department for Fighting Against Economic Crime, Criminal Service Bureau of the NPH
Maj. Marzena Kordaczuk- Wąs	Prevention and Road Traffic Bureau of the NPH
Lt. Marcin Kuskowski	IT and Communication Bureau of the NPH
Lt. Marcin Szlechta	Department for Combating Cybercrime, Central Investigation Bureau of Police
Gabriela Kuhn	Nobody's Children Foundation
Executive Vice President Polish Bank Association Ph.D. Mieczysław Groszek	The Polish Banks Association (PBA) cooperation with Polish Police
Martyna Różycka	Team Leader, Dyżurnet.pl
Łukasz Olszewski	Senior expert, Ministry of Interior and Administration
Izabela Iglewska	Senior expert, Ministry of Interior and Administration
Rafał Kierzynka	Judge, Department of Legislation, Ministry of Justice
Kuba Sękowski	Legal Counsel, Chief Expert, Department of Legislation, Ministry of Justice

Meeting 4 February 2016

Venue: Ministry of Justice, Warsaw

Person	Function/Organisation represented
Rafał Kierzynka	Judge, Department of Legislation, Ministry of Justice
Kuba Sękowski	Legal Counsel, Chief Expert, Department of Legislation, Ministry of Justice
Kazimierz Ujazdowski	Senior Expert, Department of Legislation, Ministry of Justice
Małgorzata Pawelec	Head of Coordination Unit, Department

Person	Function/Organisation represented
	of Legislation, Ministry of Justice
Magdalena Wójcikowska-Izdebska	Senior Expert, Department of Legislation, Ministry of Justice
Sławomir Piwowarczyk	Prosecutor, Prosecution General Office
Jacek Łazarowicz	Prosecutor, Prosecution General Office
Jacek Bilewicz	Prosecutor, Prosecution General Office
Konrad Gołębiowski	Prosecutor, Appellate Prosecutor's Office in Warsaw
Beata Klimczyk	Prosecutor, National School of Judiciary and Public Prosecution
Janusz Konecki	Judge, National School of Judiciary and Public Prosecution
Izabela Iglewska	Senior expert, Ministry of Interior and Administration
Łukasz Olszewski	Senior expert, Ministry of Interior and Administration
Lt Col. Marcin Golizda – Bliziński	Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Lt. Ph.D. Aneta Trojanowska	Deputy Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH

Meeting 5 February 2016

Venue: Ministry of Interior and Administration, Warsaw

Person	Function/Organisation represented
Łukasz Olszewski	Senior expert, Ministry of Interior and Administration
Izabela Iglewska	Senior expert, Ministry of Interior and Administration
Rafał Kierzynka	Judge, Department of Legislation, Ministry of Justice
Jarosław Łuba	Counsellor of the Minister, Ministry of Digital Affairs
Maj. Irmina Gołebiewska	Deputy Director of the International Police Cooperation Bureau of the NPH

Lt Col. Marcin Golizda – Bliziński	Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Lt. Ph.D. Aneta Trojanowska	Deputy Head of the Department for Fighting Against Cybercrime, Criminal Service Bureau of the NPH
Cpt. Jarosław Kończyk	Department for Fighting Against Human Trafficking, Criminal Service Bureau of the NPH
2d WO Marta Krakowian	Department for Fighting Against Economic Crime, Criminal Service Bureau of the NPH
Maj. Marzena Kordaczuk- Wąs	Prevention and Road Traffic Bureau of the NPH
Lt. Marcin Kuskowski	IT and Communication Bureau of the NPH
Jacek Bilewicz	Prosecutor, Prosecution General
Konrad Gołębiowski	Prosecutor, Appellate Prosecutor's Office in Warsaw
Sławomir Piwowarczyk	Prosecutor, Prosecution General

Annex C: List of abbreviations/glossary of terms

List of acronyms, abbreviations and terms	Full name in English	Acronym in Polish or original language	Full name in Polish
CAM	Child Abuse Material		
CCP	Code of Criminal Procedure	KPK	Kodeks Postępowania Karnego
CI	Critical Infrastructure	IK	Infrastruktura Krytyczna
CSE	Child Sexual Exploitation		
ENLETS	ENLETS		the European Network of Law Enforcement Technology Services
ENU	Europol National Unit	ENU	Krajowa Jednostka Europolu
GCD	Governmental Committee for Digitalization	KRMC	Komitet Rady Ministrów ds. Cyfryzacji
ISA	Internal Security Agency	ABW	Agencja Bezpieczeństwa Wewnętrznego
ISP	Internet Service Provider		
MDA	Ministry of Digital Affairs	MC	Ministerstwo Cyfryzacji
MIA	Ministry of Interior and Administration	MSWiA	Ministerstwo Spraw Wewnętrznych i Administracji
MND	Ministry of National Defence	MON	Ministerstwo Obrony Narodowej
NASK	Research and Academic Computer Network	NASK	Naukowa i Akademicka Siec Komputerowa
NBP	National Bank of Poland	NBP	Narodowy Bank Polski

