Council of the
European Union

Brussels, 5 April 2016
(OR. en)

5156/1/16
REV 1 DCL 1

GENVAL 2
CYBER 2

DECLASSIFICATION

of document:	5156/1/16 REV 1 RESTREINT UE/EU RESTRICTED
dated:	8 March 2016
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 Bulgaria

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, 8 March 2016
(OR. en)

5156/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 2
CYBER 2

REPORT

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

ANNEX

Table of Contents

1. EXECUTIVE SUMMARY

The evaluation visit was well organized and prepared by the Bulgarian authorities. The selection of authorities visited and participants meet was quite appropriate. However, the experts' team felt that a meeting with the representatives of the Specialised Prosecution Office would have been necessary in order to fully understand the repartition of tasks between different prosecution offices regarding cybercrime cases and to receive a feedback regarding the practical issues related to the prosecution of these cases. Nevertheless, the Bulgarian authorities provided additional information on the legal basis for the functioning and the structure of the Specialized Prosecutor's Office after the visit.

Bulgaria set up a multidisciplinary working group, with the participation of representatives of the institutions and academic sector, in charge with drafting the National Cybercrime Security Strategy. The model chosen is close to the guidelines of ENISA Practical Guide on Development and Execution of National Cyber Security Strategies.

There are no centralised statistics on cybercrime at national level, statistics are gathered and compiled by the competent institutions (Ministry of Interior, Supreme Prosecution Office) and by some non-governmental organizations.

At the investigation level, Bulgaria has a specialised cybercrime unit within Chief Directorate Combating Organized Crime dealing with a part of cybercrime cases. The investigating competence is split in special competence for the cybercrime cases that are qualified as organized crimes and the ordinary competence of the police units for the rest of the cybercrime cases.

At the judicial level, there are not any specialized prosecution office or courts in Bulgaria dealing only with cybercrime cases.

Bulgaria ratified the Council of Europe Convention on cybercrime. Bulgaria has transposed into the national legislation the Directive 2011/92/EU on combating sexual abuse and sexual exploitation of children and child pornography. The relevant amendments to the Penal Code were adopted by the National Assembly on 17 September 2015 and published in the State Gazette no. 74 of 26 September 2015. Bulgaria has not yet transposed the Directive 2013/40/EU on attacks against information system but an interdepartmental working group, including the Ministry of Justice, is working on the legislative amendments necessary to transpose this directive.

Regarding the measures countering websites containing or disseminating child pornography, national authorities can remove them, if they are located on their territory or block access to them, if they are located outside their territory.

In terms of international cooperation Bulgaria make good use of JITs, which it considered an effective tool for timely collection of evidence, for reducing the time for investigations and for enhancing mutual trust.

Bulgaria has a good cooperation with Europol, Eurojust, Interpol and also with the private sector. There is still room to further develop the training within the area of cybercrime. Until now, the National Institute of Justice has provided some training for a number of judges and prosecutors and there is also an NGO actively involved in training activities for police officers and prosecutors. Work should be continued in order to ensure the proper training for all the practitioners, especially being that there are not specialised prosecutors or judges in cybercrime. Bulgaria benefited for some European funding but a larger involvement of the Bulgarian authorities (financial or logistical) in training, would be of great use.

Bulgaria organises awareness activities on a quite regular basis. Both institutions and NGOs organise raising awareness of the population about different forms of cybercrime, especially for children, as they are the most vulnerable category.

2. INTRODUCTION

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

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which member States felt warranted particular attention. To this end, the evaluation covers three specific areas - cyber attacks, online child sexual abuse/pornography and online card fraud - and should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA[2] (transposition deadline 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems and replacing Council framework Decision 2005/222/JHA (transposition deadline 4 September 2015), are particularly relevant in this context.

1 Joint Action of 5 December 1997 (97/827/JHA), OJ L 34, 15.12.1997, p. 7-9
2 OJ L 35, 17.12.2011, p.1
3 OJ L 218, 14.08.2013, p. 8

Moreover, the Council Conclusions on the EU Cybercrime Strategy of June 2013[4] anticipated the swift ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 by all Member States and emphasised in their preamble that "the EU does not call for the creation of new international legal instruments for cyber issues". The Convention is supplemented by a Protocol on acts of xenophobia and racism committed through computer systems.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Bulgaria is the tenth Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request to delegations from the Chairman of GENVAL on 28 January 2014. The evaluation teams consist of three national experts, supported by two staff from the General Secretariat of the Council and observers. For the seventh round of mutual evaluations, GENVAL agreed with the proposal from the Presidency that the European Commission, Eurojust, ENISA and Europol/EC3 should be invited as observers.

The experts charged with undertaking the evaluation of Bulgaria were Mr. Jan Tibbling (Sweden), Mr. Emmanuel Kessler (France) and Ms. Carmen Barquilla Bermejo (Spain). From the General Secretariat of the Council there present Mrs Claire Rocheteau and Mrs Carmen Necula.

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 Bulgaria between 22 and 25 June 2015, and on the detailed replies from Bulgaria to the evaluation questionnaire, together with their detailed answers to ensuing follow-up question.

[4] 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTEC T94

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

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

Reforms of legal and political tools are currently in progress.
Currently an intergovernmental working group comprising representatives of the Ministry of Interior, the Ministry of Foreign Affairs, the State Agency for National Security, the State Agency for Technical Operations, the Commission on Personal Data Protection, the Ministry of Transport, Information Technologies and Communications, the Ministry of Defence, the Ministry of Justice, the Bulgarian Academy of Science and the representatives of universities, is developing the draft of a National Cyber Security Strategy.

The draft is following the guidelines in the ENISA Practical Guide on Development and Execution of National Cyber Security Strategies.

The national authorities clarified during the evaluation visit that the draft Strategy will be finalised and adopted at the end of this year. The process has been on going for a few years but it is not yet finalised. However, following the ENISA recommendations, Bulgarian authorities decided to follow a different and open approach (previously the strategy was classified). The coordination of the intergovernmental working group is ensured by the Ministry of Defence.
Some non-governmental organizations are also interested in the drafting process and in the public debate on the National Cyber Security Strategy, as for example, the International Academy for Cyber Investigations (ICITA), who considers that Bulgarian government should openly promote cyber security as governmental priority and that private sector should have some major position in drafting the national strategy.

The adoption of the strategy is also to impulse the reform of the Criminal Code, which is still on expectation. The future Criminal Code should allow tackle cybercrimes in a better and more efficient way.

After the evaluation visit, Bulgaria updated the state of progress of the National Cyber Security Strategy drafting, as follows:

The intergovernmental working group is chaired by the National Cybersecurity Coordinator and is set up at expert level in order to be ensured the necessary expertise. Nevertheless, the political management of the represented institutions is regularly involved and provides the overall overview on the activity of the group.

The group will draft the structure of the National Cyber Security Strategy, which will be further discussed and finalized with representatives of non-governmental organizations in the field of IT, industry, education and critical infrastructure.

The draft should be prepared in the end of August 2015 and an Action Plan to the Strategy should be prepared until the end of November 2015.

The draft will be discussed within the National Security Council as well as with international stakeholders: Member States, EU Agencies, international non-governmental organizations etc.

3.2. National priorities with regard to cybercrime

Prevention of all types of crime and developing and implementing policies in the field of cyber security are among the main priorities of the government. A special emphasis is put on the active international cooperation taking into account that the digital space does not recognize borders. A number of information campaigns were carried out in the last 3 years, aimed at raising the awareness about the internet threats. They were organized by the Ministry of Interior - within a project under the ISEC Program and by non-government organizations, including B2CENTER. Bulgaria is actively participating both in the previous and current EMPACT project on cybercrime within the EU Policy cycle. The Bulgarian officials participate in the three sub-priorities and the strategic goals of the country are harmonized with the strategic goals of the Policy cycle.

The issues of prevention, legislation, capacity building, training, public awareness and international co-operation are intended to be covered by the national strategy.

During the evaluation visit, the national authorities underlined that the Cyber Security Strategy is aiming to prevent, for example, the increasing of the number of criminal offences such as skimming and credit cards fraud, so as to attract foreign investors in Bulgaria.

The next national strategy will also cover issues of legislation, capacity building, training, public awareness and international co-operation. It should be linked with fight against cybercrime, but up-to-date, the main priorities are :
- prevention against crime, which is set out as major priority according to the Law on the Ministry of Interior;

- raising the awareness about the Internet threats through information campaigns[6] as carried out in the last 3 years and by the creation of an official platform[7] so as to support public awareness and victims reporting to law enforcement services;
- combating cybercrime, considering the Chief Directorate Combating Organized Crime (CDCOC) as the main investigating authority working in coordination with the special prosecutor department for organized crime. Other local or financial police forces are also involved in cybercrimes investigations, which are not connected to organized crime.
- an active international cooperation, favoring the use of the EU institutions, like Eurojust and Europol. Bulgarian authorities do also favor the EU (Europol-Eurojust-Enisa) support, through JITs.

Bulgaria is actively participating in the EMPACT project on cybercrime within the EU Policy cycle. Police forces participate in the three sub-priorities of the EMPACT project (skimming, child pornography and cyber-attacks). Consequently, the strategic goals of the Policy cycle are taken in consideration in the strategic goals of the country.

3.3. Statistics on cybercrime

Currently Bulgaria has increased its Internet access rate up to 60% of population, which constitutes a progress but in the same time can increase the rate of cyber criminality.
The statistics on cybercrime in Bulgaria are gathered and compiled in a decentralized way by the competent government and non-government organizations. The Ministry of Interior - Cybercrime Unit in CDCOC - is collecting and analysing information in it's data bases. Concrete and accurate data on the number of initiated pre-trial proceedings, indictments, detained persons, sentences, court decisions regarding computer crime are kept by the Bulgarian Supreme Prosecutor's Office of Cassation.

[6] The information campaigns were organized by the Ministry of Interior - within a project under the ISEC Programme and by non-governmental organizations, including B2CENTER.
[7] www.cybercrime.bg

Gathered statistics seem not to be complete. There is no data about the number of victims complaints nor victim's number.
If violence against minors on the Internet is assessed as increasing by the NGOs (grooming, cyberbullying, sexting, revenge porn), these offences seem to be barely reported to the justice.
Concerning computer fraud, some cases may not be reported to the competent authorities, while reporting depends on the good will of citizens or companies who normally receive compensations from the banks and therefore does not file complaints to the competent authorities.
During the evaluation visit, the national authorities informed the evaluation team about the main trends in cybercrime. According to their assessment, the main criminal activities in the field of cybercrime in the recent years include:

- unauthorized accesses;
- defaces;
- denying access attacks on government and corporate sites;
- interception and alteration of messages in company mailboxes, aimed at ordering undue payments (Spear Phishing);
- dissemination of pornographic material involving children;
- infecting computer configurations of government and private organizations with malicious software (CryptoLockerCTB);
- violations of intellectual property rights (IPR) on the Internet in respect of films, music, software, etc.

Skimming is a major criminal cyber activity, where local criminals are linked to other Bulgarian citizens based abroad (Dubaï, North America, other EU Member States). Bulgarian citizens may also be involved in illegal financial activities on the Internet with Ukraine, China, Russia. Bulgarian companies or citizens were also targeted by fraud attempts from Nigeria.

Although the national authorities alleged that both government and non-government organizations gather data in a decentralised manner, they provided only the relevant statistics kept by the Bulgarian Supreme Prosecutor's Office of Cassation in respect of computer crimes.

During the evaluation visit, the experts' team found that local authorities were also able to provide statistics data. For example, according to the representatives of Plovdiv Prosecution District, in the last 5 years, they were 21 cases of intrusion/data theft, 17 cases of computer fraud (only one has been brought to trial, the others falling victim to the delays involved in international mutual assistance in criminal matters: victims are not identified, or are not interviewed in time), 22 cases related to child pornography (especially upload and distribution of child pornography content) and only one case related to child pornography production.

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

In the state budget for the current year specific funding has been allocated for co-financing. In the recent years financing has been ensured from EU funds under the ISEC Programme grants. Relevant project proposals are also elaborated within the ISF 2014-2020 where the provided funding is 8 million euros. At the same time the Forensic Institute within the Ministry of Interior is launching a large-scale project with funding of 350 000 euros.

The non-governmental organization - National Centre for Safer Internet - considers that the decrease of co-funding by the European Commission from 75% to 50% affects the quality of its activities. The NGO is obliged to find co-funding from other sources, like private sector, but considers that private partners may raise some doubts due to the fact that the main goal of the private sector is to market themselves. This NGO advocates for a bigger involvement from the European Commission part in co-funding, that could really improve the awareness-raising and the prevention campaigns.

3.5. Conclusions

- Concerning the National Cyber Security Strategy the evaluation team concluded that the work is still in progress and the adoption of the strategy should be prioritised.
- The strategy should define the national priorities in the field of cybercrime and could draw a global picture of which means and targets are needed at national level.
- The statistics on cybercrime are decentralised, which affects the comprehensive picture of the country. However the statistics collected by the territorial structures of the Prosecutor's Office are integrated by the Supreme Prosecutor's Office of Cassation. The evaluation team considers that collecting statistics in a more centralised way could make detailed analysis possible, to bolster the effectiveness of the legal system in combating the cybercrime and in protecting the interests of the victims. A limited number of registered crimes may be seen as bound to the Bulgarian internet equipment rate (60%) which is lower than in other counties, but also to a lack of reporting.
- The statistics are also important to have a realistic image about "dark figure" of cybercrime. The number of cybercrime offences remains low compared to "traditional crime" but there is a dark figure cybercrime. The dark figure includes crimes which are not reported by victims, banks or companies and may includes other cases (when victims abandon the proceedings as soon as they have been reimbursed by the banks; when investigations ultimately yield limited legal results).
- The main financial source for preventing and combating cybercrime has been allocated by co-financing, mainly through EU projects and grants. This demonstrates the interests of national authorities in ensuring the necessary means for tackle this phenomenon. There is still room to improve the situation by increasing the allocation of funds, especially by using the EU projects.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

There are no specialized prosecution/courts in Bulgaria dealing with cybercrime. The common rules for defining the jurisdiction according the Penal Procedural Code are also applied for computer crimes.

