Council of the
European Union

Brussels, 8 March 2016
(OR. en)

13022/1/15
REV 1 DCL 1

GENVAL 46
CYBER 99

DECLASSIFICATION

of document:	13022/1/15 REV 1 RSTREINT UE/EU RESTRICTED
dated:	18 January 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 Romania

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, 18 January 2016
(OR. en)

13022/1/15
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 46
CYBER 99

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 Romania

ANNEX

EVALUATION REPORT ON THE

SEVENTH ROUND OF MUTUAL EVALUATIONS

"The practical implementation and operation of European policies on prevention and combating Cybercrime"

REPORT ON ROMANIA

Table of Contents

1 EXECUTIVE SUMMARY

The mission to Romania was organised very well, including logistics. The Romanian authorities met were very well prepared and the visit took place in a very pleasant and warm atmosphere. The programme was intensive and comprehensive. The evaluation team had the opportunity to talk to representatives of the different authorities involved in prevention and fight of cybercrime, including officials from the Ministries of Internal Affairs, the Ministry of Justice, the Ministry of Education, from the National Institute of the Magistracy, the National Police, the Prosecution Office, CERT-RO, etc. All the authorities met were happy to exchange views in an informal way with the evaluation team. They all show a high degree of commitment to preventing and fighting cybercrime.

Romania's approach towards cybercrime is well-established and is multidisciplinary. Romania is committed both at the national and the international levels in terms of preventing and combating cybercrime. Romania is particularly keen on prevention and also on enforcing the law. National authorities encountered are committed to making Romania a model country as regards fighting cybercrime. The intelligence service, CERT-RO, the police, the prosecution service and the judiciary all cooperate with each other. It was clear from the visit that police and prosecutorial authorities do work closely together, at least regarding cybercrime, and can rely on long-established practice and mutual trust. The intelligence service and CERT-RO are also very much involved in fighting cyber-incidents and cybercrime. All these authorities seemed to be perfectly aware of their role and competence, and at ease with their roles. It was always clear to them (e.g. CERT-RO and the intelligence service) when to contact police authorities in cases where an alert affecting cyber-security might plausibly be turning into criminal behaviour. The general coordination of the various authorities involved in cyber-security is left to a Cyber-Security Operational Council. However, for the evaluation team it was not clear who really has the role of general coordinator.

A more coordinated approach on statistics would be also beneficial to align the police and prosecutors statistics so as to have reliable statistics on the outcome of each case.

Romania has been on the frontline in the fight against cybercrime since 2000. At the national level, specialised units were created as far back as 2003 within the police and the General Prosecutor's Office as well, dedicated to investigating and prosecuting cybercrime. At the international level, Romania is engaged on many fronts: participating as a partner and providing expertise in EU and Council of Europe projects, it was a driver of EMPACT in 2012-2013, participates in all three cybercrime areas within EMPACT and in the Cybercrime Convention Committee (T-CY) on trans-border access to data and is also a member of the Cloud Evidence Group established in December 2014. Since June 2014, Romania is also vice-chair of the T-CY. In addition, Romania hosts the Office of the Council of Europe in Bucharest (C-PROC), which is responsible for assisting countries in a strengthening of justice capacity to respond to challenges posed by cybercrime and electronic evidence on the basis of standards established by the Budapest Convention.

The fight against cybercrime in Romania is part of a more global approach to protecting and guaranteeing cyber-security. A consistent legal framework is in place in Romania both at substantive and procedural level. The implementation of Directive 2013/40/EU on attacks against information systems should further improve Romanian law in this area. Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and the sexual exploitation of children and child pornography has been to large extent implemented. The evaluation team was also exposed to information from a legislative proposal aiming, among other things, to ensure a more coherent and reliable information flow from the private sector. During the evaluation visit, however, the Constitutional Court declared the law implementing the Cyber Security Strategy unconstitutional.

Cooperation with the private sector takes place on *ad hoc* basis. It was also explained that meetings take place with police and prosecutors to instruct the private sector on collecting information in a way that means it can be used as evidence in court. The police are also quite engaged with the private sector with respect to training (on reporting mechanisms for instance). Cooperation with ISP providers has occurred through the Romanian association of ISPs, where the police discuss and debrief on possible cases, *modus operandi*, etc.

Very frequently, the issue of data retention was raised, as well as the consequences of the judgment of the Court of Justice of the European Union of 8 April 2014 declaring Directive 2006/24/EC invalid. Following that judgment, the Constitutional Court of Romania also declared Law 82/2012, transposing the Directive, unconstitutional. Because data retention laws have also been annulled or declared unconstitutional in other Member States, Romanian authorities expressed concern about the negative impact of the lack of any regulatory instrument creating an obligation for the private sector to retain data. Such a loophole has a negative impact on investigations and prosecutions of cybercrime cases where data is not preserved at all or simply too briefly to be available as intelligence, let alone evidence.

At the margins of very close cooperation between the police and the prosecution service, judges are also organising themselves with a view to increasing their knowledge and readiness to deal with cybercrime cases. Training courses on cybercrime have been and are being organised for police officers, prosecutors and judges. Romania has started a project called CYBER-EX aiming at establishing a centre of expertise on cybercrime at national level encompassing police officers, prosecutors and judges. Europol/EC3 and Eurojust are well known and asked for assistance.

Taking into account the ambitious approach and active role Romania plays in terms of countering cybercrime and the significant resources the country has allocated for this purpose, the opinion of the evaluators is unquestionably positive.

2 INTRODUCTION

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

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

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

Moreover, the Council Conclusions on the EU Cybersecurity Strategy of June 2013[4] anticipated the swift ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[5] of 23 November 2001 by all Member States and emphasised in their preamble that "the EU does not call for the creation of new international legal instruments for cyber-issues". The Convention is supplemented by a Protocol on acts of xenophobia and racism committed through computer systems[6].

Experience from past evaluations shows that Member States will be in different positions regarding the implementation of the relevant legal instruments, and the current evaluation process could also provide useful input to Member States that may not have implemented all aspects of the various instruments. Nonetheless, the evaluation aims to be broad and interdisciplinary and not to focus solely on the implementation of various instruments relating to fighting cybercrime, but also on operational questions in the Member States.

Therefore, apart from cooperation with prosecution services, this will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3 and how feedback from those organisations is channelled to the appropriate police and social services. The evaluation focuses on implementing national policies with regard to the suppression of cyber-attacks, fraud and child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to people who fall victim to cybercrime.

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

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

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

[6] CETS No 189, opened for signature on 28 January 2003, entered into force on 1 March 2006.

The evaluation teams consist of three national experts, supported by 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 Romania were Mr Philippe Devred (France) and Ms Lisanne van Dijk (the Netherlands). The following observers were also present: Mr Michele Socco (Commission), Ms Anna Danieli (Eurojust) and Mr Jaroslav Jakubcek (Europol/EC3), together with Mr Francisco Rodriguez Rosales and Mr Sławomir Buczma from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings drawn from the evaluation visit, which took place in Romania between 19 and 23 January 2015, and on the detailed Romanian replies to the evaluation questionnaire, together with their detailed answers to later follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National cyber-security strategy

The Cyber-Security Strategy and the National Action Plan on the implementation of the Cyber-Security National System (CSNS) were adopted in Romania through Government Decision No 271 (Official Journal No 296 of 23 May 2013). The CSNS is the general framework for cooperation, which brings together public institutions and authorities with responsibilities and capabilities in this field, to ensure national coordination of actions relating to cyber-space security, including cooperation with academia, business, professional associations and non-governmental organisations. The aim of the CSNS is to ensure that the threats, vulnerabilities and risks specific to cyber-space are known, prevented and counteracted, as they can affect the security of the national cyber-infrastructure, including consequence management.

The CSNS presents both short- and long-term objectives, stating that the country depends on the functioning of multiple networks that structure the lives and economy of its citizens. The Strategy also emphasises that ever-increasing levels of security for the digital infrastructure are necessary, due to the rising numbers and complexity of cyber-attacks. In response to that, Romania aims to reduce the risks and improve knowledge, capabilities and decision mechanisms. In this regard, efforts will focus *inter alia* on the following actions: establishing and making operational a national cyber-security system; completing and harmonising national legislation, including the establishment and enforcement of minimum security requirements for a national cyber-infrastructure; developing cooperation between the public and private sectors, including by fostering information exchange on threats, vulnerabilities, risks related to cyber-incidents and attacks; developing national capacity for risk management in cyber-security and for incident response under a national programme, including

the creation of an efficient mechanism to provide warnings and alerts of cyber-incidents; increasing the resilience of the cyber-infrastructure; developing of entities such as the Romanian National Computer Security Incident Response Team (CERT) in both the public and the private sectors; implementing awareness campaigns for the population and developing mandatory educational programmes on the safe use of the internet; providing adequate professional training to practitioners involved in cyber-security from the public and private sectors; and developing international cooperation on cyber-security, including participation in international programmes aimed at cyber-security.

3.2 National priorities with regard to cybercrime

Romania has defined national priorities with regard to cybercrime: prevention, institutional capacity, training, international cooperation, harmonisation of legislation, and consolidation of cooperation with the private sector.

Prevention

In the field of prevention, the law enforcement structures run various events targeting mainly the private sector, as well as citizens (young people) in order to raise awareness about the dangers and risks posed by this phenomenon. For example, the following actions were taken:

- activities within Safer Internet Day and Cyber-Security Month e.g. conferences, meetings, working groups attended by the public and private sectors;
- the Project SAFERNET, targeting child pornography, aiming to provide a safe and quick way to report child pornography activities carried out on the internet. The project was run by the Romanian police together with NGOs.

Institutional capacity

Since 2003, specialised units have been created within the General Prosecutor's Office and the Romanian police for the purpose of cybercrime investigations. The units established within the Romanian police have grown in terms of responsibilities, number of police officers, competences at territorial level, resources and training of personnel.

Training

The training for police officers at the central level is planned and provided annually and includes main areas of interest. The concept of 'joint training courses' for police officers, prosecutors and judges is used in various events organised. The National Institute of Magistracy offers training to judges and prosecutors in the field of cybercrime.

International cooperation

International cooperation is a priority both at operational level, with respect to pending investigations, and at strategic level, to achieve harmonisation between the national priorities and European and international standards. Operational cooperation takes place mainly via the police and the specialised Prosecution Service (DIOCT - Directorate for Investigating Organised Crime and Terrorism), taking into account the exchange of data and intelligence necessary in solving any cases. The relevant European and international instruments are used, as well as the relevant channels (Europol, Eurojust, Interpol, 24/7 contact points etc.). Romania has consistently participated in the European and international initiatives, projects and working groups established at the level of the European Union, the Council of Europe and other organisations; for example :

- Romania has participated as a partner and/or provided expertise in joint projects of the EU and the Council of Europe (CyberCrime@IPA, CyberCrime@EAP, Project on Cybercrime in Georgia and Global Action against Cybercrime (GLACY).
- In the period 2012-2013 Romania participated as a driver in the cybercrime priority of the EMPACT projects and in the period 2014-2017 Romania is participating in all three cybercrime priorities within the EMPACT Projects (cyber-attacks, credit cards, and IT systems-based). In these projects, Romania is the driver in the credit-card fraud project and a co-driver in the cyber-attacks project.
- At the Council of Europe, Romania participated in the work of the Cybercrime Convention Committee (T-CY)[7] on trans-border access to data and is currently a member of the Cloud Evidence Group established in December 2014.

[7]http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/transborder%20access/tcy_transborder_EN.asp?