List of acronyms, abbreviations and terms	Full name in English	Acronym in Polish or original language	Full name in Polish
NPIS	National Police Information System	KSIP	Krajowy System Informacji Policji
NPH	National Police Headquarters	KGP	Komenda Główna Policji
NPIS	National Police Information System	KSIP	Krajowy System Informacyjny Policji
OEC	Office of Electronic Communications	UKE	Urząd Komunikacji Elektronicznej
PC	Penal Code	KK	Kodeks Karny
PG	Prosecution General	PG	Prokuratura Generalna

Annex D: The Polish Legislation

The provisions of Penal Code (dated June 6, 1997) regarding combatting cybercrime:

Article. 190a.

§ 1. Who by the persistent harassment of another person or persons, its nearest stirs in her circumstances justified sense of danger or indeed violates her privacy, shall be punishable by imprisonment for 3 years.

§ 2. The same punishment shall be subject to the who, pretending to be another person, uses her image or other personal data for the purpose of causing her injury or personal.

§ 3. If the consequence of the Act specified in § 1 or 2 is make an attempt on one's life by victim, the offender shall be imprisonment from one year to 10 years.

§ 4. The prosecution of the offence specified in § 1 or 2 followed by at the request of the victim.

Article. 200.

§ 1. Who sexually communion with minors below 15 years or allow such person to another sexual act or brings it to undergo such an operation or to execute them, shall be punishable by imprisonment from 2 to 12 years

§ 3. Who juvenile less than 15 years presents a pornographic content or provides him with items of such a nature or disseminate pornographic content in such a way that such juvenile to become acquainted with them, shall be punishable by imprisonment for 3 years.

§ 4. The penalty referred to in section 3 shall be subject to, who to his sexual gratification, or sexual gratification of another person presents juvenile below 15 years implementation of the sexual act.

§ 5. The penalty referred to in section 3 shall be subject to, who runs the advertising or promotion of business of distributing pornographic content in such a way as to become acquainted with them juvenile below the age of 15.

Article. 200A.

§ 1. Who in order to commit the offences referred to in article 1. 197 § 3 paragraph 2 or article. 200, as well as the manufacture or the perpetuation of pornographic content, through an it system or telecommunications network contacts with minors below the age of 15, in order, by means of the introduction of it, exploiting an error or inability to comprehend the situation either by using the threat of unlawful, to meet with him, shall be punishable by imprisonment for 3 years.

§ 2. Who through the it system or telecommunications network juvenile below 15 years includes a proposal for associating, surrender or another sexual act or participate in production or perpetuating pornography, and tends to its implementation shall be subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

Article. 200B

Who publicly propagates or applauds the behaviour of an paedophile, is subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

Article. 202.

§ 1. Who publicly presents a pornographic content in such a way that it can impose their receipt to the person who you do not wish, shall be subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 3. Who to distribute produces, perpetuates or comes down, keeps or has or disseminates or presents pornography involving a minor or pornographic content related to the presentation of violence or handling the animal, shall be punishable by imprisonment from 2 to 12 years.

§ 4. Who perpetuates the pornography involving a minor, shall be punishable by imprisonment from one year to 10 years.

§ 4a. Who holds, has or obtains access to pornography involving a minor, shall be punishable by imprisonment from 3 months to 5 years.

§ 4b. Who produces, disseminates, shows, stores or have pornographic content depicting manufactured or processed image of a minor involved in the sexual act is subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 4 c. The penalty referred to in section 4b shall be subject to the who for the purpose of sexual gratification involved in pornographic presentations involving a minor.

§ 5. The Court may declare the forfeiture of tools or other objects, which served or were designed for committing the offences referred to in § 1-4b, even if they do not constitute the property of the offender.

Article. 256. §1. Whoever publicly promotes a fascist or other totalitarian regime, Member States or calls for hatred against the background of ethnic differences, ethnic, racial, religious, or due to the non-religion, is subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 2. The same punishment shall be subject to the who for distribution produces, perpetuates or comes down, acquires, stores, showcases, carries or transmits printing, recording or any other object containing the content referred to in § 1, or being a carrier of the symbolism of fascist, Communist or other totalitarian.