The court system in Bulgaria comprises regional – district – appellative and supreme prosecution office/court. The proceeding has three instances.

There are established specialized prosecution/courts on cases of organized crime.

The crimes under Chapter 9a “Computer crimes” are under the jurisdiction of the district courts as well as the skimming crimes. The other computer crimes as these under Art. 212a and the child pornography etc. are under the jurisdiction of the regional court. If the crime is committed by organized criminal group, it is under the jurisdiction of the specialized prosecution/court for the fight against organized crime.

During the visit the experts' team found that there is a Specialised Prosecution Office, whose competences include the offences committed or ordered by an organized crime group, among them cybercrimes offences.

However the Programme of the visit did not envisage a meeting with representatives of the Specialised Prosecutor's Office and when addressed with such a request the authorities were not able to organize it in a short notice. Nevertheless the Bulgarian authorities provided additional information on the legal basis for the functioning and the structure of the Specialised Prosecution Office.

The experts team met representatives from Plovdiv District Prosecution Office, the second largest district prosecution in Bulgaria. From the discussions it resulted that some cyber criminality falls within its competence, like skimming and fishing offences. The offences committed by transnational or national organized groups are within the competence of Sofia Supreme Prosecutors Office.

Bulgarian system does not include specialised prosecutors dedicated to the whole extend of cybercrime offences. The main criteria for specialised competence of prosecutors is the organized crime. This somewhat splits the competence on cybercrime cases, which means that the cybercrime cases related to organized crime will be prosecuted by the Specialised Prosecution Office, while the rest of cybercrime cases falls within the competence of regular prosecution offices.

4.1.2. Capacity and obstacles for successful prosecution

The main practical difficulties encountered, as resulted during the evaluation visit following the discussions with the representatives meet, are:

- the length of mutual legal assistance, which can affect the efficiency of the prosecution;
- the need to speed up the JITs;
- difficulty of international cooperation, as in the past years, Bulgarian authorities had to face with the development of skimming operations carried out by Bulgarian nationals living abroad (Dubai, Canada, United States, European Union). Some cases with Nigeria, have been reported as difficult to be solved because of difficulties with local institutions. The Ministry of Justice nonetheless mentioned several instances of successful international cooperation: a Europol operation involving Italy (stolen data that was sent to Bulgaria), a skimming case involving the United States (a Bulgarian with accomplices in the United States). The individuals involved were extradited and subsequently convicted in the countries where the offences had occurred. Another skimming case involving Italy led to the apprehension of 45 people, who were sentenced within a month.

- the recent legislative amendments on data retention legislation following the invalidation of the Data Retention Directive by the European Court of Justice and as a consequence the investigators can not anymore request to the providers an IP address, without the authorisation of the court, which means a longer period of time before obtaining these data, so the prosecution becomes less effective. Other practical problem is the reduction of the data retention period from 1 year to 6 month, with consequences also for the judicial cooperation with Member States or third countries.
- the formalised procedure for collecting evidence, that could affect the criminal investigations efficiency.
- other practical difficulty during the investigations phase, reported by the police officers, is the establishment of the competent jurisdiction, between the place of data holder, the place of data provider, the place of the server or the place of the offender.
- the encryption of data remain in practice one of the most important difficulties because it makes almost impossible the identification of the offenders. According to the practitioners, the best results in prosecution of a case of child pornography are obtained if the computer is checked and the files can be send as evidence mean. If the seizure is carried out correctly, the case will be successfully sentenced.
- other technical problems refer to the impossibility to identify a specific computer or the person who accessed the computer. In the course of its investigations the CDCOC has encountered "money mules", involved in money laundering operations (connection with Ukraine, China and Russia). It has observed also the development of CryptoLocker, attacks on websites, illegal content sharing, skimming/carding, and hacking into communications between companies with the aim of diverting funds in financial transactions. In March 2014, a malware campaign specifically targeted companies.

- the length of the forensic examinations by the National Forensic Institute, which could take more than 6 months, due to the lack of sufficient human resources (technical experts and assistants) and technical resources.
- the rules of competence, related to the fact that there is no specialised competence on cybercrime but only on organized crime, which means that not all cybercrime cases are investigated by the special unit CDCOC and Special Prosecution Office. According to the practitioners from Plovdiv Prosecution Office, until 1 year ago there was a specialised unit within the office, with 3 prosecutors competent for the cybercrime cases, working with CDCOC. Now there is no longer specialised prosecution unit at the district level and prosecutors cannot work anymore with DCOC in solving cybercrime cases.
- the level of sanctions which, according to the national law, is too low and doesn't ensure a dissuasive character. In addition the level of sanctions has consequences on the jurisdiction also: the cybercrime offences for which the law provide less than 5 years of imprisonment cannot be qualified as organised crime and therefore cannot be managed by specialised jurisdiction.
- the lack of case of law that could be used as reference, has been underlined by a judges' representative met by the experts team during the evaluation visit.

4.2. Law enforcement authorities

The main entity for combating cybercrime is the Cybercrime Unit at the CDCOC. The activity of CDCOC is regulated in the Ministry of Interior Act. It has a full range of police functions. The officers in CDCOC – MoI also have investigative functions.

The authority directly involved in the fight against cybercrime in Bulgaria is the specialized Cybercrime Unit of Transborder Organized Crime Department in the Chief Directorate Combating Organized Crime (CDCOC) within the Ministry of Interior. The unit is functioning since 2006. The staff comprises about 20 police officers, divided in groups on the unauthorized access to computer data, financial fraud, intellectual property, illegal content and pornographic material involving children, national contact point on the retention of computer data in 24/7 regime and other supporting activities. Another 20 police officers from the regional structures of CDCOC in the main cities of the country are supporting the activity of the unit. In accordance with their legally defined functions the police officers interact with the Prosecutor's Offices and the Court in the process of investigation and detection of computer crime and computer-related crime. They also cooperate with the academia and other organizations and companies in order to prevent and neutralize the negative impact on the computer information security in the country.
Several lines of work can be provisionally differentiated in the specialized Cybercrime Unit at the CDCOC - MoI based on the different types of computer crimes under the Budapest Convention on Cybercrime.

A national contact point for retention of computer data and information is functioning 24/7 in the specialized Cybercrime Unit in CDCOC - MoI.

Based on decisions taken by successive political authorities, the CDCOC became part of the State Agency for National Security from 2013 to February 2015. Since February 2015 it has been moved back to the Ministry of the Interior. These reforms resulted in significant staff reductions (e.g. staff at the CDCOC Plovdiv fell from 40 to 18 persons).

This specialized unit has good achievements and organized successful operations on various issues such hackers attacks, illegal Internet activities against intellectual and industrial property, counterfeiting goods and services, illegal content of Internet (dissemination of materials containing child pornography, racism and xenophobia).

One of the problems encountered in practice is that sometimes criminal investigations carried out outside the capital cannot be coordinated locally, as the CDCOC, at both central and local level, is under the sole authority of the Specialised Prosecutor's Office dealing with organised crime, which is not always competent for all cybercrime offences.

In the course of its investigations the CDCOC has encountered "money mules", involved in money laundering operations, in connection with Ukraine, China and Russia. There is a clear development of CryptoLocker, attacks on websites, illegal content sharing, skimming/carding and hacking into communications between companies with the aim of diverting funds in financial transactions. In March 2014, a malware campaign specifically targeted companies.
Local actors experience difficulties because regional competences differ from one administration to another.

The local CDCOC unit is not under the authority of the Plovdiv prosecutor's office but of the Specialised Prosecutor's Office in Sofia (150 km away), which is problematic when it has to make requests to the judge to obtain authorisation to order an IAP to intervene. The CDCOC covers a large area around Plovdiv, and the distances between the premises searched, the service, the prosecutor's office in Sofia, etc. are sometimes significant.

Complaints may come from local police services, forwarded by the prosecutor's office, or from Sofia. Complaints received by the territorial police are subject to an initial assessment: routine cases are left with the local police, while for others notification is sent to the prosecutor, who can decide to assign the case either to the specialised regional police services (financial police or police responsible for cybercrime) or to the CDCOC in the case of organised crime. In principle, prosecutors are notified in urgent cases and in criminal cases, or if there are particular operational issues.

The local court considered that greater use could be made of the local CDCOC. Even so cooperation between local authorities (LEAs and judicial level) is very good, based mainly on personal contacts and flexible pragmatism. Officially, the CDCOC must not discuss its cases (organised crime being the responsibility of the specialised prosecutor's office in Sofia).

4.3. Other authorities/institutions/public-private partnership

Other authorities involved in the prevention and the fight against cybercrime are the Computer Security Incidents Response Team and Research Institute of Forensic Science and Criminology, responsible for the forensic reports for criminal proceedings.

- The Computer Security Incidents Response Team (GOVCERT - Bulgaria) is organised within the Executive Agency “Electronic Communication Networks and Information Systems” to the Ministry of Transport Information Technologies and Communication (TTITC).

Its mission is to assist the users of its services in the provision of proactive activities for diminishing the risks of incidents in computer security and assist in recovering from such incidents in case they have already occurred.

In accordance with the provisions of the MoI Act Cybercrime Unit with the CDCOC, which is the main responsible authority in the fight against cybercrime, has the competence to issue orders and recommendations in the cases of circumstances and conditions with a negative impact for the computer information security on a specific computer system. In a similar way the other competent authorities in the field of cybercrime have at their disposal the necessary mechanisms to implement preventive measures as stipulated by the law.

The experts' team met with the executive director of the Agency responsible for electronic communications and information systems, which include CERT Bulgaria.

The agency cooperates with the Ministry of the Interior, the State Agency for National Security (informal but effective cooperation), on national cyber security, under the authority of an intergovernmental head of cyber security.

The agency has developed a cloud infrastructure for administrations with a data center service, which takes into account the standards specified by ENISA.Its intention is to concentrate all the information in a single place, which should ensure a better and more secured protection.
CERT Bulgaria is the international contact point. It was created in 2008 and accredited in 2009.
It is responsible for network security activities, for reporting incidents, assessing threats and providing assistance. The team consists of 21 people. Its work is based on automated reporting (no technical monitoring system).

CERT is the coordinator of all institutions involved in the process of drafting the National Security Strategy in cyber matters. The discussions involve Ministry of Interior, Ministry of Defence, academics, banks, companies, Internet providers. They intend to create a global network including information security, cybercrime and cyber security. According to the CERT representatives the strategy should be adopted until the end of 2015.

The CERT is using the opportunity offered by the ongoing work on the cyber security strategy to develop its external contacts. It already established relations with NATO, US-CERT, ENISA, the International Telecommunication Union, and private companies (Kapersky, McAfee, Bitdefender, Symantec) and takes part in cyber security exercises[8].

[8] with the EU or with Turkey: Cyber Shield.

CERT has also very good cooperation with the National Internal Security Agency, the LEAs and the Internet providers. They share information, through letters, phone, emails, they receive information on any incident that could constitute a cybercrime or cyber security case.
CERT underlined that the number of cyber attacks is decreasing while the level of complexity is increasing. They receive less signals but the attacks are more difficult to detect and more complex.

In the opinion of CERT's representatives cyber security, cybercrime and cyber defence are different but interconnected systems. The main role of CERT is to ensure the coordination and to facilitate the cooperation between all the stakeholders due to the fact that the technology is developing faster than the law and in the cyber crime field there are no borders.

As regards reporting procedures, Bulgarian law requires companies to report attacks to the national CERT. However, the CERT cannot oblige private operators to take particular measures, even in the event of a major attack. Companies may only be invited to make complaints. Cooperation varies depending on the sector (very good in the area of telecommunications, more unpredictable with the commercial and banking sectors).

The CERT informs systematically the national security service whenever an attack is recorded. It is intended to publish soon a full statistical report.

- The Research Institute of Forensic Science and Criminology within MoI supports the criminal investigation services by making digital analysis of materials that are seized during the operations (searching viruses, recovering deleted data, etc). The Department of Digital and Communication Devices became part of the Institute in March 2014. The institute is registered to the Europol Network of Forensic Science Institutes (ENFNSI). Bulgarian authorities prefer to task it than private sector, as it has a good expertise and works with better equipment and less costs.

The institute has four units dealing with cybercrime: computer analysis, electronic devices analysis (skimmers, banking cards, alarm systems), video analysis, communication devices analysis (mainly mobile phones). This last unit has to face with a very significant increase of requests form the investigation services but it manages only half of them, with a processing time up to a year.

As main challenges, the forensic team underlined the lack of technical means comparing with rising number of more and more complex requests, like hard drive in terabytes, encrypted materials, cloud storage of data whose access remains extremely difficult, greater diversity of operating system, international companies who may be reluctant to give encryption codes.
The development of the institute is based on several projects: a training program for its experts, the creation of a network of 18 laboratories all around the country, new equipment and software expected at the end of 2016 (project of 350000 euros, financed by the EU).

- Another institution involved in preventing and combating cybercrime is the State Agency "National Security" (SANS). Its activities related to countering cyber crimes are regulated in Article 4 (1), item 9 “endangerment of the security of facilities or activities of a strategic nature for this country” and item 10 “actions having a disruptive effect on communication and information systems” of the State Agency for National Security Act, and also in Articles 104 and 105 of the Penalty Code, related to crimes against the Republic of Bulgaria.

SANS’s tasks in cybersecurity are as follows:

- to ensure the rights of Bulgarian citizens, business, and public administration to exchange in a free and secure way information in the cyber space and to enhance their confidence in using information and communication technologies by implementing minimal basic security levels.
- to improve the coordination mechanism of cybersecurity issues by determining clear structure connections, rules and procedures for cooperation and information exchange.