Legislation

Over the past few years, the Romanian Ministry of Justice undertook a comprehensive legislative reform process, with a view to both amending the two codes on criminal matters, and reviewing the entire criminal legislation; it resulted in the adoption of two new codes and the laws for enforcing them[8]. In 2014 these laws entered into force. In the field of cybercrime, the new codes implement international standards, in particular the Council of Europe Convention on Cybercrime. At present, the Ministry of Justice is analysing the transposition of the Directive 2013/40/EU of the European Parliament and the Council on attacks against information systems, replacing the Framework Decision 2005/222/JHA (the Directive). In implementing the Council of Europe Convention on Cybercrime, Romania to a great extent achieves the transposition of the Directive.

The Decision of the Court of Justice of the European Union of 8 April 2014, which declared the Directive of the European Parliament and of the Council 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC[9] invalid[10], had effects on the essential provisions of the Law No 82/2012 transposing the Directive into Romanian law. As a result, the Constitutional Court of Romania admitted the application to challenge the constitutionality of Law No 82/2012 and determined that its provisions were unconstitutional (Decision No 440 of 8 July 2014). Following the discussions held within an inter-institutional working group, it is considered necessary to amend the Criminal Procedure Code and other laws, e.g. Law No 506/2004 on the processing of personal data and the protection of private life in the electronic communications sector.

8 Law 286/2009 on the Criminal Code, Law 135/2010 on the new Criminal Procedure Code Law 187/2012 enforcing the new Criminal Code, Law 255/2013 enforcing Law 135/2010.

9 OJ L 105 of 13.4.2006, p. 54.

10 Judgement in joint cases C-293/12 and C- 594/12.

3.3 Statistics on cybercrime

The Romanian authorities stressed that each public institution involved in combating cybercrime keeps statistics according to priorities that need highlighting and the relevant activities.

The police keeps cybercrime statistics within a specialised structure based on data provided by operational structures with responsibilities in the area of cybercrime. These statistics are collected monthly and are highlighted in analysis and evaluation reports. The police statistics emphasise registered cases (notifications and findings) but also solved cases. Not only types of offences but also categories of offences are identified, such as electronic payment fraud against computer systems and child pornography through computer systems. The following statistical indicators have been recorded over the past two years:

- 2012: number of criminal cases recorded 2970, number of indictments 209, crimes investigated 1615, number of accused persons 796, arrested persons 512;
- 2013: criminal cases recorded 2944, number of indictments 208, crimes investigated 1574, number of accused persons 627, arrested persons 273.

These statistics cannot be broken down by type of crime (for example: unauthorised access to computer systems etc.) because of the systems used for highlighting statistics.

In 2013, 3 032 cyber-related crimes were reported at the level of the Romanian police, representing 0.46% of a total of 659 832 reported crimes. Statistics gathered in during the first ten months of 2014 show 2 451 cyber-related crimes reported at the level of the Romanian National Police, out of a total of 548 449 reported crimes (0.44%).

Statistics from the Directorate for Investigating Organised Crimes and Terrorism (DIOCT) reflect the number of cases registered within the unit and not the number of crimes committed by every person investigated. Statistics do not distinguish between the cases that concern cybercrimes *stricto sensu* and cybercrimes in a broad sense; thus, they include offences related to the forgery of electronic payment instruments, skimming or the use of forged electronic payment instruments, including the online environment, as well as computer fraud. A concrete analysis of solved cases confirms an increasing trend in statistics for 2013 (standard data for all the Prosecutor's Offices), noting that the number of cases pending resolution from previous years is still rising (1 784 criminal files in 2013 as compared to 1 602 criminal files in 2012), given the increasing number of new criminal files (1 836 criminal files in 2013 as compared to 1 521 criminal files in 2012).

Statistically, there is an increase in solved cases (1 121 criminal files in 2013 as compared to 852 files in 2012) along with an increasing number of indictments (173 indictments in 2013, as compared to 168 indictments in 2012) and the number of people tried (351 accused in 2012 as compared to 373 accused in 2013).

At the level of the Ministry of Justice, statistics collected in the databases managed by the Ministry of Justice are considered globally. There are no separate records for the articles which criminalise various offences. Statistics available in the statistics module of ECRIS database are collected at the level of each court in Romania. These data are periodically replicated on the Ministry's servers, and in the collecting and replication process there are no other bodies/agencies involved[11].

[11] The Romanian authorities reported that although the current situation indeed does not include the possibility to separate records for different conducts and circumstances provided by a legal text, this problem will be solved in the near future as measures have been already taken to introduce all the circumstances and conducts described in a legal text provided by the Criminal Code. These measures will be soon tested and at a later stage implemented by each court.

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

The Romanian police has a separate budget for carrying out specific activities in the area of preventing and combating crime, without separate sections for specific areas of crime. According to the provisions of the Finance Division of GIRP, the budget allocated for police training in subordinated schools and for financing the Romanian police cannot be divided from the total annual budget of the institutions concerned. For the purposes of training of practitioners involved in countering cybercrime, the National Institute of Magistracy allocated approximately EUR 3 500 from its budget for training judges on cybercrime in 2014.

Romania declared that EU funding was involved in finalising several cybercrime projects. For example, the following initiatives were mentioned:

- the project setting up the CYBER-EX Centre of Excellence, which seeks to integrate knowledge and expertise between the private environment, academia and law-enforcement authorities;
- two projects on cybercrime were approved within the ISF (Internal Security Funds) funded projects and submitted to the European Commission. Their aim is to develop institutional capacity, ensure investigative tools and carry out training programmes.

In addition, the Department for Information and Internal Protection (DIPI) implemented the project on 'Implementing a cybercrime defence system at the level of the Ministry of Interior through DIPI, SMIS code 32566' with European funds, which resulted in the setting up of a unitary framework for real-time monitoring of security events, linked to a rapid intervention capability to minimise impact.

The project on 'The National System for Combating Cybercrime' was implemented by CERT – RO[12]. It was funded by the European Social Fund, through the 2007-2013 Operational Programme 'Developing Administrative Capacity'. The objective of the project was to create an adequate framework to increase the capacity to formulate public policies and to achieve better strategic regulation and planning, by strengthening partnerships both between institutions and between public institutions and representatives of fields with an interest in fighting cybercrime. As part of the project, a technical Romanian "CyberCrime' team was set up. At the same time, technical, law and public policy experts carried out analysis, documentation and support work, which led to the production of a set of public policy proposals, proposals for legislative documents and proposals for procedures to combat cybercrime. The project's initial value was RON 11 103 000 plus RON 1 665 450 co-financing from the beneficiary.

The budget of the second project developed by CERT-RO through the Framework 7 Programme, i.e. Advanced Cyber-Defence Centre (ACDC) is EUR 16 338 803, with 50% of the funding provided by the European Commission. Some 28 partners from 14 European countries participate in the project. The budget allocated by CERT-RO is EUR 470 200, of which the Romanian part co-finances EUR 235 100.

3.5 Conclusions

- The National Cyber-Security Strategy has existed in Romania since 2013, and includes a number of definitions (cyber-threat, cyber-incident, cybercrime, cyber-terrorism, etc.), objectives, courses of action, threat analysis, the Cyber-Security National System (CSNS) and cooperation between the public and private sectors.

[12] http://www.cert-ro.eu/proiecte/cybercrime/articol.php?idarticol=708

- Romania has also set up national priorities on cybercrime, namely prevention, institutional capacity, training, international cooperation, harmonisation of legislation, consolidation of cooperation with the private sector and international cooperation. The Romanian authorities consider cybercrime to be a serious threat for the state and the society.

- In the opinion of the evaluators, the strategy along with the defined priorities developed in Romania provides a solid basis for fighting cybercrime. Close cooperation between public organisations creates a unique opportunity to involve a wide range of entities working together. As a consequence, a wide range of actors are involved in combating cybercrime. On the other hand, the private sector is less involved in tackling this phenomenon.

- However, fulfilment of those priorities may encounter some difficulties in terms of providing consistent legislation. For example, data retention is not regulated currently in national legislation. The national legislation implementing Directive 2006/24/EC on data retention was in place until July 2014, when the Constitutional Court of Romania determined that the data retention provisions were unconstitutional, following the invalidation of the Directive by the Court of Justice of the EU three months earlier, stating that the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality.

- It remains one of the most important legal tools for law enforcement, since ultimately most cybercrime investigations involve translation of IP addresses to corresponding subscriber details. Consequently, not being able to do this paralyses many efforts to investigate serious and organised crime, besides cybercrime, and significantly hampers the level of assistance Romania can provide to other countries. The Romanian authorities therefore need to solve this problem adequately, although in the view of the evaluators it is not solely an internal problem in Romania but is to be solved first of all at the EU level.

- Each public institution with responsibilities in cyber-security keeps statistics relating to cybercrime, in particular the Ministry of Justice (number of persons convicted for offences against Law No 365/2002 on electronic commerce); DIOCT (cybercrime cases); and the National Police (cybercrime cases). CERT-RO also keeps detailed statistics on alerts collected and transmitted by automated systems.

- In the opinion of the evaluators, there seem not to be completely standardised statistics for the actors (the police, prosecutors, judges) involved in the investigations and prosecutions due to the practical reasons relating to cybercrime. The statistics on cybercrime are generated as a single figure[13]. Consequently, it is not possible to divide the different cases of cybercrime into categories. Therefore, it would be advisable to have figures broken down into different cybercrime areas, preferably cyber-attacks, online child abuse, and online card fraud, to gain a clear picture of cybercrime.

- The Romanian police has a separate budget for carrying out specific activities in the area of preventing and combating crime, but not separate sections for specific areas of crime. Romania has frequently made use of EU funding to finalise cybercrime projects.

[13] After the on-site visit the evaluation team received an explanation that the judicial statistics collected by the courts are replicated/uploaded periodically on the servers of the Ministry of Justice and managed by the Ministry, whereas statistical data covering the investigation stage, execution of the sentence, probation etc. are managed by other authorities. Considering that the ECRIS application includes only data for the trial stage there is no direct correlation between data collected during the investigation stage, which are managed by other institutions, and data on convicted persons. Therefore, the Ministry of Justice intends to obtain under POCA 2014-2020 funding for a project aimed at creating an Integrated Information System in the field of justice, which will facilitate the collection and management of statistical data both for courts and prosecutors' offices.

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

The Public Ministry consists of the Prosecutor's Office attached to the High Court of Cassation and Justice, 15 prosecutor's offices attached to appeal courts, 41 prosecutor's offices attached tribunals (capitals of counties) and 176 prosecutor's offices attached to first courts[14]. The Prosecutor's Office attached to the High Court of Cassation and Justice consists of four operational sections: National Anti-corruption Directorate, Directorate for Investigating Organised Crime and Terrorism, Forensic and Investigation Section and Military Prosecutor's Offices[15].

The Directorate for Investigating Organised Crime and Terrorism (DIOCT) was established by Law No 508/2004 as a single structure of the Prosecutor's Office attached to the High Court of Cassation and Justice, specialising in combating the most serious crimes, such as human trafficking, drug trafficking, terrorism offences, computer crime, macro-economic / financial offences. The Directorate is headed by a chief prosecutor, assimilated to the First Deputy of the General Prosecutor of the Prosecutor's Office, and includes the following divisions: Service for Preventing and Combating Organised Crime; Service for Preventing and Combating Illicit Drug Trafficking, Service for Preventing and Combating Economic and Financial Crime; Service for Preventing and Combating Terrorism Offences and Offences against State Security; Service for Preventing and Combating Cybercrime; Judicial Service and Office for Representation and International Cooperation. The DIOCT structure is composed of 15 territorial services and 26 territorial offices. The Directorate has a total of 280 prosecutors, 40 specialists and 200 administrative personnel (clerks of the court, contractual personnel). Under Article 9 of Law No 508/2004 the prosecutor may delegate certain activities to specially appointed judicial police officers. According to the Romanian authorities, it could be contra-productive in areas in which cybercrime has incidental occurrence. Nonetheless, one or more prosecutors mainly conduct specialised prosecution for cybercrimes.