§ 3. Does not commit a crime the perpetrator of the criminal act referred to in

§ 2, if he is guilty of the Act in respect of the artistic, educational, scientific, or a collector's Edition.

§ 4. In the event of a conviction for an offence referred to in § 2, the Court shall order the forfeiture of the items referred to in § 2, even if they do not constitute the property of the offender.

Article 267.

§ 1. Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

§ 2. The same punishment shall be imposed on anyone, who, in order to acquire information to which he is not authorised to access, installs or uses tapping, visual detection or other special equipment.

§ 3. The same punishment shall be imposed on anyone, who imparts to another person the information obtained in the manner specified in § 1 or 2 discloses to another person.

§ 4. The prosecution of the offence specified in § 1 – 3 shall occur on a motion of the injured person.

Article. 268.

§ 1. Who, without being entitled to do so, destroys, damages, deletes, or modifies the record material information or otherwise thwarts, or significantly impedes a person empowered to become acquainted with it, is subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 2. If the Act specified in § 1 applies to information on data medium, the perpetrator shall be subject to imprisonment for 3 years.

§ 3. Who, while allowing to act referred to in § 1 or 2, causing significant damage to property, shall be punishable by imprisonment from 3 months to 5 years.

§ 4. The prosecution of the offence specified in § 1-3 followed by at the request of the victim.

Article. 268a.

§ 1. Who, without being entitled to do so, destroys, damages, removes, alters, or impedes the access to computer data or substantially interferes with or prevents automatic processing, collection or transmission of such data, shall be punishable by imprisonment for 3 years.

§ 2. Who, while allowing to act referred to in § 1, causing significant damage to property, shall be punishable by imprisonment from 3 months to 5 years. § 3. The prosecution of the offence specified in § 1 or 2 followed by at the request of the victim.

Article. 269.

§ 1. Whoever destroys, damages, deletes, or modifies the information data of particular interest to national defence, security, the functioning of the Government, other State body or institution of the State or local government or disrupts or prevents automatic processing, collection or transmission of such data, shall be punishable by imprisonment from 6 months to 8 years.

§ 2. The same punishment shall be subject to, who may be an act referred to in § 1, destroying or replacing data media information or destroying or damaging the device for automatic processing, storage or transmission of computer data.

Article. 269a.

Who, without being entitled to do so, by transmission, destruction, removal, damage, making it more difficult to access or change the data, it substantially interferes with the work of the computer system or the ICT network, shall be punishable by imprisonment from 3 months to 5 years.

Article. 269b.

§ 1. Who produces, acquires, disposes of or make available to others the device or computer programs designed for committing the offence referred to in article 1. 165 section 1, paragraph 4, art. 267 § 3, art. section 268a 1 or § 2 in conjunction with § 1, art. 269 section 2(1) or article. 269a, as well as computer passwords, access codes or other data used to access information stored on a computer system or network communication shall be subject to imprisonment for 3 years.

§ 2. In the event of a conviction for an offence referred to in paragraph 1, the Court shall order the forfeiture of the items specified therein, and declare their forfeiture, if they do not constitute the property of the offender.

Article. 271.

§ 1. A public officer or other person authorized to issue a document, which certifies the truth in it as to the circumstances of the relevant law, punishable by imprisonment from 3 months to 5 years.

§ 2. In the case of a minor, the perpetrator shall be subject to a fine or penalty of restriction of liberty.

§ 3. If the perpetrator of an act may be referred to in paragraph 1 in order to achieve material advantage or personal, shall be punishable by imprisonment from 6 months to 8 years.

Article. 286.

§ 1. Who, in order to achieve the material benefits, brings another person into the negative regulation of their own or someone else's property with the introduction of its error or exploiting error or inability to sound understanding of action, shall be punishable by imprisonment from 6 months to 8 years. § 2. The same punishment shall be subject to who requests the material benefits in return for reimbursement of wrongly took things. § 3. In the case of a minor, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or imprisonment for 2 years.

§ 4. If the Act specified in § 1-3 has been committed to the detriment of the person nearest, prosecution follows at the request of the victim.

Article 287.

§ 1. Whoever, in order to gain material benefits, affects automatic processing or transmitting information, or changes or deletes record or introduces a new record on an electronic information carrier, without being authorised to do so, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 2. In the event that the act is of a lesser significance, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year.

§ 3. If the fraud has been committed to the detriment of a next of kin, the prosecution shall occur on a motion of the injured person.

Article 294.