- to implement the capacity, and to extend the government structures' capabilities with cybersecurity responsibilities by targeted investments and widening of existing public-private partnership with various academic, business and non-government organizations;
- to prevent crisis and disasters in cyber space and mostly those connected to strategic installations and strategic activities;
- to determine a clear and threats-adapted commitment of the internet services providers related to the security of the end user;
- to implement predictable national cyber space which is stable to internal and external disruptive influence – "secure environment for availability of electronic services and electronic government" by integrating national institutions and organizations, education, industry and media.

The SANS's unit engaged in the field of cybersecurity matters carry out activities related to: research of approaches used in modeling and simulating of complex information systems; exploring vulnerabilities of available computer-information systems; communication systems modeling; information systems analysis; creating models of strategic installations information systems; policy making and developing security procedures, adapted to specific strategic installations; establishing of threats and disruptive influence data base; development of malware code analysis systems; participating in joint working groups on cybersecurity matters.

The activities have been determined in the existing legislation, and by SANS's competences in classified information protection and strategic installations' protection.

To date, SANS participate in a joint working group established in order to develop "National Strategy For Cybersecurity" project. The project's deadline is the end of September 2015.
The adoption of the "National Strategy for Cybersecurity" project is essential for launching planned activities and tasks regarding the implementation of the EU Strategy For Cybersecurity – "Member States should have structures for functioning on issues concerning the stability of the cyber space and fighting cybercrime or are obligated to establish such structures".

To perform its functions and powers, SANS interacts with high and expert level structures within the Council of Ministers, Ministry of Interior, Ministry of Defense, Executive Agency "Electronic Communication Networks and Information Systems" within the Ministry of Transport, Information Technology and Communications, Prosecutor's Office of Republic of Bulgaria, and other structures committed to prevention and countering cybercrimes on the territory of Bulgaria.

On an international level, SANS is a Bulgarian participant in agreements for partnerships and cooperation in fighting transnational cyber space crimes. The partnership is carried out jointly with the security services of the EU and NATO Member states, as well as with third countries which Bulgaria has agreements with.

SANS's main tasks are as follows: critical services' availability and confidentiality; critical information infrastructure identification and categorization; development of adequate minimal requirements for computer and information security; information protection control of communication and information systems serving strategic instillations and activities; development of capabilities for prevention and response during cyber incidents including the systems' recovering.

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

Other authorities involved in guaranteeing the cyber security and fighting cybercrime are the Ministry of Transport, Information Technologies and Communications - Government CERT, National Security State Agency, Ministry of Defense, Supreme Prosecutor's Office of Cassation and the competent prosecutor's offices.

Electronic Communications Act (Art. 243b) for enterprises, providing public communication networks and/or services provides the obligation to report cyber attacks.
A national contact point for retention of computer data and information is functioning 24/7 in the specialized Cybercrime Unit in CDCOC - MoI.

There is a sufficient cooperation between private sector and LEAs to prevent and fight card fraud. Meetings are held in this goal ant the LEAs are getting acquainting with the new trends. Bulgaria has developed and patented a special system for protection of the data from the magnetic tape - SKIMPROT. The technology and the product are available to the cardholders.

During 2007-2008 it was a serious increase in the irregular online transactions through Internet banking. As a result, additional measures were taken to enhance security, comprising end user software security and additional measures, such as token devices, personal codes, SMS confirmation.

The Bulgarian law enforcement authorities involved in combating online sexual exploitation of children, namely CDCOC, are in close cooperation with the Bulgarian Hotline for Safer Internet - www.112.net, which is part of the international organization INHOPE. Many training and awareness raising campaigns among students, parents and teachers across the country were conducted within this cooperation in the recent years. The trainings were conducted with representatives of CDCOC, the Hotline for Safer Internet and the International Academy for Cyber Investigation. In addition, the Cybercrime Unit at CDCOC has developed and maintains two web sites - www.cybercrime.bg and www.spasidete.bg where information on concrete measures to ensure children's safety when they surf the Internet is published. The site www.cybercrime.bg has a convenient and affordable alert platform. There is also an initiative to filter illegal content on the Internet, which is done on a voluntary basis by a number of Internet providers.
At regional level, cooperation between local authorities is based on a proactive management approach and direct relationships.

4.4.2. Resources allocated to improve cooperation

There are not yet allocated resources to improving the cooperation with the private sector.

4.5. Conclusions

- Regarding the cybercrime jurisdiction, only the cybercrime offences committed by or linked with an organised criminal group are under the competence of the specialised investigation and prosecution offices for the fight against organised crime. As a consequence cybercrimes that are not related to organised crime are investigated and prosecuted by police officers and prosecutors that are not specialised in cyber criminality.
- Due to the low level of training for judges and the lack of case law, the general knowledge of the courts about the specificity of cybercrime cases is quite low. There is a clear need of more specialised training addressed to judges and prosecutors.
- Issues as data encryption and cloud storage remain obstacles at the legislative and practical level.
- Other issues raised by the LEAs and judicial authorities are related to the national legislation, amended following the ECJ decision of invalidation of Data Retention directive. In addition the implementation of some specific investigation measures are limited to serious crimes, for which the sanction provided by the law is 5 years of imprisonment. According to the practitioners, the procedure for search and seizure requires two witnesses to be present when mirror copying hard drives. This means that mirror copying in practice cannot be done on site which may affect the capacity to analyse hard drives in a timely manner[9]. In general the judicial procedure for collecting e-evidence does not allow sufficient flexibility in terms of speed and efficiency.

[9] Examples of a waiting time until 1 year have been reported by the national authorities.

- In order to solve the problem of the length of the mutual legal assistance requests, the national authorities use frequently JITs, which are considered a helpful instrument for solving transnational cyber crime cases.
- Regarding the LEAs, the main entity for investigating and combating cybercrime is the Cyber Unit within CDCOC. The experience of this specialised unit seems to be very good. The police officers of this unit have a very good technical knowledge and conduct specialised investigations in cybercrime cases. They are also involved in the activity of prevention and reporting of cybercrime cases. The Cyber Unit is also involved in awareness campaigns, dedicated to students, parents and children for a safer Internet and it developed two web sites, where information for using Internet in a safer way is displayed.
- For a better cooperation CDCOC local forces should meet with local partners several times a year to exchange views on trends and completed investigations.
- CERT is able to share information on cyber incidents to LEAs partners. Its main role is to ensure coordination and to facilitate communication for all stakeholders involved in cyber security.
- The cooperation between LEAs and private sector is quite functional on an informal basis rather than on a legal basis. Meetings take place in order to exchange information and a number of Internet providers report on a voluntary basis the incidents for filter illegal content on the Internet.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

According to the MoJ representatives, in charge with drafting the national legislation, the specific cybercrime offences are spread in the Criminal Code, due to the fact that the main principle of offences' classification and systematisation is the type of social relations that an offence violates.

The representatives also underlined that Bulgaria is in a process of the reform of Criminal Code. A first draft of a new Criminal Code was prepared and this draft systematises the cyber crime offences in a unique chapter and up-date the level of sanctions for the computer crimes. The draft included also the transposition of the directives adopted in the field of cybercrime. The draft was criticised by the stakeholders (judicial practitioners and academics) and now the competent authorities decided to draft firstly a Strategy in Criminal Matters and after being agreed, they will start again to work on a second draft of criminal Code.

There is also a draft amendment to the Criminal Procedural Code and the MoJ asked all the practitioners to suggest necessary amendments according to the needs identified in practice.

5.1.1. Council of Europe Convention on Cybercrime

Bulgaria signed the Convention on 23.11.2001 and ratified it on 07.04.2005. The Convention is in force for Bulgaria as of 01.08.2005.

5.1.2. Description of national legislation

5.1.2.1. Council Framework decision 005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems

Regarding the Council Framework Decision 2005/222/JHA on attacks against information systems, the provisions are implemented in the following legal acts: Criminal Code, Administrative Violations and Penalties Act, Electronic Communication Act and Criminal Procedural Code.

Bulgaria has not yet fully transposed into the national legislation the Directive 2013/40/EU on attacks against information systems.

A Working Group within the Ministry of Justice has been set up to analyze the provisions of the Directive and bring proposals for necessary legislative amendments to the Criminal Code. The requirements of the Directive for criminalization of certain attacks against information systems have been already largely met due to the fact that in 2005 Bulgaria ratified the Council of Europe's Convention on Cybercrime and aligned its legislation with the standards of the Convention.

Although the Directive is not yet formally transposed, the majority of its offences are already included in the national legislation.

Bulgaria punishes as criminal offences a lot of acts including a computer, such as: Destroying or damaging another property, committed by unwarranted access to a computer of importance for a enterprise, corporate or individual, Copying, using or fulfilling access to computer data in a computer system, Introducing virus in a computer system or computer network, Adding, changing, deleting, or destroying a computer programme or computer data in significant cases (without the permission of the user or administrators), Using special technical devices, illegally reads a message not addressed to him, transmitted by telephone, telegraph, through a computer network or other telecommunication device without permission, acquiring, keeping or harbouring objects, computer software or elements for protection of banknotes, materials or instruments to design o to use it to forger currency or other notes or payment instruments, Circulating passwords or access codes to a computer system or to computer data, thus causing disclosure of personal data or information representing a state or other secrets protected by the law.

The Criminal Code establishes some aggravating circumstances when the crime has been committed by 2 or more people, when it has caused substantial damages or several consequences or is related to destruction or damaging of elements of the communication network, if the information constitutes a State secret, if the act has been committed repeatedly, or in respect of data for creating electronic signature or regarding data provided by virtue of a law, by electronic means or on magnetic, electronic, optical or other means.

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

Bulgaria has transposed Directive 2011/92/EU of 13 December 2011, relevant amendments to the Penal Code being adopted by the National Assembly on 7 September 2015 and published in the State Gazette no. 74 of 26 September 2015 .
The Criminal Code has been amended in 2009 in order to be brought in compliance with the Convention of the Council of Europe on the Protection of Children against Sexual Exploitation and Sexual Abuse (ratified by Bulgaria on 02.11.2011 and in force since 01.04.2011).

Some acts are already criminalized by the Criminal Code into force, such as: production of child pornography, which includes exhibition, presentation, offering, selling, lending or circulating in another way pornographic materials, Acquisition or possession of child pornography. The Bulgarian Criminal Code has a definition of pornography material in the article93.28 of Criminal Code, “is any indecent, unacceptable or incompatible with the public moral material depicting exposed sexual behaviour. This means any behaviour expressing real or simulated sexual intercourse between persons of the same or different sex, sodomy, masturbation, sexual sadism or masochism, or lascivious exhibition of the sexual organs”, and it is considered as child pornography material when it’s used a person younger than 18 years old or a person with such appearance. It includes not only children, but also any person appearing to be a child.

At the time of the on site visit, the Bulgarian legal framework contained three of four meanings of child pornography definition included in the Directive[10]. However, it did not include "realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes".

After the evaluation visit, the national authorities reported that Bulgaria has transposed into the national legislation the Directive 2011/92/EU of 13 December 2013 on combating sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA. The relevant amendments were adopted by the National Assembly on 17 September 2015 and promulgated in the State Gazette (issue no 74 of 26 September 2015).

Others incriminations refer to: Providing information, through Internet or in any way, of a person less than 18years of age in order to contact with this person for sexual purposes, prostitution or production of pornographic materials and Establishing contact with a person less than 14 years of age by using information provided on the Internet or in any other way for sexual purposes.

5.1.2.3. Online card fraud

In practice, the most frequent offences are skimming and other computer fraud rather than the child pornography cases. Bulgaria had participated in several JITs involved in skimming or identity theft, committed through an organized group. The practitioners consider that the most important part of cybercrime in Bulgaria is represented by computer fraud.

[10] Definitions of Directive: Child pornography means: any material that visually depicts a child engaged in real or simulated sexually explicit conduct; any depiction of the sexual organs of a child for primarily sexual purposes or any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes.

Computer fraud is considered a crime by article 212.a.2 of the Penal Code, and it punishable that enters, changes o deletes of obliterates computer data in order to obtain something.

Chapter VI - Section IV of the Penal Code includes offences against the monetary and credit system, and contains such as, forging payment instruments[11], or working out, acquiring, keeping or harbouring objects, computer software or elements for protection or banknotes, materials or instruments (in cases of the criminal knows to be designated or which have served forgery of currency or other notes or payment instruments[12], or using a payment instrument or data of a payment instrument, or producing, installing or using a technical device in order to obtain information for the content of payment instrument (also who keeps or provides other persons this information)[13].

Bulgarian legislation provides for liability of legal person for cyber crime in case of a crime committed in their favour[14] but only in the cases established in this article, and specifically, in case of computer-related production, distribution or possession of child pornography[15], computer-related solicitation or "grooming" of children[16] computer-related fraud[17] and crimes included in Chapter IX A of Penal Code called "a computer crime" [18] The liability of legal person is only administrative-punitive, not punitive on the basis of the Criminal Code.

11 Art. 243 penal code.
12 Art. 246.3 Penal Code.
13 Art. 249 Penal Code
14 Art. 83a of the Law on the Administrative Violations and Penalties.
15 Art. 159 penal code.
16 Art. 155a penal code.
17 Art. 212.a penal code.
18 articles from 319 a to 319.f.

The sanctions for cybercrimes offences are fines and imprisonment

The fine minimum penalty is up to one hundred leva[19], and the maximum penalty is a fine up to five thousand leva[20].

The lowest imprisonment is of up to six month[21] and the highest is eight years[22].
Recidivism as aggravating circumstance are provided by articles 319.a.3. and 319.d.3 of Penal Code.

The attempt of cybercrime offences is punishable [23], except in two cases contained in art. 18.3 of Penal Code[24]. Regarding the accomplice, the Bulgarian Penal Code considers that they are the perpetrator, the abettor, and the accessory, and it defines to each of them[25]. It considers the abettor and the accessory shall not be punished in case that they give up further participation and impede the commitment of the act or prevent the occurrence of the criminal consequences[26].

The legislation does not provide for specific criteria in order to define a "serious" or "large scale" cyber attack, only established high punishment in case of considerable damages, substantial harmful consequences and serious consequences. Their content is defined in the interpretative rulings of the Supreme Court.