14 See Law No.304/2004 on organisation of the judiciary.
15 See http://www.mpublic.ro/sectii.htm, http://www.pna.ro, http://www.diicot.ro

The structure specialising in combating cybercrime is the Service for Preventing and Combating Cybercrime, which is headed by a chief prosecutor, two subordinate chief prosecutors and four prosecutors, each of whom is entitled by law to personally carry out criminal prosecution functions in the relevant specialisation and the cases distributed. The offences in the remit of the Service include: illegal access to a computer system (Article 360 NCC); illegal interception of transmissions of computer data (Article 361 NCC); alteration of computer data integrity (Article 362 NCC); disruption of the functioning of information systems (Article 363 NCC); unauthorised transfer of information (Article 364 NCC); illegal operations with devices or programmes (art.365 NCC); attempted offences (Articles 360-365 NCC); cyber-forgery (Article 325 NCC); child pornography (Article 374 NCC); computer fraud (Article 249 NCC); performing financial operations fraudulently (art.250 NCC); accepting fraudulent transactions (Article 251 NCC); forgery of electronic payment instruments (Article 311(2) NCC); circulation of counterfeit securities (art.313 NCC); ownership of tools for use in counterfeiting securities (Article 314(2) NCC) (only if the act is committed by an organised criminal group (Article 367 NCC)); and any other offences.

The judiciary of Romania is organised as a hierarchical system of courts, with a civil law system. According to the Constitution and Law No 304/2004 on judicial organisation, the courts are organised as follows:

- High Court of Cassation and Justice (*Înalta Curte de Casaţie şi Justiţie*);
- 15 Courts of Appeal (*curţi de apel*);
- 41 county courts and the Bucharest Municipal Court (*tribunale*);
- 188 Local courts.

The organisation of the courts of Romania does not provide for specialised panels/judges dedicated to cybercrime.

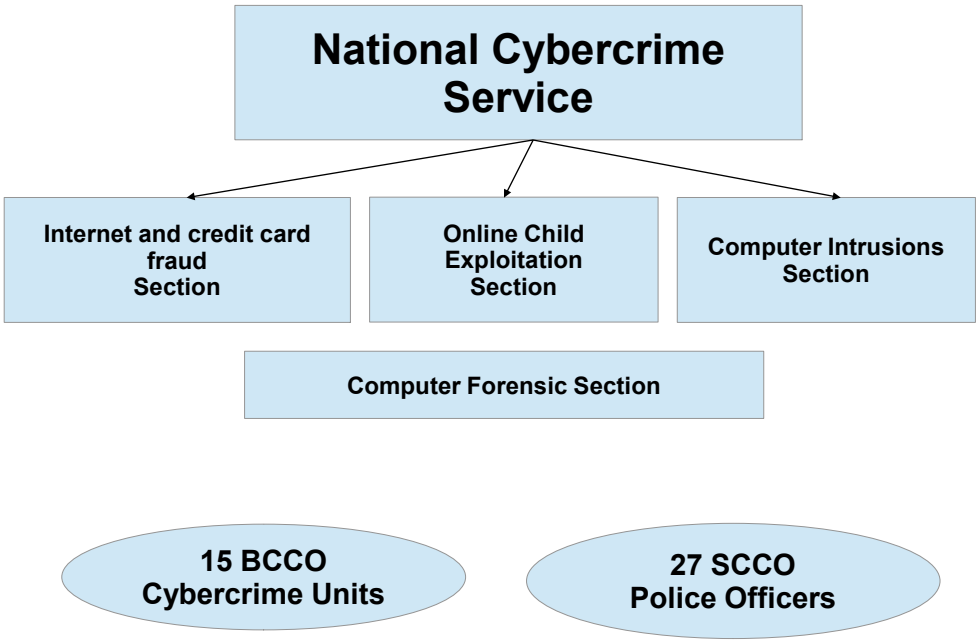
4.1.2 Capacity for and obstacles to successful prosecution

The Romanian authorities stated that the following were the main obstacles in investigating cybercrimes:

- technical challenges of new equipment from IT&C solutions, virtual payment systems that make it difficult to investigate financial products, anonymisation services, encryption solutions, technical issues concerning evidence;
- the cross-border nature of cybercrime and insufficient capacity for cooperation with foreign partners, as well as the long time it takes to obtain evidence from foreign jurisdictions;
- common solutions for accessing data storage spaces in the "cloud";
- the data retention problem, which is not regulated in the national legislation, while the available tools for obtaining the necessary data do not permit data and information to be obtained quickly.

4.2 Law enforcement authorities

The Service for Combating Cybercrime within the Romanian police's Directorate for Combating Organised Crime was established in 2003 by an internal order of the Minister of Interior. This Service has responsibility for preventing and investigating cybercrime, credit-card fraud and child pornography via the internet, as well as for searching computer systems, and is composed of a total of four offices, specialising in the investigation of online fraud and electronic payment means, investigation of cyber-attacks, investigation of child pornography over the internet and conducting computer searches. The organisation of this structure corresponds with the priorities established in the field of cybercrime at Europol, a specialised office being established for each field. This Service has a total of 34 police officers, and at local level approximately 150 police officers, who carry out their activity in the field of cybercrime investigation. The police officers employed in the central and territorial structures have legal and IT training, being mainly recruited from graduates of the Romanian Police Academy.



The main tasks of the Service for Combating Cybercrime are conducting, and coordinating with prosecutor's offices, investigations on cybercrime; promoting legal and institutional measures to improve the activities performed; investigation and gathering of information via the internet; providing training programmes and equipment for police at central and territorial levels; development of standardised procedures for conducting investigative activities; ensuring the proper functioning of inter-institutional collaboration; ensuring a partnership with the private sector and ensuring good international cooperation.

At the territorial level, there are also structures that specialise in preventing and combating cybercrime within the Romanian National Police.

The activity of obtaining and processing digital evidence is carried out by the Service for Combating Cybercrime, by the National Forensic Science Institute (NFSI), and by the specialised structures within the Romanian Intelligence Service (RIS). The differences relate to the status of the workers and the nature of the activities they can perform. The Service for Combating Cybercrime may collect digital evidence and carry out computer searches, whereas the NFSI and RIS provide digital evidence expertise. In order to strengthen cooperation on the operational level 24/7, contact points have been established. Within the police, there is a second 24/7 contact point to assist the contact point from the Prosecutor's Office. The designated personnel take incoming requests and process them. Moreover, the Directorate for Combating Organised Criminality contains an office specialising in the investigation and search of computer systems, with specialist computer-search positions, and the territorial structures have departments with specialist computer search officers. In total, there are 57 police officers specialising in computer searches. It also employs specialists in processing and exploiting information, in the economic, financial, banking, customs, IT and other fields, as well as auxiliary specialist personnel and economic and administrative personnel among the positions available.

4.3 Other authorities/institutions/ public-private partnership

CERT-RO

The CERT-RO is an independent structure, with expertise in the field of cyber-security that has the capacity to prevent, analyse, identify and respond to cyber-security incidents threatening the national cyber-space. CERT-RO is coordinated by the Ministry for the Information Society and is fully financed by the state budget. CERT-RO's main tasks are:

- organising and maintaining a national database regarding threats, vulnerabilities and cyber-security incidents identified by or reported to CERT-RO, techniques and technologies used for attacks as well as good practices regarding cyber-infrastructures protection;

- providing the required organisational and technical support for information exchange between different CERT teams, users, regulators, equipment and cyber-security solutions providers and internet service providers;
- providing a unique contact point for collecting information and complaints about cyber-security incidents in an automated and secured manner, or through direct communication, depending on the case;
- elaborating legislative proposals, submitted to the Ministry for the Information Society (MSINF) or to the Supreme Council for National Defence (CSAT), regarding changes to the legal framework to foster the improvement of cyber-security of the systems used to provide services of public interest;
- constituting the 'Early Warning and real-time information System' (EWS) regarding cyber-security incidents, which results in real-time alerts being sent on cyber-security incidents, reports being issued on their distribution and nature, and collaboration being facilitated with national authorities responsible for cyber-security, to prevent and eliminate their effects;
- supporting public services, such as: preventive services (announcements of new threats or vulnerabilities identified at national and/or international level; security audits, risk assessments and penetration testing on demand; reports regarding cyber-security incidents that could affect or involve Romanian entities), reactive services (alerts and warnings regarding suspicious activities possibly preceding an attack, handling of cyber-security incidents at national level), and consultancy services (CERT teams training, risk analysis regarding cyber-infrastructures applicable to local and national level).

CERT-RO collects data regarding cyber-security incidents and events affecting or involving entities in Romania, from national or international sources. Thus, once an incident is identified, based on the internal procedures, CERT-RO deploys a series of actions that ensure its response activity. Moreover, CERT-RO provides organisational and technical support for information exchange between various entities (national authorities, individuals or companies, CERT teams, security solution providers, internet service providers, etc.) involved in cyber-security incidents, and facilitates their smooth cooperation.

CERT–RO does not have the legal authority to solve all kinds of cyber-security incidents, e.g. those resulting from cybercrimes falling under the responsibility of law enforcement agencies. Moreover, cyber-security incidents that could constitute threats to national security are managed by institutions with competence in this specific domain. If CERT-RO receives such notification, it forwards them to the proper authority.

Centre for the Coordination of Critical Infrastructure Protection

The Centre for the Coordination of Critical Infrastructure Protection plays a role as a national contact point to other EU Member States, the European Commission, NATO and other international organisations for critical-infrastructure-related problems. One of its responsibilities is to ensure the implementation of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, as well as the management of the CIWIN platform at national level. However, it was not clear to the evaluation team whether there is a national legal instrument stipulating specific tasks for the operators of critical infrastructures and information systems that allowed information to be shared on incidents and developments in the event of a cyber-attack.

County centres for educational assistance and resources

The centres for educational assistance and resources, located in the counties and in Bucharest, play an important role in preventing and combating cybercrime and in online safety intervention. Given their objectives, they contribute to advising victims or potential victims. They have national coverage. A County Centre for Educational Assistance and Resources (CCEAR) was set up in each county and in Bucharest there is Bucharest Centre for Educational Assistance and Resources (BCEAR). These units are linked to the secondary school education system. They have legal personality and are subordinated to the Ministry of National Education. They constitute an institution specialising in providing integrated special education, coordination and monitoring of specific educational services provided to children / students, teachers, parents and community members, to ensure that everyone has access to good quality education and necessary assistance in this regard.

The main objectives of the CCEAR/ BCEAR are to enrol and keep of all children / young people in mandatory education; to inform and guide teachers for professional and educational optimisation; to work with the educational factors involved in the development of the students' personality / youth in order to better integrate them in school and in social and professional life; to involve parents in specific activities for an effective school-family-community relationship, as a basis for the adaptation to school and the social integration of the children/young people; and to develop studies on dropout, juvenile deviant behaviour, negative entourage, extracurricular activities / leisure.

Intelligence

The Romanian Intelligence Service is also involved in preventing and combating cybercrime, under Law No.14/1992 on the organisation and functioning of the Romanian Intelligence Service, some provisions of the Criminal Procedure Code and related legislation. The main objectives in that field are the transmission of data and intelligence indicating preparation of an act criminalised by the criminal law to the criminal prosecution bodies under conditions set out Article 61 of the Criminal Procedure Code. However, the Romanian Intelligence Service does not have responsibilities for criminal investigation and criminal prosecution. The Romanian Intelligence Service provides the technical coordination of the Operational Council on Cyber-Security (OCCS) in the area of cyber-security. The Romanian Intelligence Service cooperates closely with the police in obtaining and processing digital evidence.