§ 1. Whoever commits the offence specified in Article 278 § 1 or 2, Article 284 § 1 or 2, Article 285 § 1, Article 286 § 1, Article287 § 1, Article 288 § 1 or 3, or in Article 291 § 1, with regard to property of considerable value shall be subject to the penalty of deprivation of liberty for a term of between 1 and 10 years.

§ 2. The same punishment shall be imposed on the perpetrator who commits the offence specified in § 1 with regard to a property of significant cultural value.

Article 310.

§ 1. Whoever counterfeits or alters Polish or foreign money, other legal tender, or a document which entitles one to obtain a sum of money or contains an obligation to pay capital, interest, share of profits, or verifies a share in a company, or whoever removes a sign of cancellation from money, other legal tender or from such document shall be subject to the penalty of deprivation of liberty for a minimum term of 5 years or the penalty of deprivation of liberty for 25 years.

§ 2. Whoever releases into circulation money or other legal tender or document as specified in § 1 or for such purpose receives, stores, transports, carries, dispatches it or assists in selling or concealing it shall be subject to the penalty of deprivation of liberty for a term of between 1 and 10 years.

§ 3. In the event that the act is of a lesser significance, the court may apply an extraordinary mitigation of the penalty.

§ 4. Whoever makes preparations to commit the offence specified in § 1 or 2 shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

List of Polish provisions corresponding with crimes defined in Table 2 of the questionnaire – annex to the answer to question 2A.1 with comments.		
Acts unique to information systems, in particular those related to cyber attacks	Illegal access to information system	PC, Art. 267 (1): 1. Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.
		Comments: This offence may only be committed intentionally (both direct intent or potential intent are possible). Penalties for committing an offence defined in art. 267 (1) of the PC are: fine, the penalty of restriction of liberty (between 1 month and 3 years) or the penalty of deprivation of liberty (from 1 month) for up to 2 years. Attempt to commit an offence defined in art. 267 (1) of the PC is punishable.
	Illegal system interference	PC, Art. 269a: Whoever, without being authorised to do so, by transmitting, damaging, deleting, destroying or altering information data, significantly disrupts a computer system or telecommunications network shall be subject to imprisonment for three months to five years.
		Comments: This offence may only be committed intentionally (both direct intent or potential intent are possible). Penalty for committing an offence defined in PC, Art. 269a is a deprivation of liberty between 3 months and 5 years. Attempt to commit an offence defined in PC, Art. 269a is punishable.
	Illegal data interference	PC, Art. 268a: 1. Whoever, without being authorised to do so, destroys, damages, deletes or alters or hinders access to information data, or who hinders or prevents the automatic collection and transmission of such data shall be subject to imprisonment for up to three years. 2. Whoever, by committing the offence specified in § 1, causes a significant loss of property shall be subject to imprisonment for between three months and five years.
		Comments: This offences may only be committed intentionally (both direct intent or potential intent are possible). Penalty for committing an offence defined in PC, Art. 268a (1) is a deprivation of liberty (from 1 month) for up to 3 years and, in case of qualified type defined

		in PC, Art. 268a (2) the penalty is a deprivation of liberty between 3 months and 5 years. Attempt to commit an offences defined in PC, Art. 268a is punishable.
	Illegal interception of computer data	Same as illegal access to information system.
	Misuse of devices - production, distribution, procurement for use, import or otherwise making available or possession of computer misuse tools	PC, Art. 269b.1: 1. Whoever creates, obtains, transfers or allows access to hardware or software adapted to commit the offences specified under Article 165 § 1 section 4, Article 267 § 2, Article 268a § 1 or § 2 in connection with § 1, Article 269 § 2 or Article 269a, including also computer passwords, access codes or other data enabling access to the information collected in the computer system or telecommunications network shall be subject to imprisonment for up to three years.
		Comments: This offence may only be committed intentionally (both direct intent or potential intent are possible). Penalty for committing an offence defined in PC, Art. 269b is a deprivation of liberty (from 1 month) for up to 3 years. Attempt to commit an offence defined in PC, Art. 269b is punishable. Forfeiture of assets: PC, Art. 296b (2) In the event of a conviction for the offence specified in § 1, the court orders the forfeiture of the items referred to therein, and may order the forfeiture even if they do not constitute the property of the offender.
Content-related acts, in particular those related to child sexual abuse online and child pornography	Computer-related production, distribution or possession of child pornography	PC, Art. 202 (1), (3), (4a) and (4b) 1. Whoever publicly presents pornographic material in such a manner that it is imposed upon a person who may not wish so shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year. 3. Whoever for the purpose of dissemination produces or imports or stores, possesses, distributes or presents pornographic material, in which minors participate, or pornographic material associated with the use of violence or the use of an animal shall be subject to the penalty of the deprivation of liberty for a term of between 2 and 12 years. 4a. Whoever stores, possesses or obtains access to pornographic content involving a minor shall be punished by the deprivation of liberty for a term of 3 months to 5 years. 4b. Whoever manufactures, distributes, presents, stores or possesses pornographic material containing