19 Art. 216.4, art. 216.6
20 Art. 319.b.3; Art, 319.c.2.
21 Art. 216.4
22 Art. 319.a.5
23 Art. 18 Penal Code
24 Art. 18.3: When the perpetrator has given up to complete the commitment of the crime or has prevented the occurrence of the criminal consequences.
25 Art. 20 Penal Code.
26 Art. 22 penal code.

5.2. Procedural issues

5.2.1. Investigative Techniques

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

Search and seizure of computer systems and data is carried out only under the provisions of Art. 159; Art.160; Art. 161, Art. 162, Art. 163 and Art. 165 of the Bulgarian Penal Procedure Code (PPC), following authorization by the chairperson of the relevant court. The only hypothesis of conducting search and seizure of information and data systems without permission of a judge is referred to in Art. 161, para. 2 of the PPC - in the case of urgency, where it is the only possibility to collect evidence for the purposes of the conducted proceedings. In that case, the protocol for the conducted search and seizure shall be provided immediately and not later than 24 hours to the prosecutor, to be submitted for approval by the competent Judge.

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

Interception of real-time data, traffic and content /real data traffic capture/ is carried out under the conditions of application of special investigative means and is carried out by the Technical Operations State Agency, after having received an authorization by a judge.

- **preservation of computer data;**

Under the provisions of Art. 251b of the Electronic Communications Act (ECA), the telecommunication service providers in Bulgaria shall store identification data for the end users for a period of six months and provide them to the investigation authorities for the purposes of detection and investigation of serious crime.

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

Under the provisions of the ECA traffic data can be provided upon authorization form the competent Court.

- **order for user information.**

Basic information about users, with the exception of traffic data, can be requested directly by the police by a reasoned written request.

Other investigative techniques, provided by the Criminal Procedural Code or by the Electronic Communication Act, than can be used are:

- obligation for delivery of objects, papers, computer information data, data about the subscriber of a computer information service and other data,

- provision of data by undertaking providing electronic communication networks and/or services,

- search and seizure,

- interception and seizure of correspondence,

- interception of electronic communications related to protection of national security and maintenance of public order.

The specialized Cybercrime Unit at the CDCOC reported serious difficulties in obtaining e-evidence due to the amendments of the national law on data retention, following the decision of ECJ, which shortened the time limits for data retention (6 months) and for data preservation (3 months).

In addition, they are not able anymore to request data for computer crimes with a penal value of less than 5 years since the law provides this possibility only for serious crimes. According to the national legislation, serious crimes mean those offences for which the law provides at least 5 years of imprisonment and the sanctions for the majority of computer crimes are lower. However they can still require data for the child pornography cases. In conclusion the police officer experiment practical difficulties in the collection of evidence due to the limits imposed by the national law.

5.2.2. Forensics and Encryption

Within the Research Institute of Forensic Science and Criminology, subordinated to the Ministry of Interior, there is the Digital and Communication Technology Unit in charge with the forensic reports. The unit deals with the following types of forensic reports:

- audio and video identification,

- computer systems and networking devices,

- communication devices and electronic devices (skimmers, bank cards, electronic payment instruments).

The institute uses a quality guidelines which include templates, procedures and rules. The workflow supposes an automatic assignment and the obligation to keep tracks of the process, which grants the integrity of the evidence.

The representatives of the institute signalled some difficulties related to the big numbers of requests from the investigation services and the short dead- lines in relation to their capacities.

The technical capacities also need to be improved and the representatives mentioned a co-funded project with EU that aims to obtain modern hardware and software.

The experts benefited from a few training courses organized by Europol and non-governmental organizations, but they assess that more training is necessary, in order to increase the level of expertise.

Concerning the workload, the Institute received approximately 400 of orders every year, the large majority of them being made during the pre-trial phase, by police and prosecution services.

In terms of encryption the institute has not the technical capacities to decrypt. Each seized computer has to be mirrored in the laboratory and not on the spot, as mirroring on the spot would require the presence of witnesses and the whole process could last 10 to 12 hours which in practice make impossible these actions.

Due to the lack of technical equipment and training the institute is unable to read some skimmer devices, to decrypt and to access cloud structures.

The representatives of the institute claim the need to recruit more human resources, to increase the training and the technical capacities.

The representatives of the Institute up-dated the information given during the evaluation visit, as follows:

- RIFS does not have a specialized unit for decrypting. While conducting examinations and preparing expert analyses, some specialized programmes for decrypting information may be used.

- RIFSC has software for recovering passwords - “Passware Password Recovery”. The necessary time to recover some passwords is however very long and it exceeds the time for preparing the expert analysis. Beside that, this software does not cover all the cases of password protected files.

Very often (for example while exchanging data on skimmed bank cards) PGP encrypted files are found. For the time being there are no tools for the decryption of these files as well as for the decryption of encrypted hard disks until now RIFSC has not contacted specialized centres for decryption.

5.2.3. e-Evidence

There are specific requirements regarding collection of e-evidence in order to be admissible in the courts. In principle, the e-evidence should be collected by an expert with technical knowledge in order to preserve its integrity. The main reason is that, as the data are dynamic, they have to be collected by an expert in order to preserve the integrity.
However, the practitioners consider that rules for collecting e-evidence should be simplified.
Another issue is the fact that it is not possible to have access to e-evidence located in other country or in cloud, consequently the prosecutors considered that the national or international legislation should be amended in order to allow access of these kind of e-evidence located in specific places, for example to have access to the mobile phone of a suspected or accused person located in another country. In practice there were some successful transnational skimming cases either in EU, either in USA, that involved Bulgarian citizens .

The conclusion of the practitioners is that the specificity of the cybercrime requires specific and simplified rules for obtaining and collecting evidence.
After the evaluation visit, the representatives of the Institute sent additional information in order to clarify further some more aspects. According to the Rules for the structure and activity of the MoI, RIFSC performs technical expert analyses including those on electronic evidence/evidence of electronic character. The investigating authorities assign expert analyses to RIFSC on the basis of a decree by the Criminal Code. RIFSC receives the decree together with the evidence. As a result of the quality management system introduced into RIFSC, the traceability of the process as well as the movement of the evidence are ensured.
The tendency is to accredit under ISO 17025 the activities for examining electronic evidence so that objectivity of the results received be guaranteed. There are clear procedures and methods. With the help of specialized technical and programme products the electronically stored information may be recovered and acquired. At the end of the examination an expert report is prepared which gives the answers to all the questions of the investigating authorities, and together with the decree, the evidence, sealed and secured in the appropriate way, and the information required, it is handed back to the assignor.

As it was already stated in the replies to questioner, the following concepts are legally defined: computer system, computer data, computer network, computer programme, computer virus. The concept “electronic document” is defined in the law on electronic document and electronic signature.

In Bulgaria there is no legal definition for “evidence of electronic character”. At the moment a process of regulating these matters is going on likewise the processes in EU, and standards after ISO 27039 are expected to be developed and adopted. These standards give important guidelines for identification, gathering, acquiring, processing, protecting and preserving electronic evidence.

5.3. Protection of Human Rights/Fundamental Freedoms

The fundamental rights and freedoms of the Bulgarian citizens are enshrined and protected by the Constitution, the laws and the secondary legislation of the Republic of Bulgaria. Interference in the privacy of personal life, home, correspondence, data, freedom of expression, etc. can be undertaken by the law enforcement authorities only with the permission of the Chair of the competent Court for the purposes of detection and prevention of serious crime. In Bulgaria the competent national authority for the implementation of special investigative means is the Technical Operations State Agency. Very strict rules are applied with regard to its activities and accountability. A number of governmental and non-governmental organizations are monitoring the observance and protection of the rights and freedoms of the citizens: National Bureau on Control of the Special Investigative Means, Parliamentary Committee on the Control of the Security Services, the Bulgarian Helsinki Committee, etc. In the beginning of 2015 the Constitutional Court declared some provisions of the Law on the Electronic Communications unconstitutional and limited the possibility of the law enforcement authorities to intervene in the private life of the citizens by using their traffic data. The decision of the Constitutional Court is based on the Court of Justice of the EU Decision of 2014 pronouncing the Data Retention Directive 2006/24 invalid.

The Constitution sets the principle that the mentioned rights are not absolute and as such can be subjected to restrictions. Posing such restriction is possible only in the cases strictly provided by the law and following the prescribed conditions.

According to the Bulgarian legislation limitations to parts of the fundamental rights and freedoms, private life, home, correspondence and personal data are permissible only for the purpose of detecting and preventing serious crime and after authorization from the Chair of the competent Court. There are no legal possibilities to restrict freedom of expression in Bulgaria. In the Penal Code the only computer crime, unique to information systems according to Table 2 above / computer crime / that is qualified as serious is the act committed under the aggravating circumstances, specified in Art. 319a, para. 5 - unauthorized access, copying and use of classified information, which is state secret or other information protected by the law, which has led to serious consequences. There is another crime in the Penal Code, which is not included in Chapter 9A "Computer Crime", but in "Destruction and Damage" Section, which has the characteristics of a computer crime, unique for computer systems, in accordance with Table 2 above - Art. 216, para. 3 and para. 5 “destruction of another's property as a result of unauthorized access to a computer system”.

Bulgarian legislation allows the limitation the fundamental rights and freedoms, like as private life, home, correspondence and personal data, but only for the purpose of detecting and preventing serious crime and after authorization from the Chair of the Competent Court.
The only serious crime is the creation of the child pornographic material[27], and the act committed under the aggravating circumstances specified in art. 319a para.5 - Unauthorized access, copying and use of classified information, which is state secret or other information protected by the law which has led to serious consequences.

[27] Art. 159.4 penal code

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

According to the general principles of the Criminal Code of the Republic of Bulgaria, criminal jurisdiction is established over acts committed within the territory of Bulgaria, acts committed by Bulgarian nationals, as well as acts committed abroad by foreign nationals, affecting the interests of the Republic of Bulgaria or of a Bulgarian citizen and acts committed abroad by foreigners wherever stipulated by an international agreement to which the Republic of Bulgaria is a party.

The jurisdiction is also established over offences committed only partly in Bulgaria.

Article 3 of Bulgarian Criminal Code states that the code shall apply for every crimes committed on the territory of Bulgaria (principle of reality). Article 4 sets out the principle of personality, which means that the Criminal Code is applicable for the Bulgarian citizens and for the crimes committed by them abroad. There also provision regarding the foreigners who have committed crime abroad, affecting the interests of Bulgaria or one of its citizens or against the peace and mankind, that affect the interests of other countries or foreign citizens.

The issue on the competence and jurisdiction of the criminal act in cases of cross-border cybercrime is open in Bulgaria just like in many other countries. There is different practice, as in some cases the jurisdiction is determined by the location of the offender at the time of conducting the criminal act. In other cases the jurisdiction is considered according to the location of the used computer infrastructure /server/. A change in the jurisdiction is also possible, whereas the competent court or prosecutor could be determined according to the place of residence of the victim or the witnesses.

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

When a conflict of jurisdiction occurs in the course of the criminal proceedings contacts are made between judicial authorities. Cases of conflicts of jurisdiction are successfully resolved by means of referral to Eurojust for coordination and consultation, transfer of criminal proceedings, issuance of a new modified European arrest warrant.

However, Bulgaria has not yet established the mechanism set out in Council framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings. The act is not implemented yet into the Bulgarian legislation but according to the national authorities draft amendments to the Penal Procedure Code have been elaborated and are expected to be approved by the Council of Ministers and submitted to the Parliament early 2016.

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

The fundamental principles of the Bulgarian legislation determining the competence of the Bulgarian state to prosecute criminal acts are regulated in Chapter One, Section II of the General part of the Criminal code of the Republic of Bulgaria “Scope of application of the Criminal code”. According to them the Criminal code of the Republic of Bulgaria shall apply:
- for all crimes committed on the territory of the country no matter if they are committed by Bulgarian or foreign citizens (Article 3, paragraph 1, CC):
- in regard to Bulgarian citizens who have committed crimes abroad (Article 4, paragraph 1, CC);
- in regard to foreigners who have committed crimes abroad which affect the interests of Bulgarian citizens or the Republic of Bulgaria (Article 5, paragraph 1, CC);
- in exceptional cases, a Bulgarian citizen may be extradited to another country for the purposes of criminal justice only if it is provided in an international agreement to which the Republic of Bulgaria is a party (Article 4, paragraph 2, CC).

These principles are applicable in relation to the competence of the Bulgarian law enforcement and judicial authorities regarding computer crimes committed in the so-called Cloud (in terms of Cloud Computing). In the context of the question those principles of competence mean that:
a) when a Bulgarian citizen commits illegal acts on Bulgarian or foreign territory, related to data located on a server in a foreign country and those acts are crimes according to the Crime Code of the Republic of Bulgaria, the competence of criminal prosecution is of the Bulgarian state. If the criminal actions have affected the rights and interests of foreign citizens or foreign country, and Bulgaria receives a request to extradite a particular person for trial to a foreign country, this may happen only in accordance with Article 4, paragraph 2, CC (the presence of an international agreement, which has been ratified, published and entered into force in respect to the Republic of Bulgaria).

b) when a foreign citizen commits a computer crime on the territory of the Republic of Bulgaria they may be submitted for prosecution to a foreign country under the terms and conditions of the Law of the Extradition and the European Arrest Warrant.

In regard to gathering of evidence with electronic character, if the operator that provides the service is located on the territory of the Republic of Bulgaria, the request to retain and/or provide the necessary information (traffic data) for the investigation shall be made after the permission of the court under Article 159a of the Penal Procedure Code of the Republic of Bulgaria and Article 251b-251h of the Electronic Communications Act.