NACPA

In terms of the responsibilities conferred by law on the National Authority for Child Protection and Adoption (NACPA), it does not have specific authority strictly relating to combating cybercrime. Its intervention in this area is carried out from the general perspective of ensuring the protection and promotion of the rights of all children. However, in all inter-institutional cooperation mechanisms devoted to this issue, the role of NACPA is to facilitate the collaboration and involvement of local structures in terms of providing specialised services for child victims of this phenomenon, in order to support and rehabilitate them. At the same time, NACPA can cooperate with other institutions in terms of reporting cases of children who become victims of this phenomenon, in order to initiate specific checks and investigations by the competent authorities. Given the duties incumbent on the general regulatory framework ensuring the protection and promotion of children's rights, NACPA can support the promotion of various legal acts relating to this area, initiated by other ministries or authorities with distinct responsibilities in this matter.

CYBER-EX

The Cybercrime Centre of Excellence (CYBER-EX) was set up as a viable partnership between law enforcement authorities, judicial authorities, higher or specialised education institutions and private companies. It was created to integrate knowledge and expertise and provide professional development in the fight against cybercrime, making use of EU funds (for more information see chapter 8.1).

The Romanian authorities also reported that there were public/private partnerships with various private institutions in order to prevent and combat cybercrime. For example, the partnership between the Romanian police and Microsoft RO was mentioned, whose aim is to develop preventive and awareness events in the field of cybercrime. The other type of partnership between the Romanian National Police and an NGO (namely Save the Children) relates to online child pornography in the internet. There is also a Western Union representation in Romania to exchange information.

4.4. Cooperation and coordination at national level

4.4.1 Legal or policy obligations

The Cyber-Security National System (CSNS) represents the general framework of cooperation between public institutions and authorities in charge in this field to provide national coordination of actions to ensure the security of cyber-space. Furthermore, the aim of the CSNS is to ensure that the threats, vulnerabilities and risks specific to cyber-space are known, prevented and counteracted, as they can affect the security of the national cyber-infrastructure, including management. According to Romania's Cyber-Security Strategy, cybercrime represents one of the threats to cyber-space, together with cyber-terrorism and cyber-war. To fulfil those tasks, the Operational Council on Cyber-Security (OCCS) was established at the top of the national structures.

The OCCS includes representatives of the: Ministry of Foreign Affairs, Ministry of National Defence, Ministry of Home Affairs, Romanian Intelligence Service, Foreign Intelligence Service, Special Telecommunications Service, Protection and Guard Service, and the Office of the National Register of Classified Information at the level of state secretaries. The president of the OCCS is the presidential counsellor on national security and its vice-president is the counsellor of the Prime Minister on issues of national security.

In the opinion of the evaluators the composition of the OCCS does not reflect all stakeholders involved in countering cybercrime, such as the Ministry of Education. Moreover, despite the significant role it should play taking into account the representatives assigned to it, the OCSC is not a legal entity and thus does not have powers to take decisions relating to cyber-security. It plays a purely advisory and coordinating role between competent institutions. However, it promotes proposals and recommendations to the Supreme Council of National Defence (SCND)[16] on, for instance, measures to harmonise responses to threats and cyber-attacks, requesting assistance from other states or international organisations and bodies, and replies to requests for assistance; plans or lines of action, depending on the conclusions reached and the evolution of cyberspace; programmes on cyber-security; cyber-security policies for public authorities and institutions). Nonetheless, the acts adopted by the SCND do not have a normative character but an administrative one.

The role of the Ministry of Education among the institutions with responsibilities in preventing and fighting cybercrime is based mainly on two components, namely prevention and intervention, using the subordinated units (school inspectorates, county centres/Bucharest centres of educational psychology, the advisers and school psychologists network, the teachers' houses, palaces and children's clubs), and cooperation with educational partners and stakeholders (NGOs, professional associations, other associations etc.). The challenge of preventing and fighting cybercrime is tackled at the following levels: intra-curricular, extracurricular, and extra-school.

[16] It consists of the President of Romania as chair, the Prime Minister as vice-chair and the Minister for Defence, the Minister for Internal Affairs, the Minister for Foreign Affairs, the Minister for Justice, the Minister for Economic Affairs, the Minister for Public Finance, the Director of the Romanian Intelligence Service, the Director of the Foreign Intelligence Service, the Chief of the General Staff and the Presidential Adviser on National Security.

From the point of view of criminal justice, inter-institutional cooperation is stipulated by the competences of each institution, being covered by the legal provisions, internal regulations and existing protocols between them. For each institution, the responsibilities are different, as follows:

- the police are responsible for: receiving complaints, collecting data and information, carrying out investigations, analysing technical evidence and using special means of investigation;
- the Prosecutor's Office is responsible for: receiving complaints, conducting criminal investigations and ordering police units to take special investigative measures, as well as cooperation with the courts for approving special investigative or restrictive measures;
- The Intelligence Service collects specific data and information and provides them to the police or prosecutors for investigation.
- Courts have powers to authorise the use of special investigative or restrictive measures and to adjudicate the case.

Under Law No 161/2003 on ensuring the security of computer systems and the protection of personal data, the public institutions and authorities tasked in this field, service providers, NGOs and other representatives of civil society develop joint activities and programmes to prevent cybercrime. They are required to promote policies, practices, measures, procedures and minimum security standards for computer systems and organise information campaigns regarding cybercrime and the risks that the computer systems users are exposed to.

4.4.2 Resources allocated to improving cooperation

The level of resources, institutional capacities and staff training offered for law enforcement is very satisfactory, in the view of the Romanian authorities, considering the cybercrime situation in Romania. However, there are continuous improvement requirements. For example, at the level of the Service for Combating Cybercrime and territorial police units there are hardware and software solutions (Encase software) to carry out computer forensic activities.

However, there are no special budget allocations at the level of law enforcement structures regarding cooperation with the private sector, but in jointly undertaken projects and events there are activities also funded by public authorities.

It should be pointed out that during the visit to CERT-RO, the evaluation team was informed that the staff payroll only covers around 60% of the staff budgeted for. The centre seems to be punching above its weight now and would benefit significantly from an allocation of additional resources, which could be used to set-up a 24/7 call centre and real-time monitoring projects.

4.5 Conclusions

- In Romania a number of stakeholders are involved in cyber-security, and in cybercrime in particular. All have clear and distinct roles, encompassing the entire cybercrime spectrum. The general framework for cooperation is the Cyber-Security National System (CSNS), which is also responsible for addressing cooperation with academia and the business environment, professional associations and non-governmental organisations. The Operational Council of Cyber-Security (OCCS) aims to allow for unitary coordination of the CSNS at the central level.

- The evaluation team was told on a number of occasions and by different authorities that coordination among the different authorities involved is not a problem and takes place in accordance with existing laws, internal regulations and protocols. There is a multitude of actors, which seems accurately to reflect Romania's multidisciplinary approach to cybercrime (from prevention, to awareness and enforcement). They seem to work well together, but nevertheless it was difficult to understand who is coordinating all these efforts in practise. Moreover, not all actors involved in fighting cybercrime are represented directly within the OCCS but through the ministerial level.

- A new draft law was presented to the Parliament with regard to cyber-security, but it did not pass the Constitutional Court's scrutiny (*see* Decision No 17/2015). After the on-site visit, the evaluation team was informed that the law was declared unconstitutional in its entirety by the said Court Decision, which fact has a final effect on the legislative act, resulting in the termination of the legislative process.

- There is a close relationship between prosecutors and the police, which is laid down in law but also works operationally at both national and regional levels. The prosecutors of the DIOCT carry out criminal prosecution in cases related to cybercrime that covers all the crimes provided for in the Budapest Convention and Directive 2013/40/EU such as computer depended crimes (*stricto sensu* e.g. illegal access, computer hindering, misuse of devices, etc.) and computer enabled crimes (computer forgery, computer fraud, child pornography, grooming, credit card fraud, etc.). The Romanian police's Service for Combating Cybercrime conducts specialised investigations in the field of cybercrime. Both services have competences and personnel deployed at the national and local level.

- There are no judges appointed to deal with cybercrime. Therefore, in the opinion of the evaluators, raising awareness amongst judges of this type of crime requires regular training.

- The Romanian Intelligence Service (RIS) is significantly involved in the fight against cybercrime and, although it does not have criminal investigation and criminal prosecution responsibilities, it provides support, from a technical point of view (interceptions, expertise) and with intelligence upon request or *ex officio*, to the criminal investigation and prosecution led by the prosecutor. The evaluators believe that this close and efficient cooperation in countering cybercrime could serve as an example of best practices.

- The work and activity of CERT-RO is noteworthy and has both cyber-security and cybercrime aspects. One of the key tasks of CERT-RO is to identify and prevent cyber-security incidents threatening national cyberspace. One very promising project aims to bring about close cooperation with the largest ISP in Romania, which should lead to notification of malware-infected clients, particularly the compromised systems in Romania that are part of botnets and are used as proxies to carry out attacks on targets outside the country. Its involvement in cybercrime at both national and international levels should be highlighted, particularly CERT-RO's development of both a comprehensive training programme on preventing and combating cybercrime and a set of policy proposals for fighting cybercrime.

- Bearing in mind the important role it plays and its budgetary and human resources, the evaluators believe an assessment should be made regarding increasing the number of staff appointed, so as to reach the planned staff complement and thereby make it more effective. This is a very commendable effort, capable of very effective active prevention of the cybercrime attacks. Therefore, in the opinion of the evaluators, the efforts made by CERT-RO to combat cyber-attacks should be regarded as examples of best practice.

- The Centre for the Coordination of Critical Infrastructure Protection is the national competent authority in the field of critical infrastructure protection. The Centre is responsible for the implementation of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures, but it remains unclear whether there is a comprehensive list of national critical infrastructures, due to the fact that at least some of the articles of the draft law on cyber-security, which was supposed to regulate the concept of CINI, have been declared unconstitutional, so it will not come into force in the short term. It is therefore not clear whether there is a national legal instrument stipulating specific tasks for the operators of critical infrastructures and information systems in the event of a cyber-attack.

- The evaluation team recognised during the on-site visit that cooperation with private companies is growing. ISPs are working with CERT-RO on a voluntary basis and there are some understandings with companies. The Romanian authorities reported that taking into account the composition of the OCCS, the interaction between the private sector and the OCCS occurs via the institutions that are represented within it, namely via the Ministry for Information Society and CERT-RO. However, the question remains how the private sector interacts in practise with it in such a way as to allow the CSNS to fulfil its responsibility for cooperation.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on Cybercrime

On 15 May 2004 Romania was among the first states to ratify the Council of Europe Convention on Cybercrime. Law 161/2003[17] (Title III - Preventing and combating cybercrime) implemented closely the provisions of the Convention, and has been used by the Council of Europe as a model law in many technical assistance activities[18]. The substantive and procedural provisions of this law were later incorporated into the new criminal codes.

Since 2006, Romania has cooperated with the Council of Europe in the field of cybercrime, actively supporting the promotion of the Convention. The legislative and practical experience of Romania has been used in many activities organised by the Council of Europe. Most of the Council of Europe's projects in this field used expertise and personnel from Romania (Romanian Police, DIOCT, Ministry of Justice, CERT) and during 2009-2013 seconded an expert from the Ministry of Justice to the Council of Europe who worked as the Head of Cybercrime Unit.

Following the offer made by the Government of Romania in October 2013, the Committee of Ministers decided to set up the Council of Europe Office in Bucharest in the field of cybercrime (C-PROC). Thus, on 15 October 2013, a Memorandum of Understanding was signed in Bucharest, which was ratified by the Romanian Parliament in March 2014 (Official Journal of 2 April 2014)[19].

[17] Law No 161/2003 on measures to ensure transparency in performing high official functions, public functions and the business environment, preventing and sanctioning corruption, published in the Official Journal of Romania, Part I, No 279 of 21 April 2003, with subsequent modifications and amendments.

[18] www.coe.int/cybercrime

[19] Memorandum of Understanding between the Government of Romania and the Council of Europe on the Council of Europe Office in the field of cybercrime in Bucharest signed in Bucharest on 15 October 2013 and ratified by Law No 33/2014.