		a generated (fabricated) or transformed (processed) image of a minor image of a minor participating in sexual activity shall be punishable by a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to two years.
		Comments: This offences may only be committed intentionally (both direct intent or potential intent are possible). However, the offence defined in PC, Art. 202 (3) requires a direct intent – acting for the purpose of dissemination. Penalty for committing an offences related to child sexual abuse and exploitation vary between particular types of offences. Attempt to commit an offences defined in PC, Art. 202 is punishable. According to the nomenclature of the PC a person who has not reached 18 years is described as a "minor". Term "child" is not used for this purpose.
	Computer-related solicitation or "grooming" of children	PC, Art. 200a: 1. Whoever, in order to commit the offence specified in Article 197 § 3 section 2 or Article 200, as well as for the purpose of producing or preserving pornographic materials, by an information system or telecommunications network, establishes a connection with a minor under the age of 15, with the intention of using deceit or an illegal threat to meet with him or her, shall be subject to imprisonment for up to three years. 2. Whoever, through an information system or telecommunications network, makes an offer to a minor under the age of 15 of sexual intercourse, submission or performance to another sexual act, or participation in the production or preservation of pornographic material and intends to carry through this offer, shall be subject to a fine, the restriction of liberty or imprisonment for up to two years.
		Comments: This offences may committed intentionally (a direct intent – a purpose of producing or preserving pornographic materials – is required under PC, Art. 200a (1), and a material act leading to meeting with a child is required under PC, Art. 200a (2)). Penalty for committing an offence defined in art. 200a (1) is imprisonment for up to three years, and relation to the offence defined in art. 200a (1) – a fine, the restriction of liberty or imprisonment for up to two years. Attempt to commit aforementioned offences is punishable. According to the nomenclature of the PC a person who has not reached 18 years is described as a "minor". Term "child" is not used for this purpose.

Acts where computer/IT systems were involved as tool or target, in particular online card fraud	Computer-related	forgery	The conduct described as "computer-related forgery" falls under definition of forgery set out in the PC, Art. 270 (1) – material forgery and Art. 271 (1) – intellectual forgery: PC, Art. 270 (1): 1. Whoever forges, counterfeits or alters a document with the intention of using it as authentic, or who uses such a document as authentic, is liable to a fine, the restriction of liberty or imprisonment for between three months to five years. PC, Art. 271 (1): 1. A public official, or another person authorised to issue a document, who certifies an untruth therein, in circumstances of legal significance, is liable to imprisonment for between three months and five years.
			Comments: This offences may committed intentionally (a direct intent – an aim to use a forged document as it was authentic – is required under PC, Art. 270 (1)). Penalty for committing an offence defined in art. 270 (1) and 271 (1) of the PC is a deprivation of liberty between 3 months and 5 years. In case of forgery (PC, Art. 2710 (1)) penalties of fine and restriction of liberty are also foreseen. Attempt to commit aforementioned offences is punishable. The term "document" (used in PC, Art. 270 and Art. 271) is defined in the PC, Art. 115 (14) as: an object or record on a computer data carrier to which is attached a specified right, or which, in connection with the subject of its content, constitutes evidence of a right, a legal relationship or a circumstance that may have legal significance.
		fraud	Article 287 (1) of the PC: 1. Whoever, in order to gain material benefits, affects automatic processing or transmitting information, or changes or deletes record or introduces a new record on an electronic information carrier, without being authorised to do so, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years
			Comments: This offence may only be committed intentionally (a direct intent – an aim of gaining material benefits is required). Penalty for committing an offence defined in art. 287 (1) of the PC is a deprivation of liberty between 3 months and 5 years. Attempt to commit an offence defined in art. 287 (1) of the PC is punishable. Privileged type of the offence: PC, Art. 287(2) § 2. In the event that the act is of a lesser significance, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year.

	Computer-related identity offences	The conducts described as "computer-related identity offences" fall under the definition of forgery or fraud.
	Sending or controlling sending of Spam	Art 24 (1) of the Act of 18th of June 2002 on services provided through ICTs: Who sends by means of electronic communication unsolicited commercial, shall be subject to a fine.
		Comments: The conduct defined in aforementioned provision is a petty offence. The attempt to commit this offence is not punishable.