For fast data retention (under Art. 16 and Art. 17 of the Cybercrime Convention) located outside the territory of the Republic of Bulgaria, the power of the Contact point 24/7 at CDCOC/MoI, established under Art. 35 of the Cybercrime Convention, is used. Subsequently, in order to be used as evidence in the criminal proceeding, a request for mutual legal assistance under the rules of international cooperation is made to the foreign country in order to provide the stored data. A similar procedure is applied when data necessary for investigation carried out by a foreign country, is stored on a server located on the territory of the Republic of Bulgaria.

5.4.4. Perception of Bulgaria with regard to legal framework to combat cybercrime

The national legal framework complies in full level with the challenges in the investigation of cyber crime, which in recent years, by definition, include an international element.
Low punishments for crimes under Chapter 9a (real computer crimes) of the Criminal Code of Republic of Bulgaria do not allow in their investigation to ask the operator, through the court, to retain or access relevant service to electronic data, including traffic and to use special investigative means, under national and international law. That is because access to the data, necessary for the investigation, may be granted under Article 159a of the Criminal Procedure Code only in the case of "serious crime". The same requirement applies and to the use of special investigative means according to Article 172, Para. 2 and 3 of the Criminal Procedure Code.

"Serious crime" within the meaning of Article 93, p. 7 of the Penal Code is the one, which by law is punishable with "deprivation of liberty more than five years", life sentence or life imprisonment without exchange.

The provided sanctions under Chapter 9a of the Penal Code, punishments are a penalty or deprivation of liberty to a maximum of three years.

Another problem of the Bulgarian legislation is the short period to retain the data. According to Article 251b, Para. 1 of the Electronic Communications Act, traffic data may be kept by the operators providing the service only for a period of six months. In many cases the victims of computer crimes find out about the unauthorized interference much later - at the end or after the expiry of that period. In such a situation law enforcement authorities and prosecutors are not able to collect electronic evidence.

Some of the problems could be solved by updating the definition of "serious crime" in the Penal code (since 1968). The period of punishment “deprivation of liberty” in that definition should be synchronized with national and international legislation, providing limitation of human rights, in relation to criminal proceedings (European Convention on extradition, Law on the extradition and European arrest warrant, Cybercrime convention).

5.5. Conclusions

- Bulgaria signed and ratified the European Council Convention on Cybercrime in 2005 and transposed Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography.
- Directive 2013/40/EU on attacks against information systems are not yet transposed into the national legislation. However, a number of incriminations of the directive exist already in the Criminal Code into force.
- However, given the fact that drafting and adopting a new Criminal Code involves a length and complex processthat could last a few years, the evaluation team considers that the national authorities should transpose the directives in a separate approach, respectively by amending the Criminal Code into force. The efficiency of the fight against cybercrime needs a consistent and coherent legislation, which offers the necessary instruments to the practitioners.

- In relation to investigative techniques, there are a number of measures for the purpose of gathering evidence (e.g. search and seizure of information system or computer data, real time interception and collection of traffic or content data, order for stored traffic and computer data, order for user information). However the competent authorities consider that there is a real need that special investigation techniques should be available for all cybercrime cases, not only for serious crimes, which do not cover the computer related crimes, for example).
- Another problem of the currently Bulgarian legislation is bound to the fact that the Prosecutor can not request Internet Service Provider to identity the owner of the IP, they must request through the Court, thus preventing a quick investigation.
- The regional units of the CDCOC operate under the sole authority of the Specialised Prosecutor's Office in Sofia, which causes problems in the management of investigations when seizure authorisations have to be obtained from the magistrate upon physical presentation of the evidence (problem of time and distance).
- The Bulgarian authorities reported having difficulties in establishing the jurisdiction in some specific cases and in having access to encrypted files or communication. The seized data are, increasingly, encrypted, they are stored in the cloud, and the volume of data to be analysed is increasingly exponentially (terabyte disks). Private companies are not involved in decryption in criminal investigations, only the National Forensic Institute does this type of activities, but it reported practical difficulties due to the lack of the appropriate technical equipment.
- According to the questionnaire, Bulgarian authorities have not experience in cybercrime committed via the "cloud". It could mean that a number of cybercrimes remains in practice unknown.

- Bulgarian has jurisdiction for acts of cybercrime committed in “the cloud” by Bulgarian citizens and by foreigners who have committed crime affecting the interest of the Republic of Bulgaria or of a Bulgarian citizen. In exceptional cases, a Bulgarian citizen may be extradited to another country only if it is provided in a international agreement to which the Republic is a party.
- The Bulgarian authorities considers that its current regulations regarding the access to the data (only in the case of “serious crime”) and the short period of retain data do not allow the efficacy in investigation on cyber crimes. They thought it is necessary to change the definition of serious crime including crimes punished with a deprivation of liberty from three years, because the cyber crime is punished with a deprivation of liberty to a maximum of three years.

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1. Nature of cyber attacks

One can get an idea about the number of cyber-attacks in the Bulgarian internet space from the reports of the Bulgarian government CSIRT within the Executive Agency "Electronic Communication Networks and Information Systems". These reports contain the number of the signals about violations in the Bulgarian Internet space. Of them, the ones with a higher degree of severity are classified as incidents and are processed following specific procedures. The number of incidents cannot be absolutely accurate due to the fact that the Bulgarian CSIRT does not have its own monitoring system and relies on signals from external resources, which gives no guarantee that the whole Bulgarian Internet space is covered.
The following data about the number of signals (incidents respectively) can be derived from the above-mentioned reports for the first quarter of 2015 and the whole 2014:

	Signals	Incidents
1Q 2015	1061	120
2014	2949	637

The statistical data about the cyber attacks as per type of the attack is also important. Data for 2014 shows that the most frequent attacks were distributed denial of services (44%), followed by infection will malicious codes - malware (32%), botnets – 10%, intrusion attempts - 7 %, spam – 5% , etc.

It can be concluded that this “national” distribution is not substantially different form the international one, i.e. global trends are also valid for Bulgaria.

6.1.2. Mechanism to respond to cyber attacks

There is not a coordinated multidisciplinary mechanism to respond to a serious cyber attack, but according to the national authorities it will be implemented after the adoption of the National Cyber Security Strategy. Interaction is carried out in the framework of the police co-operation with the competent authorities of countries outside the EU. The SELEC Convention provides good opportunities and is a good example of co-operation with the countries in the Balkan region. The efficiency always depends on the willingness of the country to actively co-operate in the respective field.

6.2. Actions against child pornography and sexual abuse online

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

A Central Police Register containing information on all citizens of the Republic of Bulgaria, including those registered for criminal activities is operational at the Ministry of Interior of the Republic of Bulgaria. Due to this database the law-enforcement authorities can successfully identify every Bulgarian citizen. The fact is, however, that Bulgaria does not have a special database designed for identification of victims only.

There are no measures in place to avoid re-victimisation if images/videos are not deleted. CDCOC works with real operational tools (ICACOPS software to track downloading of illicit contents on peer-to-peer network). It also takes part to the Interpol CAPSEND project, currently under tests to be operational at the end of 2015.

There are special procedural measures used to avoid the children's revictimization during the criminal proceedings: hearings are carried out in a special environment and the children are assisted by a psychologist; also they may be hosted in foster care placements. Practitioners declared that as much as possible the hearing of the child victim is limited. Bulgaria has also specialized courts where the victims receive special protection measures during the trial.

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

Statistically, Bulgaria deals with very few sexual offences against minors and lacks reference cases (even if the data is stored in Bulgaria, the connections often come from abroad). No child pornography networks have been detected. More often, there are isolated individuals exploiting very vulnerable children.

In contrast to the approach taken by the Ministry of Justice, the Bulgarian correspondent at Safer Internet, has noted an increase in offences affecting young people in recent years (grooming, cyberstalking, "sextorsion", revenge porn). The Bulgarian correspondent at safer Internet is involved in efforts to transpose the EU Directive on combating child pornography, led by the Ministry of Justice which does not consider a legal definition of child pornography to be necessary. He stated that there are issues with the way in which cases of child pornography are dealt with by the courts in Bulgaria, which have their own methods of interpretation. Outside the cities, judges are few in number and are not very responsive, preferring to focus on other priorities. There is no provision in law for the offence of attempted enticement of a child. The CDCOC is the main entity involved in combating cybercrime, and is responsible for organised crime, which does not follow the same pattern as cases involving paedophiles.

According to the national authorities, there is no problem with the legal definition of child pornography. Prosecutions are not systematically pursued in cases involving an adult who looks like a child (discussion on interpretation during the trial). The difference between eroticism and pornography can be used by the defence. The judge interviewed have nonetheless stated that sentences are too lenient, particularly in relation to child pornography.

The structure put in place by the CDCOC for investigating cyber offences against children comprises three officers in Sofia and one officer in each of the 19 territorial divisions. The Bulgarian services use peer-to-peer surveillance software (ICACOPS-FBI) which enables them to trace illegal content downloads.

The CDCOC has been successfully countering criminal offences related to on-line sexual exploitation of children and the accompanying acts of sexual extortion, sending messages with sexual content/sexting/ and/or cyber bullying. Training and awareness raising campaigns among children of different age have been regularly conducted with a view to prevent them from becoming victims of such crimes.

The CDCOC recently dealt with a case involving a 15 year-old arrested for distributing child pornography (having started at age 10). The proceedings are ongoing and have ramifications for the Czech Republic.

A national image database is planned. The CDCOC is also taking part in the Interpol CAPSEND project which is currently in its test phase with a view to becoming operational from the end of 2015.

In their opinion the way forward is to establish national data base and to use CAPSEND, a program that develop Interpol in order to create database.

Bulgaria is one of the 7 countries which block access to the sites containing child pornography materials.

Awareness campaigns were also implemented, namely in schools, where local police forces task police trainers to raise awareness of children. Theses police officers benefited from a special training.

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

National legislation which transpose Directive 2011/93/EU introduces a legal definition of pornographic performance (Article 93 new item 30 of Penal Code).

Bulgarian law enforcement authorities countering on-line sexual exploitation of children and in particular the Chief Directorate for Combating Organized Crime work in close cooperation with the Bulgarian hot line for safe internet - www.112.net, which is part of INHOPE International Organization. Within the framework of the said cooperation a number of trainings and public-awareness campaigns aimed at students, parents and teachers throughout the country have been carried out during the last years. The trainings have been conducted with the participation of CDCOC officials, the Hot line for safe internet - www.112.net, as well as the International Academy on Cyber-Investigation Training. Further to that, the officials of Cybercrime Unit with CDCOC have developed and are maintaining two web-sites: www.cybercrime.bg and www.spasidete.bg, where information is being published on concrete measures in view of ensuring safety for children surfing the Internet. In addition, the www.cybercrime.bg web-page provides for a user-friendly and accessible platform for submitting signals.

6.2.4. Actors and measures countering websites containing or disseminating child pornography

Under the MoI Act the Bulgarian law-enforcement authorities have at their disposal the necessary legal instruments to immediately remove a domain address revealing scenes of sexual exploitation of children (photos and or/ video clips), that have been hosted on the Bulgarian internet space. In the last five years two domains with the above mentioned content have been identified as hosted at the Bulgarian internet space and have been removed within four hours. The main competences of this unit is the possession of child pornography materials and the extortion. In practice the police officers use some specialized tools, developed by Dutch Police Academy and FBI.

At the end of 2014 the Cybercrime Unit with the CGCOC started to develop a specialized system for blocking access to sites containing child sexual exploitation material which are not hosted in Bulgaria. Since the beginning of 2015 the Bulgarian law-enforcement authorities jointly with Interpol and the Bulgarian Interpol Bureau, have successfully started the process of blocking the access to forbidden sites, using for this purpose Interpol List of Forbidden Domains – "Worst of" list. The initiative is currently being implemented in partnership with two of the biggest Bulgarian internet providers. CDCOC is planning to extend the system to all the other big Internet providers by mid 2015.

The CDCOC has developed a specialized system to manage the process of blocking sites, containing materials with child sexual abuse. One of the functionalities of the system allows for detecting other sites with such content that are not included in the Interpol restrictive list ("Worst of" list). After analyzing the content of these sites, they are being entered into the filter and the domains themselves are sent to the General Secretariat so that they can be included in the restrictive list. In such a way Bulgaria tries to contribute to up-dating the List.

CDCOC is the authority responsible for blocking the access and removing web pages containing child sexual exploitation material. The private sector in Bulgaria is familiar with this initiative of the law enforcement authorities and they can notify CDCOC in case they detect such pages with a view to undertaking follow-up activities, which could be either removal of a web-page (if it is hosted in Bulgaria) or its introduction into a filtering mechanism so that it could not be accessed by users from our country.

Blocking access to web-pages containing child sexual abuse material is on a voluntary basis in partnership with the internet services providers and individual agreements are signed for this purpose with each one of them. Due to the fact that the process of filtering such web pages is relatively new for Bulgaria; we still do not have any experience with urgent cases.
The specialized system developed by CDCOC, which is used to coordinate the filtration of access in Bulgaria to sites with prohibited content, has the functionality to visualize the “territorial” location of the so called banned sites. This means that it can indicate the country where the hosting server is located. Using the channels for bilateral and multilateral cooperation (Europol and Interpol), CDCOC exchanges information and informs the other countries on the existence of a website uploaded in its internet address space.

There is a group within the Cybercrime Unit at CDCOC - MoI, dealing with counteraction to crimes involving illegal internet content. Combating child pornography falls within the competences of this group. It is composed of three officers. In addition to that, The CDCOC has 17 regional offices across the country, where at least one officer is responsible for counteracting those crimes. Thus, the total number of law enforcement officers in Bulgaria involved and successfully counteracting child pornography is 20.

6.3. Online card fraud

6.3.1. Online reporting

In most of the cases the affected citizens and the private sector (mainly bank institutions) provide information to the competent law enforcement authorities. This information is submitted in the form of complaints, signals or answers to questions received by the law enforcement authorities.

6.3.2. Role of the private sector

The national authorities consider that there is sufficient cooperation between private sector and LEAs, meetings are held and the law enforcement officers are getting acquainted with the new trends on online card fraud.