On 7 April 2014, C- PROC became operational. C-PROC in Bucharest, Romania, is responsible for assisting countries worldwide in strengthening the capacities of their criminal justice systems to respond to the challenges posed by cybercrime and electronic evidence on the basis of the standards of the Budapest Convention on Cybercrime. This includes support for strengthening of legislation, including human rights and rule of law safeguards and data protection; training judges, prosecutors and law enforcement officers; establishment of specialised cybercrime and computer forensic units and improvement of inter-agency cooperation; promoting public / private cooperation; protecting children against sexual violence online; and enhancing the effectiveness of international cooperation. C-PROC, with its capacity-building function, complements the work of the Cybercrime Convention Committee (T-CY) through which State Parties follow the implementation of the Budapest Convention. Romania has been actively participating in the activities of the Committee of the Convention on Cybercrime (T-CY) and since June 2014 has held the position of vice-chair.

5.1.2 Description of national legislation

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

There is extensive legislation in place in Romanian law regarding cybercrime[20]. Council Framework Decision 2005/222/JHA on attacks against information systems has been transposed into Romanian law. As a consequence, the following act are criminalised in the Romanian Criminal Code (CC): computer fraud (Article 249), fraudulent financial operations (Article 250), computer data forgery (Article 325), illegal access to a computer system (Article 360), illegal interception of computer data transmissions (Article 361), altering computer data integrity (Article 362), disruption of the operation of computer systems (Article 363), unauthorised transfer of computer data (Article 364), illegal operations with devices or software (Article 365), sexual intercourse with a minor (Article 220), recruitment of minors for sexual purposes (Article 222), child pornography (Article 374).

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

The law stipulates that attempts are also punishable as regards these offences, except for those specified in Articles 220, 222 and 325 of the CC. Incitement, aiding and abetting are also criminalised under the Romanian law. Legal entities, except for state and public authorities, may be criminally liable for offences perpetrated in the performance of the object of activity of legal entities or in their interest or behalf.

There is no definition of cybercrime in the Criminal Code but it is set out in the National Cyber-Security Strategy for policy reasons.

Romania was at the time of the on-site visit analysing the transposition of Directive 2013/40/EU. According to the Romanian authorities, by implementing the Convention on Cybercrime, Romania ensures to a great extent the transposition of the Directive, leaving only some aspects to be refined, such as the need to introduce special aggravating circumstances, to clarify some definitions and to provide statistics. The new Criminal Code and provisions of Title III, Chapter 2 of Law No 161/2003, on measures to ensure transparency in performing high official functions, public and business functions, preventing and sanctioning corruption, with subsequent modifications and amendments, implement the Convention on Cybercrime and thus also the Directive[21].

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

A number of normative acts transposed provisions of Directive 2011/93/EU, in particular the new Criminal Code. However, the transposition has not been completed yet. The Romanian authorities stated that a draft law transposing the remaining provisions is in the process of endorsement and after public debate it will be submitted to the Government.

[21] Following the on-site visit the evaluation team was informed that the Romanian legislation is already in line with Directive 2013/40/EU and no additional legislative amendments are needed. Romania notified the European Commission in July 2015 regarding the total transposition of the Directive.

C/ Online card fraud

The Romanian law counters any fraudulent financial operations made online. According to Article 250 of the CC the following actions are punishable:
a) making cash withdrawals, loading or unloading an electronic money instrument or a fund transfer instrument, by using, without the consent of the owner, an electronic payment instrument or the identification information that allow its use;
b) actions performed by means of the unauthorised use of any identification information or by using false identification data;
c) the unauthorised transmission to another person of any identification information, in order to perform one of the operations.

5.2 Procedural issues

5.2.1 Investigative techniques

The Criminal Procedure Code (Article 138 of the CPC) establishes the following special methods of surveillance or investigation measures:
a) **wire-tapping of communications or of any type of remote communication** (covers wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device);
b) **accessing a computer system** (penetration of a computer system or other data storage device, either directly or from a distance, through specialised programmes or through a network, for the purpose of identifying evidence);
c) **video, audio or photo surveillance** (taking of pictures of persons and observation or recording of their conversations, gestures or other activities);

d) **tracking or tracing with the use of technical devices** (use of devices that establish the location of the person or object to which such devices are attached);

e) **obtaining data regarding financial transactions of individuals** (operations that provide knowledge of the contents of financial transactions and other operations performed or to be performed through a credit institution or other financial entity, as well as the obtaining from a credit institution or other financial entity of documents or information held by it referring to the transactions or operations of a person);

f) **withholding, delivery or searching of postal deliveries** (inspection, through physical or technical methods, of letters or other postal deliveries or objects transmitted by any other means);

g) **use of undercover investigators and informants** (use of a person with an identity other than their real one, for the purpose of obtaining data and information regarding the commission of an offence);

h) **authorised participation in specific activities** (means the commission of acts similar to the objective component of a corruption offence, the performance of transactions, operations or any other kind of arrangements related to an asset or to a person who is presumed missing, a victim of trafficking in human beings or of kidnapping, the performance of operations involving drugs, as well as the providing of services, based on an authorisation from the judicial bodies of competent jurisdiction for the purpose of obtaining evidence);

i) **controlled delivery** (a surveillance and investigation technique allowing for the entry, transit or exit from the territory of the country of goods in respect of which there is a suspicion that their possession or obtaining is illicit, under the surveillance of or based on an authorisation from the competent authorities, for the purpose of investigating an offence or of identifying the persons involved in its commission);

j) **obtaining data generated or processed by providers of public electronic communication networks** or by providers of electronic communication services intended for the public, other than the content of communications, stored by these under the special law on storing data generated or processed by providers of public electronic communication networks and by providers of electronic communication services intended for the public[22].

There are procedural distinctions between the special methods of surveillance and the special investigation measures, as well as substantive conditions related to the type of an investigated offence. Electronic surveillance may be ordered only in case of offences considered serious listed under Article 139(2). The other measures, while respecting the provisions referring to the need to use them, may be ordered irrespective of the nature of the offence committed.

Electronic surveillance is ordered by the Judge for Rights and Liberties when there is a reasonable suspicion in relation to the preparation or commission of one of the offences listed below, it is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offence and it cannot be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat to the safety of persons or of valuable goods. Electronic surveillance may be ordered in case of offences against national security stipulated by the Criminal Code and by special laws, as well as in case of other specifically listed offences, including offences committed by means of computer systems or electronic communication devices.

[22] See Decision No.440 of 8 July 2014 of the Constitutional Court on the application to challenge the constitutionality of the provisions of Law No 82/2012 on the retention of data generated or processed by the providers of public networks of electronic communications or by the providers of electronic communications services for the public, and on the modification and amendment of Law No 506/2004 on the processing of personal data and the protection of private life in the electronic communications sector and the provisions of Art.152 of the Criminal Procedure Code.

Electronic surveillance may be ordered during the criminal investigation, for a term of a maximum of 30 days, if requested by the prosecutor, by a competent Judge for Rights and Liberties. If the judge decides that the application is justified, an electronic surveillance warrant is issued (Article 140 of the CPC). However, the prosecutor may authorise electronic surveillance measures for a maximum period of 48 hours, with the obligation to notify the Judge for Rights and Liberties within a maximum of 24 hours following expiry of a measure and to forward a report presenting a summary of the electronic surveillance activities performed and the case file.

Pursuant to Article 147 of the CPC, the withholding, surrender and search of postal deliveries may be ordered by a Judge for Rights and Liberties of the court of first instance or a court having a corresponding territorial jurisdiction in respect of letters, postal dispatches or items sent or received by a perpetrator, suspect or defendant or by any person suspected of receiving or sending, by any means, such goods from/to a perpetrator, suspect or defendant, or goods intended for it, if:
a) there is a reasonable suspicion related to the preparation or commission of an offence;
b) such a step is necessary and proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or of the evidence to be obtained or the seriousness of the offence;
c) evidence could not be obtained in other way, or obtaining it would imply extreme difficulties that would have a negative effect on the investigation or there is a threat against the safety of persons or of high-value goods.

Preservation of computer data (Art. 154)
If there is a reasonable suspicion regarding the preparation or commission of an offence, for the purposes of collecting evidence or identifying a perpetrator, suspect or defendant, the prosecutor supervising or conducting the criminal investigation may order the immediate preservation of computer data, including data referring to information traffic, that were stored by means of a computer system and are in the possession or under the control of a provider of public electronic communication networks or a provider of electronic communication services intended for the public, in the event that there is a danger that such data may be lost or altered.

The preservation is ordered by the prosecutor, *ex officio* or upon request by criminal investigation bodies, for a maximum of 60 days, by an order that must mention the obligation of the person or the providers of public electronic communication networks or the providers of electronic communication services intended for the public to immediately preserve the specified computer data and maintain its integrity, under conditions of confidentiality. The preservation measure may be extended for a maximum of 30 days.

If data referring to information traffic is held by several providers of public electronic communication networks or providers of electronic communication services intended for the public, a provider holding or controlling the computer data is obliged to provide the criminal investigation bodies forthwith with the information necessary for the identification of other providers, in order to enable them to learn of all elements of the communication chain used. The prosecutor supervising or conducting the criminal investigation may, with prior authorisation from the Judge for Rights and Liberties, request a provider of public electronic communication networks or a provider of electronic communication services intended for the public to transmit the data preserved under the law or may order cancellation of such a measure. The Judge for Rights and Liberties must rule on requests transmitted by criminal investigation bodies regarding the transmission of data within 48 hours. Before completion of the criminal investigation, the prosecutor is obliged to inform, in writing, the persons in relation to whom the criminal investigation is being conducted and whose data were preserved.

Collecting evidence

A computer system search or a computer data storage medium search designates the procedure for the investigation, discovery, identification and collection of evidence stored in a computer system or in a computer data storage medium, performed by means of adequate technical devices and procedures, of such a nature as to ensure the integrity of the information contained by these (Article 168 of the CPC). During the criminal investigation, the Judge for Rights and Liberties of the court of first instance or the court corresponding to its level may order a computer search, at the request of the prosecutor, if the investigation of a computer system or a computer data storage medium is necessary for the discovery and collection of evidence. The application is ruled on in chambers, without summoning the parties.

If there is reasonable suspicion in relation to the preparation or commission of an offence and there are reasons to believe that an object or document can serve as evidence in a case, the criminal investigation bodies or the court may order the natural person or legal entity holding them to provide and surrender them, subject to receiving proof of surrender (Art. 170 of the CPC).

5.2.2 Forensic and Encryption

The Romanian Criminal Procedure Code does not specifically provide for the remote forensic expert report. The general framework for ordering an expert report or a finding of fact is provided in Article 172 of the CPC. An expert report is ordered when the opinion of an expert is also required for the ascertainment, clarification or assessment of facts or circumstances that have importance for finding the truth in a case. Also, where there is a danger of evidence disappearing or of a factual situation changing, or when urgent clarification of facts or circumstances of the case is necessary, criminal investigation bodies may, through a prosecutorial order, issue an order to establish a finding of fact. Such fact finding is conducted by a specialist working with the judicial bodies or by an external one.

Encryption ensures the security and safe transmission of computer data, but there are issues that are generated for law enforcement structures in conducting investigations, for the identification of communications or computer data protected by encryption, which are used by suspects. In the case of investigative activities conducted by specialised police structures, identifying encrypted computer data or communications is done in cooperation with their owner, to the extent that he/she wants that or has good faith. There are no legal provisions for encryption to criminalise lack of cooperation by the owner or any aggravating circumstances that can be applied in such situations.