In order to increase the security of non-cash payment and minimize the vulnerability of magnetic stripes, Bulgaria has developed and has patented a special system for protection of the data from the magnetic tape – SKIMPROT. The technology and the product are available to the cardholders.

In the period 2007 - 2008 there was a serious increase in the irregular online transactions through Internet banking. As a result, following an analysis of the bank institutions and recommendations of the specialized Cybercrime Unit, additional measures were taken to enhance security, comprising end user software security and additional measures, such as token devices, personal codes, SMS confirmation, etc. Currently most of the crimes result not from security breaches, but end users negligence.

6.4. Conclusions

- Bulgaria is one of the 7 countries in the world that block the access web pages containing child sexual exploitation material.
- Bulgarian authorities either block the access of a site containing child sexual exploitation material located outside their territory, either remove this kind of sites, if they are located on their territory.
- The initiative of blocking sites containing child sexual exploitation materials which are not hosted in Bulgaria is implemented in partnership with two of the biggest Internet providers and the intention of national authorities is to extend this partnership to all Internet national providers.
- The evaluation team considers that this activity of blocking the access web pages is very efficient in terms of combating child pornography and congratulates the LEAs for being so efficient. This is a good practice that could be shared with the other Member States in order to be applied as much as possible.
- Bulgarian CSIRT collects the statistics of the signals and the incidents reported in cyber attacks . However due to the fact that CSIRT has not its own monitoring system, the is no guarantee that all of the incidents are registered.
- At the national level it doesn't exist a coordinated multidisciplinary mechanism to respond serious cyberattacks.
- Bulgaria does not have a special database designated for identification of cybercrime victims.
- In practice there are some special measures dedicated to avoid the revictimization during criminal proceedings (e.g. limitation of number of hearings of a child victim, keeping secret his/ her identity, special protection measures during the trial).
- The sexual exploitation of children on line is countered also by mean of awareness campaigns organized by the LEAs namely in schools.

- The Cybercrime Unit within CDCOC developed and maintains two web sites where concrete measures are published in view of ensuring safety for children using Internet. There is also a platform where signals and complaints can be submitted on line.
- The cooperation between private sector and LEAs is well functioning, the Internet providers report on a voluntary basis the web-pages that contain child sexual pornography material.
- The cooperation with telecoms equipment providers raises some difficulties in obtaining technical codes required for smartphone analysis and the cooperation with the major American operators is patchy. Bulgaria has started a dialogue with these entities and relies mainly on Europol data.
- In terms of online card fraud reporting, the citizens and private sector report on a voluntary basis the incidents and submit complaint. Nevertheless it seems there is no legal obligation for the private sector to make complaints or to provide information.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

There are not any specific rules, the general procedures on information exchange and co-operation are being followed.

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

The Bulgarian authorities have provided some examples of major international cases, which had very good results in the fight against computer crime, carried out with the support of EUROPOL:

1. An international police operation was carried out in July 2011 with the participation of Bulgaria, Italy, US Secret Service and Europol, called NIGHT CLONE CARD (the Bulgarian Shock operation) aimed at neutralizing an organized criminal group comprised mostly of Bulgarian citizens and engaged in skimming and misuse of payment instruments. The operation was described by Europol as the biggest one against payment cards fraud. In its framework, 73 European arrest warrants were issued by Italy. A total of 59 persons were arrested, of which 48 in Bulgaria, 7 in Italy, 2 in the U.S. and 2 in Spain.

2. In December 2012an international police operation named CLONING CONNECTION was carried out with the participation of Bulgaria, Italy and Europol (the Bulgarian Shock 2 operation) aimed at neutralizing an OCG engaged in skimming and misuse of payment instruments. The investigation was supported by Europol (FP TERMINAL) by means of preparing analytical reports on established links with other cases and investigations in the EU. Within its framework 64 European arrest warrants were issued by Italy. 51 persons have been arrested, of which 40 in Bulgaria.

3. The joint IMPERIUM operation of the Bulgarian and the Spanish police services, aimed at dismantling an organized crime network, involved in different criminal activities (ATM skimming, fraud, counterfeit documents, misuse of payment instruments) was carried out in end September 2014 in co-operation with Europol. 31 arrests and 40 house searches were carried in the framework of the operation in different towns of Bulgaria (Sofia, Bourgas and Silistra) and Spain (Malaga). 8 criminal laboratories were discovered and dismantled.

4. Within the ONYMOUS operation of November 2014 law enforcement and judicial agencies around the globe undertook a joint action, coordinated by Europol, FBI, ICE, HIS and Eurojust against dark markets running as hidden services on the Tor network. The action was aimed at stopping the sale, distribution and promotion of illegal and harmful items, which were sold on online dark marketplaces. 410 hidden services were taken down as a result of this operation and 17 vendors and administrators were arrested. 1 million USD worth of Bitcoins, 180,000 Euro in cash, drugs, gold and silver were seized.

The Bulgarian authorities highly assess the work of Europol within the established Focal Point. Also they appreciate as very beneficial to their work the setting up of the European cybercrime centre at Europol.

They consider that the future Internet Referral Unit in Europol also have a significant added value to the member States common efforts to remove the illegal content in Internet.

In the framework of the cooperation with ENISA the following initiatives, which contributed to the enhancement of the capacity and strengthening co-operation between the competent authorities, have to be mentioned:

- consultations related to the foundation of CSIRT

- training

- participation in cyber-trainings, organized by ENISA

- participation in different fora, organized by ENISA.

The functioning at the time models has been successful and effective enough. We expect the future Internet Referral Unit in Europol also to have a significant added value to the Member States joint efforts to remove the illegal content in internet.

Bulgaria is a member of the European Union Cybercrime Task Force since 2011 and is represented at the group meetings.

7.1.3. Operational performance of JITS and cyber patrols

Bulgaria participated up to day to 4 JITs on cybercrime - especially, skimming and payment card fraud. The investigation in one of the JITs is still ongoing.

They have not yet participated in cyber patrols, but part of the envisaged of the cyber patrols are carried out by employees of the specialized Cybercrime Unit without using the term cyber patrols.

In their opinion, JIT is an effective tool for the timely collection of evidence and a means of enhancing trust among national authorities, involved in the JIT. It can contribute to the shortening of the time for investigation and timely closing of cases at the pre-trial phase. Some of the cases, where JIT were set up ended with a conviction, and in some of the cases the judgements were final in the first instance. There is a growing interest in the Bulgarian national authorities to use this tool for judicial cooperation.

Our overall assessment of this tool of cooperation is that it is extremely useful in the investigation of complicated cases with an international element. The advantages of using JIT, in addition to the option for a comprehensive evaluation of cases and maximization of the demand for a wide range of criminal liability of persons who have committed a crime in the territory of different countries, are as follows:

- There is a possibility for direct use of the evidence gathered in each of the participating countries for the purpose of prosecution, and a possibility for direct exchange of information between members of JIT, without the need to formally forward letters rogatory. The latter, in turn, contributes to achieving higher speed of the pre-trial phase;

- A possibility for directly requesting investigative measures between team members;
- A possibility for team members to be present during the carrying out of investigative actions in all jurisdictions covered, which would help to overcome language barriers in examinations, etc.;
- Building trust between practitioners in this area from different jurisdictions;
- A possibility for Europol and Eurojust to participate with direct support and assistance;
- A possibility for applying for funding and getting funding;
- Raising awareness about conducting international investigations and creating conditions to achieve better results from them.
- The national member at Eurojust and the assistant of the national member have been involved in JIT together with experts from Europol. Their involvement in JIT creates a good opportunity for coordination, communication, exchange of information in real time, especially in the cases where, within the framework of JIT, a joint day of action is conducted, where actions are coordinated by a Coordination centre, based at Eurojust.
- Since both institutions have been set up to support the Member States in their fight against serious crimes, their respective jurisdictions and functions presuppose that Eurojust and Europol play an important role in the joint investigation teams.

Especially at the stage of preliminary assessment and negotiations, the two organizations can assist Member States by providing legal advice and expertise from participation in JIT. Furthermore, rooms for meetings and interpretation are at the disposal of the Member States. Moreover, given their role in the exchange of information and coordination of mutual legal assistance, Europol and Eurojust could identify cases suitable for setting up a JIT, and then ask the Member States to take action on this request. Although the participation of Europol and Eurojust in the setting up and operation of JIT is not mandatory, the two organizations play a crucial role in ensuring efficiency and operational capacity of JIT and thus – the ultimate success of the investigation.

The Eurojust JIT Funding project encompasses financial support to cover travel/accommodation and interpretation/translation expenses, as well as logistical support. Operational meetings can also be supported by Europol, and coordination meetings – through Eurojust. Participation of national members is extremely important in relation to: consultations at an early stage concerning the suitability of a particular case for JIT, if compared to traditional means; consultation at an early stage related to the practical and legal aspects regarding the JIT agreement and its provisions; providing premises for meetings, including translations and secure environment for the negotiation and coordination meetings; sharing experience related to JIT and the main tasks of coordinating and supporting cross-border investigations; providing analytical support; facilitating the exchange of information and implementation of international mutual legal assistance with other non-participating countries; advice on current availability, conditions and procedures for financing and rental of equipment, including the use of mobile offices.

- The National member of Bulgaria for Eurojust has always provided active assistance to prosecutors both in the negotiations for setting up JIT and in their work, termination and evaluation.

Supplementary information concerning the Joint Investigation Teams was offered by the national authorities after the evaluation visit:

JIT „ANADE" (Bulgaria, Spain, Eurojust and Europol) is a project which includes the exchange of information regarding establishing of all individuals in OCG, which was responsible for illegal activities connected with forgery of mean of payments other than money. Also among all aims was that to find the main base, where the perpetrators made all skimming devices and other similar technics.

On 16/01/2014 were made joint and coordinate actions by Bulgarian and Spanish competent Police in Karlovo, Bulgaria and Spain, when were arrested 13 Bulgarian citizens.
Then operative actions were supported by Eurojust. In Bulgaria and Spain were located Europol experts, even in Spain there was mobile office. In February 2014 was conducted the second phase of the operation. In the framework of JIT after request from State Agency National Security and National Investigative Service in mart 2014 in Bulgaria joined technical expert from Europol. He helped by the conducting of technical expertise. The final results were that 25 Bulgarian individuals were arrested.

The second successful JIT was „JIT LYON"- Bulgarian OCG- organized criminal group was investigated for skimming in France, Austria, Switzerland and Germany. The illegal withdraws were committed in these countries including USA. From 19/05/2014 till 23/05/2014 in Silistra, Bulgaria was finished the final stage of the operation including Europol experts with mobile office. As a result of this French police arrested 11 Bulgarian citizens, over 30 addresses were searched, 3 workshops for production of skimming equipment were fined and also officers at the all addressed performed checks in data bases of Europol via mobile office.

7.2. Cooperation between the Bulgarian authorities and Interpol

Cooperation is carried out through Interpol in the cases which do not involve an EU Member State. In theses cases we use the possibility to communicate with third countries through the Interpol channel.

7.3. Cooperation with third states

In the context of the cooperation with the USA FBI agents specialized in countering cybercrime are regularly seconded at the Cybercrime Unit at the CDCOC since 2010.

The fact that most of the countries in the Balkan region are not EU members can be regarded as impediment in the process of cooperation with those countries.

As a good practice can be mentioned the cooperation with SELEC as the organization comprises all of the Balkan countries. The involvement of Europol/EC3/Eurojust brought an added value to cases related to third countries. The necessary steps have been undertaken to raise the awareness of the European law enforcement agencies on the opportunities for cooperation with third countries and private companies based in third countries, including though presentations during various expert meetings at Europol.

7.4. Cooperation with the private sector

The information received in the GOVCERT Bulgaria on specific IP addresses in the Bulgarian internet space, which are the source or target of cyber attacks, is sent to the respective internet providers. GOVCERT can recommend, but it cannot oblige them to take action to counteract those attacks.

Explicit responsibility for services offered by the internet providers is not implied under the national law. On the other hand there is an obligation for the service provider to block a content provided through its service when it is notified for illegal content.

The national authorities have cooperated directly the private companies that have their main quarters in a third State. In some cases requests have been sent directly to foreign companies, although they do not have representatives in the country. Here again the question is open on the competence as it is possible not to receive an answer in some cases. The national legislation does not provide the possibility for search and seizure from a distance.

The law enforcement bodies carry out constant information exchange on national and international level. The key goal is timely provision of information, maintaining contacts with the international partners through the various channels. Court-investigative orders are carried out, JITs are concluded, EAWs are implemented. Our country has representatives in international law enforcement institutions that facilitate cooperation. If needed operational meetings with international partners are organised.

CDCOC works with most of the major international Internet companies, namely using their usual channel dedicated to LEAs. CDCOC also uses the EPE (Europol platform) which provides an information manual and guidelines about relations with GAFA.

A dialogue has been established with the main international social media actors, such as Facebook and Twitter, with which CDCOC communicates via a portal for law enforcement agencies. Dialogue with Gmail and Microsoft is more difficult.

The national authorities consider that links with banks must be further strengthened: currently CDCOC meets twice a year representatives form the banks sector.
Cooperation with major international producers of electronic communication devices has been more difficult to establish since these companies are often reluctant to disclose all technical features and codes etc.

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

There is no any specific legal basis in Bulgaria for provision of Mutual Legal Assistance (MLA) for cybercrime, the general legal framework is fully applicable.
The Ministry of Justice is designated as Central Authority responsible for sending and answering requests for mutual assistance at the trial stage and requests for extradition under the Convention on Cybercrime and under the Convention on Mutual Assistances in Criminal Matters /except from MLA for legal assistance in pre-trial proceedings/.

The Supreme Cassation Prosecutor's Office is responsible in respect of receiving/sending requests for mutual assistance at the pre-trial stage and requests for provisional arrest under the Convention on Cybercrime and a under Convention on Mutual Assistances in Criminal Matters /regarding pre-trial proceedings/as well. The authorities who take decisions on requests are the relevant Courts or the Prosecutor's Offices with territorial competence for initiating and executing the requests. Under 2000 MLA Convention, requests for mutual assistance shall be made directly between competent judicial authorities. Bulgaria accepts and executes requests for legal assistance, received by fax and e-mail. There are no separate authorities responsible for receiving/sending requests for MLA on cybercrime.

Various investigative actions may have to be performed depending on the specifics of the case. Some of them - search and seizure, disclosure of bank secrecy, special intelligence means /observation, tapping, surveillance, penetration, marking, interception of mail and computerized information, controlled delivery, trusted transaction and investigation through an undercover officer/ require an authorization by the respective judge, upon request from the prosecutor. Except from disclosure of bank secrecy, where the district judge shall rule on the motion by a motivated judgment within 24 hours, fixed term is not set for the respective Court to rule in case of request for search and seizure or for use of special intelligence means. However, in these cases the Court usually takes its decision within a few hours.

The Bulgarian authorities may, if needed, turn to the mediation of Eurojust, if the case is in its competence. Informal consultations by phone or email are also held if necessary.
The national authorities have not yet experienced offences committed in the "cloud", so they could not provide specific answers regarding this particular matter related to the mutual legal assistance.

Interaction is carried out in the framework of the police co-operation with the competent authorities of countries outside the EU. The SELEC Convention provides good opportunities and is a good example of co-operation with the countries in the Balkan region. The efficiency always depends on the willingness of the country to actively co-operate in the respective field.

The Bulgarian investigation services highlight that shortened data retention period (following the decision of the European Justice Court) also prevented the investigation of who is using an IP address also in some international cases.

This situation results in the fact that criminals may never stand trial: the Plovdiv Court noticed that on these last years, only one fraud case out of 17 reached trial, as for the others, victims were not identified or heard on time.

Too often, they have to provide in the trial, only evidence which have been gathered in Bulgaria and as a consequence, criminals are lightly sentenced.

The delays involved in international mutual legal assistance in criminal matters mean that it is not possible to process cases within the legal time limit allowed for provisional custody (eight months according to the national law), even though the investigations can involve many states at once (Germany, France, Spain, Switzerland, etc.). They prefer to use the joint investigation teams, which they consider appropriate for dealing with organised crime. The Bulgarians consider that these operations are primarily of benefit to their foreign partners.

They would like Eurojust to be more closely involved, although personal contacts are considered very useful in facilitating investigations. Their main partners are Italy, Spain, France and Germany.

7.5.2. Mutual recognition instruments

No specific statistics have been provided with regard to the application of various mutual recognition instruments. The Bulgarian authorities have not any experience in using EU mutual recognition instruments in relation to prevention, investigation and prosecution of cybercrimes.

7.5.3. Surrender/Extradition

According to Art.5 and Art.36 of Extradition and European Arrest Warrant Act, extradition shall be granted, or European arrest warrant may be issued or a surrender on the bases of a European arrest warrant shall be carried out, where the act constitutes a criminal offence under the Bulgarian law and under the law of the requesting State which is punishable by deprivation of liberty or under a detention order for a maximum period for at least one year. Extradition shall also be granted for the purpose of serving a prison sentence or detention order by the person concerned, as made it in the requesting state for a period of at least four months. There are exceptions for European arrest warrant – no double criminality shall be required for the list of crimes under art.36 of Extradition and European Arrest Warrant Act.

Acts unique for information systems, in particular those, related to cyber attacks, are criminalized under art.319a to art.319 f of the Penal Code. An offender, who commits such a crime, may be extradited only if essential elements of the crime are present and significant damage or other grave consequences have occurred as a result of the crime.

Content-related acts, in particular those related to child sexual abuse online and child pornography. Art.159, par.3 of Penal Code covers these issues. Crime under art. 159, par.3 is punishable by imprisonment of up to three years, so the offender may be a subject of extradition.

Acts where computer/IT systems are involved as a tool or target, in particular online card fraud.Art.249 and Art. 212a of the Penal Code are applicable. Computer fraud is punished by imprisonment from two to eight years under Art.249 and from one to six years under Art.212a. In this regard there are not obstacles for extradition of a person who has committed a crime as describe above.

A request for extradition shall be submitted by a competent authority of the requesting State in writing with the Ministry of Justice of the Republic of Bulgaria. Diplomatic channels, International Criminal Police Organization, or other means of communication may also be accepted. A request for extradition of a person who has committed an offence triable by Bulgarian court shall be made by the Prosecutor General – in respect of an accused or convict whose sentence has entered into force and the Minister of Justice in respect of trial defendants, at the proposal of the respective court.

A European arrest warrant issued by the competent authority of a MS shall be executed by the District Court on the territory of which the person is located. The European arrest warrant shall be received directly by the District Court, under the jurisdiction of which the person is located, except for the cases where it is effected through SIS, EJN or INTERPOL.

A European arrest warrant in the Republic of Bulgaria shall be issued by the respective prosecutor with regard to an accused or a person convicted by an enforceable sentence and by the respective court in respect of a defendant.
No specific statistics have been provided with regard to surrender/extradition cases on cybercrime.

7.6. Conclusions

- There is a pragmatic, willing and open approach to international cooperation, especially European cooperation.
- The Bulgarian police cooperate closely with Europol/EC3 and Eurojust.
- Bulgaria has an impressive record of accomplishments regarding JITs in cybercrime investigations.
- However, Bulgarian authorities consider mutual legal assistance as being too slow in practice, which may hamper investigations. The custody cannot exceed 8 months during the pre-trial phase, which can create some problems, as investigations may need sequential checking in many countries. The length and complexity of mutual legal assistance does not suit to basic identifications (e.g. IP addresses). Furthermore, the requirement to identify a victim before indictment seems to be a particular problem in this respect, especially when the victims are located outside its territory.
- Bulgaria is actively involved in cooperation with ENISA, especially by participation in cyber trainings and different other specialised fora.
- CDCOC takes actively part in the EMPACT actions (card frauds and cyberattacks) as it did in many international skimming cases on these last years. In the area of combating child pornography, the CDCOC seems to be well integrated into the international mechanisms (use of ICACCOPS software, participation in Interpol's CAPSEND project, close synergy with the SAFER INTERNET scheme). The creation of a national database on child pornography cases is being planned.
- Bulgaria has an effective cooperation also with Interpol, which offers training on the proper use of data bases.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

In Bulgaria we have witnessed an increase in cybercrime offences with computer fraud being the most widely spread, but also credit card fraud and data deletion. Also phishing and identity theft are connected to the widespread usage of social networks. The objectives of the MoI Academy training strategy are focused on investigating cybercrime and also collecting and securing digital evidence. The lectures on these crimes are included in our basic training for police cadets obtaining bachelor degree and also there is a module in the initial training for police officers working in the units for combating economic crime and organized and serious crime. 6 lecture hours are devoted to cybercrime. Currently we are planning an e-module on cybercrime which will be delivered on the Ministry Intranet network. The idea of the e-learning is to put some lectures and teaching modules online and also to create an electronic library specifically focused on securing digital evidence for first responders and computer crimes investigators.

The types of training activities provided by the National Institute of Justice to magistrates (police investigators are also invited to participate in most of these activities) are specified in the information under question 3 here bellow.

The officers of the specialized Cybercrime Unit of CDCOC also participate in trainings, organized by Europol, OLAF, UCD and the FBI.

Seminars are organized at national level, in which the police officers, prosecutors and judges are taking part.

Currently there is no training module on cybercrime for the international operational police cooperation staff. As liaison officers appointed abroad may provide a real asset in cooperation with some countries (for example third countries outside EU), they could usefully be trained or made aware about needs of the operational services. This could be performed during special training session or through specialised and dedicated materials which could be shared in the liaison officers network.

In 2009 was established the International Cyber Investigations Training Academy (ICITA), a non-governmental organization aimed at raising the awareness of all stakeholders in the investigation and the criminal prosecution.

This non-governmental organization focuses on strengthening public-private partnership, training public and private actors (banking and telecom sectors), prevention activities (raising awareness of cyber professions among secondary school students).

In five years it has organized around thirty activities for central and provincial public administrations. Current projects include the development of forensic tools in partnership with the Bulgarian Ministry of Defence, the organization of professional seminars and the development of a methodology for investigating and prosecuting cybercrimes.

The academy also does consultancy work and takes part in public debate on cyber security issues. It closely monitors the ongoing negotiations on EU security rules (the draft Directive on network and information security and the draft Regulation on data protection).

In particular, it monitors the development of the National Cyber Security Strategy, and has criticized the Bulgarian authorities for not involving enough the private sector in this and for seeking to avoid public debate on the matter. As considering itself as an interface between public security actors and the private sector, and considering that it enjoys the trust of both**,** the non-governmental organization would like to steer the drafting of the future strategy, bringing in expertise from the private sector.

However, the academy considers itself limited by its financial resources (regretting the lack of European or national funding) and unable to work more proactively. Its main supporter remains the America for Bulgaria Foundation, which finances its activities and its small team.
For police officers investigating cybercrime there is a specialized module based on CEPOL common curriculum on cybercrime and it is included in their training. No specialized modules exist for judicial experts at the moment.

Usually, for training of the officers the national authorities rely on international courses organized by various institutions. Thus the training of experts complies with the international requirements for developing a computer-technical expertise.

The Academy of the Ministry of the Interior is responsible for the professional training of police officials. The CEPOL common curriculum on cybercrime is used and some of the Academy trainers have actively participated in its development. ECTEG and Europol cybercrime materials are currently not used in the training due to the fact that until recently cybercrimes were investigated by the State Agency for National Security and now with the creation of the General directorate for combating organized crime they will be investigated again by police officers.

The National Institute of Justice is a public institution, which provides training for the Judiciary. In 2012 and 2013 under the Programme for regional training of the National Institute of Justice, the issues related to cybercrime are covered within the trainings "Computercrimes.Art.319a and the following provisions of the Penal Code" (organized by the Pernik District Court) and "Legal practice in cases on money laundering, financial crimes and corruption offenses committed on the Internet" (organized by the Regional Prosecutor's Office). These courses were attended by 27 magistrates (10 judges, 15 prosecutors, 2 investigators) and 5 experts from the Ministry of Interior.

In cooperation with the International Cyber Investigations Training Academy in 2014 the National Institute of Justice developed a specialized training on cybercrime –"Cybercrime. Bank card fraud. Crimes related to skimming devices ". The training was attended by 33 magistrates (22 judges, 6 prosecutors, 5 investigators), 5 Ministry of the Interior officials and 5 experts from the National Security State Agency. The training was included in the Regional training program of the National Institute of Justice for the Courts and Prosecutor's Offices. At the initiative of the Burgas Regional Prosecutor's Office the training was held in a regional format and the content was focused on cybercrime trends associated with the use of mobile devices and social networks. The regional training was attended by 34 magistrates (3 judges, 26 prosecutors, 5 investigators) and 2 clerks.

The curriculum for 2015 for ongoing training of magistrates envisages training under the pilot program of 2014, dedicated to cybercrime and payment card fraud. The National Institute of Justice can offer this training in a regional format - at the initiative of the Courts and Prosecutors' Offices in the country, that have confirmed their participation in the Regional program for the current year.

The approximate cost of one training provided by the National Institute of Justice for 35 participants is 5000 BGN (approx. 2500 Euro).

According to the up-dated information provided after the evaluation visit, The National Institute of Justice provided some training programmes as follows:

In 2012 and 2013 under the Programme for regional training of the National Institute of Justice, the issues related to cybercrime are covered within the trainings "Computer crimes. Art.319a and the following provisions of the Penal Code" (organized by the Pernik District Court) and "Legal practice in cases on money laundering, financial crimes and corruption offenses committed on the Internet" (organized by the Regional Prosecutor's Office). These courses were attended by 27 magistrates (10 judges, 15 prosecutors, 2 investigators) and 5 experts from the Ministry of Interior.

In cooperation with the International Cyber Investigations Training Academy in 2014 the National Institute of Justice developed a specialized training on cybercrime – "Cybercrime. Bank card fraud. Crimes related to skimming devices ". The training programme contained practical topics related to cyber attacks and illegal intrusion in networks. The training was attended by 38 magistrates and other officials (22 judges, 6 prosecutors, 5 investigators and 5 experts from the National Security State Agency).

This training which was included like a pilot project in 2014 is currently envisaged in training schedule of the National Institute of Justice for 2015 (2-4 December 2015) taking into account the high interest of magistrates, MoI and SANS officials to this topic.

The following trainings were carried out by the National Institute of Justice within the Regional training program for the Courts and Prosecutor's Offices:

- "Cybercrime. The new trends related to mobile devices and the social networks", 25 April 2014 for the Burgas Regional Prosecutor's Office. The regional training was attended by 36 magistrates (3 judges, 26 prosecutors, 5 investigators and 2 clerks).

- "Investigation of cybercrimes", 25 October 2013 for the Blagoevgrad Regional Prosecutor's Office. The regional training was attended by 75 magistrates (12 judges, 50 prosecutors and 13 investigators).
- "Crimes related to the internet – practical cases, methodology of the investigation and problems", 18 May 2012 for the Pazardjik Regional Prosecutor's Office. The regional training was attended by 52 magistrates (23 judges, 15 prosecutors, 11 investigators and 3 clerks).
- "Crimes committed by the use of electronic signature", 19 November 2012 for the Veliko Tarnovo Regional Prosecutor's Office. The regional training was attended by 13 prosecutors.
- "Frauds and other crimes committed in the Internet", 26 November 2012 for the Smolyan Regional Prosecutor's Office. The regional training was attended by 22 magistrates and officials (15 prosecutors, 2 investigators and 5 investigators).
- "Computer crimes. Penal characteristics – classifying signs, evidence and tools", 2-3 June 2011 for the Gabrovo Regional Prosecutor's Office. The regional training was attended by 13 judges.
- In July 2015 the Management Board of the National Institute of Justice agreed on a partnership in the project "European judicial cooperation in the cybercrime field." implemented by the Foundation "Bulgarian Institute for legal initiatives" in cooperation with the Center for criminal justice and security studies of Romania. The duration of the project is 10 months as the activities include:
- opening conference for 60 participants;
- elaborating and carrying out of 3 training courses for 60 magistrates from Bulgaria and Romania;
- developing a Handbook in European judicial cooperation in the field of cybercrime;
- closing conference.