In order to solve cases involving encryption of data or communications, available tools and applications are used by the police. There is also collaboration with specialised structures in the field within the Romanian Intelligence Service. At the level of the police these activities are investigated by the structure specialising in cybercrime. Cooperation is also possible with the private sector in solving specific cases relating to encryption by the provision of technical support (applications) to public authorities. Institutional cooperation is effected on the basis of the current legal framework and under the cooperation agreements and protocols. The Advanced Technology Institute (Romanian Intelligence Service) has structures that establish technical and scientific findings in the field of computing and communication facilities. According to the cooperation protocols with competent institutions and on the basis of the authorisation documents issued by the judicial bodies, the Institute for Advanced Technologies, through specially designated personnel, can carry out forensic activities.

The Romanian authorities became aware of some problems with encryption within the expert / scientific findings, objects (files, data volumes etc.) ciphered with high complexity, digital algorithms have been identified, for which there are no effective attacks without information on the password or key. The issue was tackled by using commercially available tools and developing new tools.

No cooperation with private companies for decryption has been registered so far.

5.2.3 E - e v i d e n c e

The Criminal Procedure Code provides a definition of evidence and methods of proof, specifying that evidence is obtained in criminal proceedings through means and objects of evidence and is presented through the methods of proof provided by law.
Practice admits that 'electronic evidence' (digital evidence) represents any factual element created or existing in an electronic (digital) medium serving to ascertain the existence or non-existence of an offence, to identify the person who committed such an offence and to determine the circumstances necessary for a just settlement of a case. According to Article 100 of the CPC, during criminal proceedings, bodies with responsibility for crime gather and produce evidence, including electronic evidence, both in favour of and against a suspect or a defendant, *ex officio* or upon request.

Article 197(1) and (2) of the CPC stipulates that objects containing or bearing traces of an offence committed are physical evidence (for example an HDD, CD, DVD, router, memory stick or any other piece of equipment) and the objects used for the commission of an offence are *corpus delicti* (for example the computer system used). Taking into account the particular nature of an item of evidence that is produced, transmitted or kept in a computer system, the CPC has established special rules on how electronic surveillance is performed, how a computer search is carried out, and how computer data are surrendered or preserved.

Electronic surveillance (Article 142-143)
Any authorised person conducting electronic surveillance activities can ensure the electronic signing of data resulting from electronic surveillance activities, by using an extended electronic signature based on an approved certificate issued by an accredited certification services provider. Prosecutors or criminal investigation bodies are obliged to prepare a report for each electronic surveillance activity, in which they must record the results of activities conducted in respect of an act subject to investigation or contributing to the identification or localisation of persons, the identification data of the medium containing the results of electronic surveillance activities, the names of persons to whom these refer, if known, or other identification data, as well as the dates and times when the electronic surveillance activity started and ended.

Any authorised person making copies of a computer data storage medium containing the results of electronic surveillance activities can check the integrity of the data included in the original medium and, after making a copy, sign the data included in it, by means of an extended electronic signature based on an approved certificate issued by an accredited certification services provider, which permits the unequivocal identification of the authorised person, the latter thereby assuming responsibility for the integrity of the data.

Computer search (Article 168)

A computer system search or a computer data storage medium search designates the procedure for the investigation, discovery, identification and collection of evidence stored in a computer system or in a computer data storage medium, performed by means of adequate technical devices and procedures, of such a nature as to ensure the integrity of the information contained by these. While conducting the search, the prosecutor must order the making of copies of the computer data stored on the seized objects in order to ensure their integrity. If the seizure of objects containing computer data seriously hinders the performance of activities by the persons holding such objects, the prosecutor may order the making of copies of them, which would serve as methods of proof.

Surrender of objects, documents or computer data (Art. 170)

In the event that there is a reasonable suspicion in relation to the preparation or commission of an offence and there are reasons to believe that an object or document could serve as evidence in a case, the criminal investigation bodies or the court may order the natural person or legal entity holding them to provide and surrender them, subject to receiving proof of surrender.

There are no special rules with regard to the admissibility of e-evidence specifically if it is obtained outside Romania. The ordinary rules apply whether or not evidence is collected on the national basis or via mutual legal assistance.

5.3 Protection of Human Rights/Fundamental Freedoms

Communication via the internet and other communication means are protected and guaranteed under Romanian law. At the same time, personal data are protected by Romanian legislation in force, and their illegal dissemination on the internet is penalised by a fine.

The Constitution of Romania guarantees a series of fundamental human rights and freedoms, among which are rights to privacy, family and private life (Article 26); inviolability of domicile (Article 27); secrecy of correspondence (Article 28); and freedom of expression (Article 30). Those constitutional principles are also reflected in the criminal legislation, including the Criminal Procedure Code and the Criminal Code, by the criminalisation of acts infringing the right to domicile and private life (Chapter IX).

Taking into account Romania's membership in the Council of Europe and in the European Union, the criminal reform in Romania sought to adjust the legislation in criminal matters to the exigencies and requirements of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as of other relevant international and community instruments. Therefore, Law no 677/2001 concerning the Processing of Personal Data and Free Circulation of Such Data (Official Journal No 790, 12 December 2001) provides the general framework for the protection of persons, with the objective of guaranteeing and protecting the fundamental liberties and freedoms of persons, in particular the right to private life, family and processing of personal data. Illegal activities connected to cybercrime are criminalised by the legislation in force.

The objectives of the new Criminal Procedure Code included the unitary protection of the human rights and freedoms guaranteed by the Constitution and by the international legal instruments, as well as the adequate regulation in the criminal legislation of the international obligations undertaken by Romania. In terms of respecting the right to private life and correspondence, the Criminal Procedure Code establishes procedural rules regarding special methods of surveillance and

investigation, which meet the criteria of accessibility, predictability and proportionality. Whenever such measures are authorised, the criminal law requires that reasonable suspicion should exist regarding the perpetration of a crime, the principle of subsidiarity should be respected—the exceptional character of interference into one's private life being noted—as well as the principle of the proportionality of the measure in regard to restricting the right to private life, related to the specificity of the case, the importance of the information or of the evidence that is to be obtained, or the seriousness of the crime.

With the same objective of guaranteeing the right stipulated by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Criminal Procedure Code establishes as a principle the obligation that, once the technical surveillance has ended, the prosecutor should inform in writing the subject of any warrant concerning the surveillance measure taken against them.

5.4 Jurisdiction

5.4.1 Principles applied to investigate cybercrime

The Criminal Code makes reference to the principles of the legal standing, reality and universality of criminal law. Romanian criminal law applies to offences committed on the territory of Romania, which is defined as the expanse of land, the territorial sea waters and inland waters, complete with the soil, sub-soil and airspace located inside the national borders. The offence is also considered as having been committed on the territory of Romania when on that territory or on a ship sailing under the Romanian flag or on an aircraft registered in Romania an action was perpetrated with the intention to perform, instigate or aid in the offence, or the results of the offence have been manifest, even if only in part.

Romanian criminal law also applies to offences committed outside Romanian territory by a Romanian citizen or a Romanian legal entity if the sentence stipulated by Romanian law is life imprisonment or a term of imprisonment longer than ten years. In other cases, Romanian criminal law applies to offences committed outside Romanian territory by a Romanian citizen or a Romanian legal entity if the act is also criminalised by the criminal law of the country where it was committed or if it was committed in a location that is not subject to any state's jurisdiction. A criminal investigation can begin on receiving authorisation from the Chief Prosecutor of the Prosecutor's Office attached to the Court of Appeals in whose jurisdiction the first Prosecutor's Office is located that received information about the violation, or, as the case may be, from the Prosecutor General of the Prosecutor's Office attached to the High Court of Review and Justice.

At the same time, Romanian criminal law applies to offences committed outside Romanian territory by a foreign citizen or a stateless person against the Romanian State, against a Romanian citizen or against a Romanian legal entity. A criminal investigation can begin on receiving authorisation from the Prosecutor General of the Prosecutor's Office attached to the High Court of Review and Justice, and only if the violation is not the object of judicial procedures that are already ongoing in the state on whose territory it was committed. Romanian criminal law also applies to other violations committed outside Romanian territory by a foreign citizen or a stateless person who is located voluntarily on Romanian territory, in the following cases:
a) an offence was committed that the Romanian State has undertaken to repress on the basis of an international treaty, irrespective of whether it is stipulated by the criminal law of the state on whose territory it was committed;
b) extradition or surrender of the violator has been requested and denied.

No person can be investigated or prosecuted for an offence when a final criminal judgment has already been returned concerning that same person for the same offence, even if the charges were different.

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

Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings had been transposed into Romanian law on the basis of the Law No 300/2013. However, the Romanian authorities reported no cases where this question arose.

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

The same rules apply to investigate crimes committed in the 'cloud' as to offences committed outside Romanian territory by a Romanian citizen, or by a foreign citizen or a stateless person against the Romanian State, against a Romanian citizen or against a Romanian legal entity (see point 5.4.1).

5.4.4 Perception of Romania with regard to legal framework for combating cybercrime

The national legal framework makes it possible to handle cases relating to offences committed abroad. However the main obstacle to the investigation of crimes committed outside the national territory is the production of evidence, as the traces specific to these offence are partly found on the territory of another state. Obtaining evidence through letters rogatory is expensive, especially as regards the time needed to carry out certain activities. Moreover, the obstacles can also include the obtaining of identification data of IP addresses, the content of communications (mailbox), and technical or physical surveillance of persons. Although the legislation of states has changed as a result of the adoption of international cooperation instruments, including the Budapest Convention, the structure of the institutions responsible for the execution of requests for international judicial assistance has undergone no real changes, either in the actual number of people affected by the activity or in terms of personnel training in new forms of crime, such as cybercrime. The Romanian authorities also stressed a need to identify common solutions for collecting electronic evidence, such as accessing or authorised searches of storage space in the 'cloud'.

5.5 Conclusions

- Romania signed and ratified the Convention on Cybercrime, the one of the first countries in Europe to do so. The Convention entered into force for Romania on 1 September 2004. The way Romania implemented the Convention is being used by the Council of Europe as a model law in many technical assistance activities. Active participation in T-CY and involvement in the promotion of the Convention resulted in the decision to establish C-PROC in Romania. The evaluation team takes the view that the establishment of C-PROC strengthens Romania's active support for the promotion of the Convention as a global instrument.

- Council Framework Decision 2005/222/JHA on attacks against information systems has been implemented into Romanian law. The implementation of the Convention on Cybercrime greatly facilitated the transposition of Directive 2013/40/EU on attacks against information systems. The Romanian authorities reported that the Romanian law is consistent with the Directive.

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

- Combating credit card fraud is addressed in the Romanian Criminal Code.

- There is no definition of cybercrime in the Criminal Code but it is defined in the National Cyber-Security Strategy. Therefore, the tendency is to use the definition in the National Cyber-Security Strategy, which refers to any act provided for by criminal law or by any other criminal provision, causing social harm, committed with intent, via cyber-infrastructure or upon it. Consequently, cybercrime stakeholders may not share a broad common understanding of the same concept.

- In February 2014 the new Criminal Code and the new Criminal Procedure Code entered into force. Changes that concern cybercrime are inter alia grooming and making fraudulent financial data. Cyber-related investigative methods and related activities are provided for in the Criminal Procedure Code. Five of the nine investigative methods are defined as electronic surveillance, which may be ordered only in the case of offences considered serious and which requires specific measures. Other cyber-related activities are also described, such as computer searching, preservation of computer data and notably the use of electronic signatures.

- Despite the close cooperation between the police and the Romanian Intelligence Service and their efforts in terms of expertise, training and development of technical tools, encryption has been identified as one of the main issues that hinders the success of investigations carried out by the police. In the opinion of the evaluators, the lack of cooperation with private companies in decryption of data and the lack of legal provisions to criminalise, at least in serious crimes, the reluctance of suspects to cooperate in opening encrypted files on their computers could be mentioned as reasons creating those hindrances. A way to go in increasing the effectiveness of investigations could be introduction of the concept of decryption order which should be elaborated at the European level based on the best practices from Member States.