It would be more difficult to specify the amount of the expenses for the trainings conducted by the MoI Academy, as it works with a centralized budget, but they can be roughly estimated at (approx.) 2000 BGN (1000 Euro).

Currently there is no training module on cybercrime for the international operational police cooperation staff.

Specialists from the Computer Virusology National Laboratory with the Bulgaria Academy of Sciences /http://www.nlcv.bas.bg/ are involved in the training in the Academy of the Ministry of the Interior with lectures on hacking techniques, computer viruses and social engineering. Information for the activities of the b2center can be found on the internet site b2center.In the 4-th year of the Bachelor's degree program of the Ministry of the Interior Academy, the subject "Countering economic crime" includes lectures focusing on internet investigations, including the examination of historical internet data, such as emails and website posting to identify the author or originator of the internet activity by looking at system artefacts and attributes and online investigations, which focus on the live and active interrogation of online data, such as investigating websites and attempting to determine their physical location.

8.2. Awareness-raising

An information-alerting platform was developed to combat cybercrime - cybercrime.bg, which aims to inform consumers about the threats on the Internet and how to enhance their own security.

Awareness-raising is conducted by both governmental and non-governmental organizations. International Academy for Cyber Investigation organizes campaigns with the aim to raising the awareness of all stakeholders in the investigation and the criminal prosecution.

Also representatives of CDCOC, both at central and regional level, attend periodically various academic lectures, both in schools and in universities, seeking to raise user's awareness and to contribute to the prevention.

Other campaigns are developed by several ISEC projects aimed at prevention and awareness of the population, including the private sector.

Some of the projects are developed with international organizations and address to different categories, as students, parents and teachers.

The National Center for Safer Internet (a non-governmental organization) focus on awareness-raising addressed to the children school: how to protect themselves from the Internet dangers. This NGO has operated in its current form since 2012 and works to improve the online safety of young people. It is a member of the management board of the National Network for Children and of the INHOPE network.

Its work includes prevention activities (campaigns, training, distribution of materials) for the public (parents, children, public actors) with regard to internet use, a website[28], a helpline (for assistance in serious situations) and a hotline for reporting child pornography content. It supports other child protection organizations. Its projects include a training course and the preparation of a handbook for police services.

Its president deplored the decrease of European Union funding for the Safer Internet program.
He works closely with the CDCOC and considers the Bulgarian Ministry of the Interior to be his best partner. However, reported facts are not always systematically communicated to the police.

[28] Safenet.bg

This depends on the initial research carried out by the NGO staff, who take into account the international nature of some cases from the outset and forward the information directly to foreign contacts or to Interpol (even if the data is stored in Bulgaria, the connections often come from abroad).

There are also two web sites - www.cybercrime.bg and www.spasidete.bg - where information on concrete measures to ensure children's safety when they surf the Internet is published.
The National Cyber Security Strategy is expected to define the approaches for developing the relations with the different target groups (citizens, children, end users) as an important aspect of security and both awareness of the population.

8.3. Prevention

With the last amendments of the Law on the Ministry of Interior from January 2015, the prevention is set out as major priority.

Under the legal provisions the prevention is carried out by a complex of measures on the identifying and eliminating of the causes and conditions for committing crimes and other offences.

Periodically CDCOC representatives of the unit, both at central and regional level, attend various academic lectures, both in schools and in universities, seeking to raise user's awareness and to contribute to the prevention. The abovementioned projects with international funding can be referred as private sector involvement in prevention activities.

A project HOME/2010/ISEC/AG/045 aimed at prevention and awareness of end users was implemented in 2012 in cooperation with the private sector. Videospots were developed which, completely free of charge, are broadcast on several national television and internet media. On preventive purposes is realized also this ISEC project, carried out by the unit, within which was created the website spasidete.bg. CDCOC-MoI is a partner in the completed project within the ISEC Bulgarian Cyber Center of Excellence for Training Research and Education - b2centre.com.

8.4. Conclusions

- It seems that Bulgaria has not yet established a permanent training structure to respond the LEAs needs in cybercrime.
- The National Institute of Justice should be encouraged to provide more regular specific training for judges and prosecutors.
- A non-governmental association - International Academy for Cyber Investigation - organizes, on a regular basis, training for police officers and prosecutors, with funds provided mainly by the private sector.
- The specialised police officers participate in training organized by Europol, OLAF and FBI.
- Awareness campaigns are organized on a more regular basis and involve especially the Cybercrime Unit within CDCOC and non-governmental organizations. The campaigns addresses to different categories of citizens that could be affected by cybercrime activities. The target is to create awareness among private sector and specific categories of citizens (children, parents, teachers).
- Bulgarian authorities implemented and developed, in cooperation with private sector, several projects aimed to the prevention of cybercrime, including by broadcasting of videospots, completely free of charge.
- Training, awareness and prevention campaigns seem to be mostly supported by EU projects, non-governmental associations and private sector. The efforts to find funds and alternative solutions in order to implement projects dedicated to training, awareness and prevention campaigns are commendable but cannot replace the funding by the state.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Bulgaria

9.2. Recommendations

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

Bulgaria should conduct a follow-up on the recommendations given in this report 18 months after the evaluation and report on the progress to the Working Party on General affairs, including GENVAL.

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

9.2.1. Recommendations to Bulgaria

1. Bulgaria should transpose into the national legislation the EU instruments, respectively, Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.

2. Bulgaria should draft and adopt the National Security Strategy as soon as possible, preferably with consultation of the involved stakeholders.

3. Bulgaria should consider to extent the competence of the specialised police Unit for Trans-Border Organized Crime to investigate a larger part of cybercrime offences due to its high level of specialisation and experience in this field.

4. Bulgaria should also consider to designate specialised prosecutors in cybercrime cases, who will be also competent for cases which are note linked to organised crime.

5. Bulgaria should develop a mechanism to provide standardised and comprehensive statistics on investigations, prosecutions and convictions and reported incidents related to cybercrime, in order to have a clear picture of the overall cybercrime phenomenon, including the dark figure.

6. Bulgaria should develop a comprehensive programme of training on cybercrime issues for all stakeholders and practitioners involved in combating cybercrime, including liaison officers abroad and the staff of the National Forensic Institute, especially by consolidating the capacities in the field of the National Institute of Magistracy.

7. Bulgaria should further explore the possibilities offered for training by Eurojust, Europol and ENISA, which could cover all the practitioners (police officers, prosecutors and judges).

8. Bulgaria should be encouraged to continue raising awareness of the population about the different forms of cybercrime, especially for children which are the most vulnerable targets of the criminal offenders.

9. Bulgaria is encouraged to enhance further contact with the private sector, especially banks, in order to increase the rate of reporting the cybercrime incidents in order to get better results in combating cybercrime offences.

10. Bulgaria should consider what action to take as follow-up to the report and to share the progress made and the results achieved with the GENVAL working group, 18 months after this evaluation.

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

1. Following the annulment of Directive 2006/24/EC of 15 March 2006, the European Union and Member States are encouraged to reflect on the most appropriate way to remedy the lack of harmonisation of national laws regarding the electronic traffic data retention, while fully considering both operational needs and the protection of fundamental rights.

2. Member States which have not yet ratified the Council of Europe Budapest Convention on Cybercrime and its additional protocol are encouraged to do so.

3. Member States are recommended to consider possible solutions allowing more efficient investigations on data stored or located in the cloud.

4. Member States should consider the Bulgarian good practice in blocking and filtering web sites with illegal content.
5. Member States should consider following the Bulgarian example and use JITs more often in cybercrime investigations.

6. The European institutions should increase the EU funding to help Member States to organize more training for national practitioners in cybercrime.

7. The European Union and its Member States should study the possibility to simplify the exchange of information, as for example, traffic data through police channel within the Union.

8. The European Union and its Member States should reflect how to improve the cooperation with the major international telecommunication companies.

9.2.3. Recommendations to the Eurojust/Europol/ENISA

1. Eurojust, Europol and ENISA should consider raising awareness of the services and the existing possibilities for cooperation and specialised training that they offer in the area of cybercrime.

2. Eurojust, Europol and ENISA should consider actively supporting events that strengthen international cooperation with regard to combating cybercrime, such as the Global Cyber Space Conference.

Annex A: programme for the on-site visit

7th Round of Mutual Evaluations - Bulgaria - 22-25 JUNE 2015

Monday 22-06-2015

- PM arrival GENVAL experts in Sofia (expected in the afternoon)
- between 20.00 - 21.30 Informal meeting and introductions of experts team

Tuesday 23-06-2015

- 9.00 - 10.30 Meeting with the Deputy Minister of Interior
  - introductory meeting and presenting the teams – competent institutions in Bulgaria (MoI, MJ, MTITC and SPOC) and main aspects of the fight against cybercrime.
  - legal framework for combating cybercrime – a working meeting with the participation of experts from the Ministry of Justice.
- 11.00 - 13.00 Presentation of the main activities of the Cybercrime Unit of CDCOC and the practice of investigating cybercrime
- 13.00 -14.30Lunch
- 14.30 -16.00Meeting with representatives of Research Institute of Forensic Science and Criminology - forensic expertise in combating cybercrimes

Wednesday 24-06-2015

- 9.00 - 11.30 Supreme Prosecutor's Office of Cassation - investigation and prosecution of cybercrime (meetings with representatives of SPOC, Sofia District prosecutors Office, Sofia City Court)
- 11.30 - 12.30Ministry of Transport, Information Technologies and Communications (MTITC)
  - Electronic Communication Networks and Information Systems Executive Agency– presenting the activities of GOVCERT
  Computer Security Incidents Response Team (GOVCERT - Bulgaria)
- 12.30 - 13.30 Lunch
- 14.00 - 15.00 International Cyber Investigation Training Academy- initiatives of public - private cooperation

- 15. 30 - 17.00 National Centre for Save Internet- initiatives of public - private cooperation
- 19.30 - 21.00 Dinner on behalf of the Deputy Minister of Interior

Thursday 25-06-2015

- 9.00 - 11.00 Travel to Plovdiv (transport to be provided)
- 11.00 - 12.30 District Prosecutor's Office – Plovdiv - Investigation and prosecution of cybercrime
- 13. 00 - 14.30Lunch with representatives of District Prosecutors Office
- 15.00 -17.00 Travel to Sofia
- 17.00 -19.00 Debriefing at the MoI

Annex B: Persons interviewed/met

Person interviewed/met	Organisation represented
Mr. Phillip Gounev, Deputy Minister of Interior	Ministry of Interior
Mrs. Dora Zgurovska, Head of Unit, EU and International Cooperation Directorate	Ministry of Interior
Mr. Nikolay Danovski, EU and International Cooperation Directorate	Ministry of Interior
Mr. Alexander Stefanov	Ministry of Justice
Mr. Florian Florov	Ministry of Justice
Mr. Stefan Dzolev, Deputy Director of CDCOC;	Countering Organised Crime Chief Directorate
Mr. Yavor Kolev, Head of Combating Transnational Crime Department in CDCOC	Countering Organised Crime Chief Directorate
Mr. Kiril Milev, Head of Combating Cybercrime Unit, CDCOC	Countering Organised Crime Chief Directorate
Mr. Lyubomir Tulev, Combating Cybercrime Unit, CDCOC	Countering Organised Crime Chief Directorate
Mr. Vasil Petkov, Combating Cybercrime Unit, CDCOC	Countering Organised Crime Chief Directorate
Mr. Plamen Vidolov, Head of Department	Research Institute of Forensic Science and Criminology of MoI
Mr. Vasil Genov, Head of Unit	Research Institute of Forensic Science and Criminology of MoI

Mr. Tsvetomir Yosifov, Head of International Department	Supreme Prosecutor's Office of Cassation
Mrs. Emilena Popova, International Department	Supreme Prosecutor's Office of Cassation
Mrs. Daniela Masheva, Analytical Department	Supreme Prosecutor's Office of Cassation
Mrs. Mariyana Lilova, International Department	Supreme Prosecutor's Office of Cassation
Mr. Ivan Koev, judge	Sofia City Court
Krasimir Simonski, Executive Director	GOVCERT
Mr. Vasil Grancharov	GOVCERT
Mr. Todor Dragostinov	GOVCERT
Mr. Rumen Popov, prosecutor	District Prosecutor Plovdiv
Mr. Galin Gavrailov, Deputy	District Prosecutor Plovdiv
Mr. Plamen Uzunov, Director	Regional Police Directorate Plovdiv
Mrs. Albena Spasova	International Cyber Investigation Training Academy
Mr. Georgi Apostolov	National Center for Save Internet

Annex C: List of abbreviations/glossary of terms

List of acronyms, abbreviations and terms	Acronym in original language	Full name in original language	English
CAPSEND			Central Aggregation Point for Sexual Exploitation Network Data
CDCOC			Chief Directorate Combating Organized Crime
ECTEG			European Cybercrime Training and Education Group
EMPACT			European Multidisciplinary Platform against Crime Threats
ENISA			European Union Agency for Network and Information Security
EPE			Europol Platform
ERA			Academy for European Law
GENVAL			Working Party on General Matters including Evaluations
GOVCERT			Computer Security Incidents Response Team
ICITA			International Cyber Investigation Training Academy
INHOPE			International Association of Internet Hotlines
IP			Internet Protocol
MLA			Mutual Legal Assistance
MoI			Ministry of Interior
MoJ			Ministry of Justice

List of acronyms, abbreviations and terms	Acronym in original language	Full name in original language	English
MTITC			Ministry of Transport, Information Technologies and Communications
NSSA			National Security State Agency
RIFSC			Research Institute of Forensic Science and Criminology
SELEC			South East Europe Law Enforcement Convention
SPOC			Supreme Prosecutor's Office of Cassation