- Romania acknowledges that law enforcement authorities face difficulties in producing evidence - including obtaining identification data of IP addresses and the content of communications (mailbox) - of crimes committed outside the national territory, not least given the cross-border implications of cybercrime. A similar problem is faced regarding accessing data storage spaces in the 'cloud' as well as use of the evidence gathered abroad.

- Romanian law imposes an obligation to investigate crimes committed with the Romanian territory. Moreover, the Romanian Criminal Code provides jurisdiction grounds for many specific offences committed outside of Romania. The Romanian Criminal Code establishes jurisdiction over almost all cybercrimes, when committed by Romanian nationals abroad.

- During the on-site visit the Romanian authorities indicated problems linked to the lack of provisions at European level on administering data retention. Since the Court of Justice of the European Union declared the Directive of the European Parliament and of the Council 2006/24/EC on data retention invalid, it has had effects on the essential provisions of the Law No 82/2012 transposing the Directive into the Romanian legislation. As a result, the Constitutional Court of Romania admitted the application to challenge the constitutionality of the Law No 82/2012 and determined that its provisions were unconstitutional. There is a working group established to find solutions for this situation. There is a new law in preparation on cyber-security. In the opinion of the evaluators, action should be taken at the level of the EU to bridge the gap resulting from the Court of Justice's decision, since similar problems could occur in other EU Member States as a result of the implementation of the invalidated Directive.

6 OPERATIONAL ASPECTS

6.1 Cyber -attacks

6.1.1 Nature of cyber- attacks

There are no statistics for cyber-attacks against the information systems of public authorities, but there are general statistics on cybercrime. The public institutions (such as courts, the Prosecution Service and the police) collect their own statistics on investigations and criminal cases (see more in chapter 3.3).

In 2013 CERT-RO received the following alerts:

1. Total number of automatic alerts received: 43 231 149;
2. Total number of unique IPs extracted from all alerts: 2 213 426.

Most alerts analysed by CERT-RO, from the automatic or individual segment of alerts, refer to entities in Romania, victims of attacks/attackers that have usually exploited technical vulnerabilities. The main goal of the attacks was to infect the computer systems with various malicious applications in order to make them part of different types of botnets (zombies). These compromised systems (victims) are often used to serve as 'proxies' for carrying out other attacks on targets outside Romania. There are significant advantages for the attacker using such an approach, for example the ability to hide his real identity and also to use a large number of computers (depending on the number of infected computer systems) to launch attacks. Also, based on the malware types specific to the Romanian national cyberspace and on the types of compromised systems, it appears that most attacks are directed towards obsolete, outdated systems, with no native security features (i.e. systems affected by Conficker) or that are not updated with the latest security patches/updates.

According to data given by the Romanian authorities, Romanian entities have become more frequent targets for APT threats, i.e. cyber-attacks with a high degree of complexity, launched by groups that have the capacity and motivation to persistently attack a target in order to obtain certain benefits (usually sensitive information).

6.1.2 Mechanism for responding to cyber-attacks

Romania applies the principle of legality with regard to investigation of crimes. According to Article 3 of the CPC, judicial functions must be exercised *ex officio*, unless the law requires otherwise. Therefore, for a wide range of offences, which includes cybercrime, criminal prosecution is carried out *ex officio*. However, under certain circumstances, the prosecutor may decide not to continue the criminal prosecution on the basis of Article 314(1)(b) of the CPC (offences punished with a fine or imprisonment of no more than seven years).

Reporting illegal activities is an obligation for those who have knowledge of such activities, including cyber-attacks. Pursuant to Art. 16 of Law No 365/2002 on electronic commerce, the service providers are obliged to notify the competent public authorities immediately about activities that seem illegal carried out by recipients of their services or about information supplied by such recipients that seem to be illegal (Article 16(1)). The service providers must also interrupt the transmission into a communication network or the storage of information supplied by a recipient of the service, especially by eliminating the information or by blocking access to it, access to a communication network or the supply of any other information society service, should the public authority so require (Article 16(3)). A service supplier that infringes the conditions established by Article 16(1) - (3) of Law No 365/2002 may be fined.

However, national law does not stipulate a specific task for operators of critical infrastructures and information systems. The lack of specific legal provisions on responsibilities regarding notification, response, combat and elimination of the effects of security incidents by the state authorities or private entities, which has the effect of hindering the real-time response to such incidents, is one of the main difficulties reported by the Romanian authorities in responding to cyber-security incidents. In this context, internet service providers sometimes respond to requests by the state authorities and sometimes they argue that material losses or increased costs will follow if they put in practice such requests.

Where there are clear indications of violations of law, they comply with the requests of the state, but sometimes the mere delay in responding to the requests generates unwanted effects. Nonetheless, the evaluation team was told that the bill on cyber-security regulates the concept 'Cyber-Infrastructures of National Interest' (CINI), as well as the tasks that fall with all the holders of these infrastructures on providing network security and diminishing the effects of cyber-attacks.

Reporting illegal activities (including cyber-attacks) can be done directly, by fax, phone, e-mail or other communication, to the prosecution or police units specialised in cybercrime. The police has developed a website for taking online complaints pertaining solely to cybercrime[23]. These complaints cover all kind of computer crimes. Among the main difficulties reported regarding incident response activity was the lack of explicit legal regulations regarding the responsibilities for notification, responding, prevention and mitigation of cyber-security incidents by the state institutions or companies in the private sector. Citizens have embraced the tool, and hundreds of incidents are being reported through the website, which, after verification, may form the basis of criminal investigations or be sources of information for intelligence. The police has also developed a set of eleven standard operating procedures that supports the implementation of legislation on cybercrime, thus providing a harmonised compendium of practices for use by all police units when engaging in cybercrime investigations.

Among the main obstacles reported by the Romanian authorities when responding to a cyber-attack are those related to the challenges posed by new ITC devices, lack of legislation on data retention, evidence stored abroad in various information systems, anonymous services, encryption solutions, the short time available for data analysis, and a lack of response from some holders/owners of the information systems. However, in the opinion of the evaluators, streaming the use of the CSNS to discuss incidents, trends and developments with representatives of the private sector could facilitate cooperation with the private sector.

[23] www.efrauda.ro

6.2 Actions against child pornography and sexual abuse online

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

According to the Romanian authorities, specific databases have been created by using the computer applications Netclean Analyze and C4ALL, these applications being currently used for image and video analysis resulting from investigations. These databases contain signatures of HASH MD 5 and PhotoDNA of the analysed files, organised into four categories, according to a category standard established by the methodology of investigating child pornography via information systems. The police also store image and video files that are evidence of child pornography resulting from specific investigations. The internet service providers are obliged to remove illegal material involving minors to avoid re-victimisation.

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

Under the Criminal Code Romania criminalises the following acts related to sex exploitation/abuse online, sexting, cyber-bullying:

- trafficking in underage persons (Article 211 of the CC);
- exploitation of persons (Article 182 of the CC);
- rape (218 of the CC);
- sexual assault (Article 219 of the CC);
- sexual intercourse with a minor (Article 220 of the CC);
- sexual corruption of minors (Article 221 of the CC);
- harassment (Article 208 of the CC);
- recruitment of minors for sexual purposes (Article 222 of the CC);
- child pornography (Article 374 of the CC).[24]

[24] Their content has been inserted in Annex D.

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

Romania ensures the transposition of Article 21 of Directive 2011/93/EU by criminalising in the Criminal Code persons who, with direct intent, make another commit an act covered by the criminal law (Article 47 – the Instigator) and/or deliberately facilitates or helps in any way with the perpetration of an act covered by the criminal law or who promises to conceal the products originating from it or to favour the perpetrator, even if, after the perpetration of the act, the promise is not fulfilled (Article 48 – the Accomplice).

The Romanian authorities reported that over the past years there have been cases of foreign citizens convicted in their countries for child pornography via the internet, who later came to Romania and developed activities for recruiting and sexually abusing minors. Identification and investigation of those persons were carried out on the basis of intelligence held or notifications received from foreign authorities. When data or intelligence exist/are received about persons travelling to Romania investigated for acts of sexual exploitation of minors, those persons are monitored in order to establish whether they travel with criminal purposes and to prevent possible criminal activity. The monitoring activities are carried out with *inter alia* the help of the territorial police structures, with the suspected persons' countries of destination, where applicable, being notified. Taking into account the high degree of difficulty involved in proving this manner of sexual exploitation of minors, the police specialised unit carries out specific activities in the online environment in order to identify and investigate the criminal activity of the persons committing such crimes.

The following actions have been taken to prevent online child pornography:

- the Ministry of Justice administers a website displaying details of the information hotline for victims of crime, as follows: 0800 800 886, Monday to Friday, 09.00 - 17.00.

- The Information and Counselling Centre Internet Helpline set up within the Safe Internet project offers a toll-free number (031 80 80 000) and normal rate numbers (0744 300 476, 0762 639 300, 0722 753 744).
- The complexity of the school environment issue made an educational partnership necessary, one case of good practice being the cooperation between the Ministry of National Education and the Child Helpline Association. The social service call centre focused on children has a toll-free number for assistance, the European Single Phone Number for child assistance, 116111.

The Ministry of National Education works with the Child Helpline Association on putting into practice the Ministry of Education's strategy to reduce the phenomenon of violence in high school units. This cooperation seeks to monitor, combat and reduce the crisis in schools, often embodied by manifestations of violence. Children and parents can report problems they face by sending an e-mail to: telefonulcopilului@gmail.com. Moreover, the European Single Phone Number for child assistance, 116111, is displayed in every school in a visible location - close to the students' entrance. The Child Helpline Association provides support to children in need of care and protection, to children affected by violations of their rights and to parents who need counselling, directing the issues raised by the institutions and bodies and providing them psychological and educational counselling. The free service call centre facilitates communication from the Ministry of National Education with beneficiaries of education (students, parents, civil society entities), promoting the educational initiatives and policies of the Ministry.

- *Sigur.Info*

The *Sigur.Info* national programme is multi-annual and is run by the Save the Children Organisation in Romania, in partnership with Positive Media Iaşi and FOCUS Centre - Romanian Centre for Missing and Sexually Exploited Children, with funding from the European Commission (Safer Internet). The following institutions and organisations were involved in developing this programme: the Ministry of National Education, the Ministry for the Information Society, the National Authority for Management and Regulation in Communications, the National Association of Internet Service Providers, the Romanian Police, the National Authority for the Protection of Child Rights and Adoption, Microsoft, UPC, Orange, Vodafone, Cosmote, Kaspersky Lab, ECDL etc.

The goal of this programme is to promote internet safety through multiple activities, organised on three levels:

1. Awareness - awareness-raising and education on the benefits of using new technologies and risk prevention measures available on the internet;
2. HelpLine - information and permanent counselling for children and adults;
3. Hotline - to report illegal content to the authorities.

Thus, tools have developed both online (games, commercials, videos) and offline (brochures specific to the target group: children, teenagers, teachers, parents). Also, tools / resources have been developed in other projects (e.g. the project Safe Youth on Internet, translated CEOP videos etc.). The National Programme *Sigur.Info* has proved to have an important role in raising the awareness of children, parents and teachers of the benefits / advantages of using the internet and new online technologies, and the dangers / risks associated with them, by conducting national campaigns to promote children's safety on the internet and mobile phones, and to be highly effective in activating effective partnerships among the institutions mentioned above. So far, since the beginning of its implementation, the programme has involved more than 650 volunteers in activities, informing more than 43 000 parents and teachers and 98 000 children about the benefits and risks involved in unsupervised use of the internet by minors.

- *The School Guide*

In February 2014 the first school guide to safe and efficient internet use was launched in Romania, to train teachers in its use under INSAFE, European Safer Internet Network (the European Commission Safer Internet Plus Programme). The School Guide provides both theoretical information and practical applications for promoting safe use of the internet by students. The purpose of this guide is to provide easy resources for teachers and adults who want to work with children and young people on the topic of safe and effective use of the internet. The theoretical aspects are reinforced by practical applications that do not require the use of advanced computers or technologies. It covers issues (illegal content, cyberbullying, personal data protection etc.), recommendations (sheets on the role of schools, advising teachers), classroom activities (theme introduction, a set of lessons, conclusions, additional materials for children / parents) and includes an assessment component (assessment of classroom activities, questionnaires).

- *Safernet.ro*

The other initiative worth mentioning is Safernet.ro that is an example of a website aimed at ensuring a safe way to quickly report child pornography activities carried out on the internet. It is administered by the police in partnership with an NGO.

Although there are so many initiatives and so many organisations involved, in the opinion of the police, the results proved usefulness of this cooperation.

6.2.4 Actors and measures countering websites containing or disseminating child pornography

According to Article 25(2) of Directive 2011/93/EU, the measure of blocking is optional. If websites have illegal content, they can be blocked or removed by the internet service providers that host that content, as required by law, on the basis of a request made by the competent body. According to the Romanian law, the police require internet service providers in Romania to remove illegal material with minors, after verifying them according to specific procedures. In cases where it is found that the images are hosted by service providers from other states, the judicial authorities in those countries are informed.

However, the Romanian authorities reported that no specific tools are currently used to filter access to sites that host illegal material involving minors. Nonetheless, once illegal content on a specific website is noted, access to the site is blocked. The competent authorities who may authorise blocking access and removing illegal material involving minors are the police and the prosecutor's office or, where appropriate, the court, whose competence in the matter is established by the legal provisions in force. The private sector is responsible for implementing the measures taken by the competent authorities or by blocking or removing the illegal content. In general, service providers are not reliable for the content in the case of the services they provide; the person who rented or who uses the service is responsible for the content.

However, if the service providers are aware of any illegal content, they order that it should be removed and report it to the competent authorities to investigate. In practice, this situation consists in verifying the source of the website - if it falls under the national jurisdiction - and the illegal nature of the content presented, after which the service provider is contacted with a request immediately to apply the measure ordered (blocking, removal etc.).

There are no separate procedures for emergencies, but there are contact points for major service providers which are used in such cases. The Romanian authorities pointed out that if the private sector reports such activities, the competent authorities immediately order the necessary measures and the investigation of the case, depending on the nature of the illegal content. If the server that hosts the illegal material is outside the country, the state concerned is informed via Europol, through the 24/7 contact point or through the liaison officers' network, depending on the nature of the content and the severity of the offence. An important aspect taken into account when using the instrument by means of which a state is informed is the stage of the investigation in Romania. The main tools used to request assistance measures are police requests for conservation and letters rogatory. For countries outside the EU the main tools used are 24/7 contact points and Interpol.

To report acts connected to child pornography over the internet, a police website has been created, and it is managed jointly with the Save the Children Organisation Romania, Positive Media Iaşi and FOCUS Centre - the Romanian Centre for Missing and Sexual Exploited Children.

The Romanian police have a specialised unit for preventing and investigating crimes of child pornography over the internet (within the Service for Combating Cybercrime), and at local level in each county structure, there is at least one officer specially appointed and trained to carry out activities in this area. This specialised unit has six officers in total, and has the following tasks: investigation of child pornography over the internet; collection and use of data and information on the internet regarding child pornography through information systems; carrying out studies, analyses and assessments on the evolution of the crime phenomenon in the field, and proposing

measures accordingly; coordination of child pornography investigation at national level; cooperation activities with the private sector and international cooperation; promoting preventive events in the field; activities for the identification of the victims from pornography materials with minors, and administration of specific databases. For child pornography not related to the online environment, there are specialised structures within the Criminal Investigation Directorate of the Romanian Police.

6.3 Online card fraud

In 2012 the Service for Combating Cybercrime of the Romanian National Police (RNP) started an investigation regarding Point-of-Sale Intrusions and selling of compromised credit card data on automated vending websites, with USD 25 000 000 losses to the Australian Banking industry. RNP performed surveillance, covert investigations and online undercover operations to identify the suspects. The case prosecutor from the DIOCT requested and obtained from the Bucharest Tribunal almost 100 telephone and internet data interception warrants. RNP carried out cell-phone tower localisations to identify the locations from which the suspects carried on their criminal activity, remote authorised server cloning and data interceptions. RNP and Australian Federal Police (AFP) officers had weekly conference calls that resulted in receiving complaints, forensic reports and subpoena information obtained by the AFP and used in the criminal investigation by the RNP. AFP officers travelled to Romania to transfer to the RNP the forensic clones of the compromised computers, provide intelligence information and give written testimonies.

RNP identified new compromised USA-, Canada-, Brazil- and France-based POS systems and credit card data. RNP, AFP, FBI and USSS agents participated in case coordinating meetings in Bucharest. AFP, FBI and USSS provided the Romanian authorities with subpoena information regarding victims identified and also login access logs from the email accounts and user forum accounts that the suspects used in their illicit activity. RNP subpoenaed Romanian ISPs and Telephone Providers in order to identify the suspects, it being of critical importance to speed up the intelligence flow between the foreign LEA and the RNP.

A Romanian individual was identified, suspected of managing a data centre which contained servers used by hackers all over the world to launch cybercrime attacks. He was well known by the hackers as providing bulletproof hosting. At the end of the investigation, 34 home searches were carried out simultaneously. One of the addresses was the location of the main suspect data centre used for bulletproof hosting (over 400 TB of data seized). The data centre was taken down. Almost USD 400 000 in cash were seized. Sixteen suspects were investigated, and seven arrested.

6.3.1 Online reporting

The Romanian authorities ensured that online card fraud activities are reported to the authorities, and private-sector entities, especially financial institutions, assist in conducting investigations by providing the necessary data to the authorities, in accordance with the law.

6.3.2 Role of the private sector

In the opinion of the Romanian authorities, cooperation between authorities and financial institutions is positive in all aspects of preventing and combating online card frauds. Contact points are established by financial institutions and the police, for rapid and efficient exchange of information. Joint training and awareness activities are also carried out by the financial institutions and representatives of public authorities.

Possible gaps in national legislation on the application of measures that would help to improve the cyber-security and therefore prevent cybercrime have been filled by the signing of cooperation agreements between state institutions and private entities. Thus, CERT-RO has so far signed over 20 such documents with representatives of the private sector, including banking, which share information to prevent or combat the effects of security incidents in the information systems.

6.4 Conclusions

- Romania collects statistics on cybercrime on a yearly basis. These include statistics on incidents collected by CERT-RO and others more related to ongoing criminal proceedings collected by courts, the Prosecution Service and the police. However, there is no institution in charge of collecting all statistics and providing them to the decisive bodies to build an overall picture of this phenomenon in Romania (such as the OCCS). The evaluators believe that could help to measure the development of cybercrime in Romania and undertake appropriate actions.

- Romania applies the principle of legality, which may result in strengthening the policy to combat cybercrime more efficiently. The other example of the response to cybercrime is the reporting obligation in place on illegal activities addressed to those who have knowledge of such activities, including cyber-attacks. However, there are no specific provisions addressed to the private sector. In the evaluators' view, a clear obligation specifying situations in which it would be compulsory for private companies to generate an automatic report could help counter cybercrime.

- Moreover, national law does not stipulate a specific role for operators of critical infrastructures and information systems. Nonetheless, the evaluation team was told that the bill on cyber-security regulates the concept of Cyber-Infrastructures of National Interest (CINI), as well as the tasks that fall to all the holders of these infrastructures on providing network security and diminishing the effects of cyber-attacks. In the evaluators' view, there seems to be room for improvement in cooperation with the private sector. Proactive structured cooperation with the banking sector should be extended to the other relevant sectors. The organisation of regular meetings or a structure for discussing incidents, trends and developments with representatives of the private sector (from banks, ISPs and IT companies) could also strengthen this cooperation.

- The police developed a set of standard operating procedures that supports the implementation of legislation on cybercrime, thus providing a harmonised compendium of practices to be carried out by all police units when engaging in cybercrime investigations. The procedures were prepared by the central Police Unit, after consulting the regional services, and cover different aspects of cybercrime investigations such as computer searches, interception or preservation of computer data storage, child pornography crimes committed via information systems, etc.

- Romania has a tool for online reporting of cybercrime incidents: www.efrauda.ro. Such incidents may be reported by citizens with regard to all types of cybercrime. They are used by the Romanian Police to trigger an investigation, or they may serve as intelligence.

- There are also websites specifically established to deal with child pornography. Safernet.ro is an example of a website seeking to provide a safe way to rapidly report child pornography activities carried out on the internet. The project Sigur.info is designed to raise awareness among children, parents and teachers about the benefits / advantages of using the internet and new online technologies, and the dangers / risks associated with them, by conducting national campaigns to promote children's safety on the internet and with mobile phones, and to be highly effective in activating effective partnerships among the national institutions.

- According to the Romanian authorities, there is synergy between the tools mentioned above, because they are administered by the Romanian Police. In the event of wrongly addressed incidents, the request will be redirected for investigation to the competent authority. Nonetheless, no incidents have been noted of wrongly addressed reports. The evaluators consider it a commendable approach to online reporting of cybercrime, and a similar model could be considered for development in the Member States.

- Child pornography via information systems occurs in Romania mainly through the distribution and exchange of images on the internet. Cases of recruitment of minors and production of pornographic material are rare. There has been an increase in the number of cases involving distribution of images, but production of such images is low compared to international trends.

- According to the Romanian authorities, internet service providers are obliged to remove illegal material involving minors, a procedure having been in place since the entry into force of the Law on Electronic Commerce in 2002. Nevertheless, the development and use by police investigators of specific tools to filter websites for child pornographic content would increase the possibility of using the provisions concerned to their full potential.

- Preventive measures, including monitoring activities, are taken by the Romanian authorities when they are made aware that people investigated for acts of sexual exploitation of minors are travelling to Romania for criminal purposes and to prevent possible criminal activity. The evaluation team was told that there is no provision for such measures in the reverse case, so there is no communication to the destination country when a Romanian citizen convicted of any serious child sexual abuse is known to be travelling abroad, unless the court decision refers to such a provision in its sentence. The evaluators consider the lack of an option to send a reverse message leaves some room for improvement.

- Romania invests in the relationship between public and private partners in many ways. Sharing information with private partners on incidents, technical measures and possible solutions is one method. The police and prosecutor's office organise numerous conferences where private partners get a platform to share their approach.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

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

Romania created the legal environment for cooperation with Eurojust by implementing Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (Ordinance No 123 of 5 November 2007) and Council Decision 2009/426/JHA on the strengthening of Eurojust (Law No 35 of 19 March 2012). The provisions of the enactment are organised under three headings, dedicated to institutional and operational measures necessary for the exchange of liaison magistrates (Title I), cooperation with Eurojust (Title II) and the operation of existing and future networks at national and EU level in the field of judicial cooperation (Title III). It provides for an obligation to exchange information under Article 13(5)-(7) of the consolidated Eurojust Decision. From the DIOCT, the information is transmitted via a secure connection in a structured manner, using templates developed by Eurojust.

In the Romanian National Police, there is extensive experience of cooperation between Europol and the Directorate for Combating Organised Criminality. It has targeted several areas, such as cyber-attacks, sexual exploitation of minors via the internet and card fraud. In addition, in the EMPACT, Romania has undertaken the role of driver for the field of card fraud and the role of co-driver for the field of cyber-attacks. Representatives of the Romanian police participate in the events organised by Europol/EC3, whether in the form of seminars/workshops or meetings of experts in various fields, as well as in coordination meetings. Europol representatives have participated in activities carried out in Romania, in certain operations, to ensure efficient exchange of data and to provide the necessary support. The representative of the Romanian police attends the Europol/EC3 board meetings and is driver for the credit-card fraud project EMPACT. In addition, Romania is co-leading one (out of 18) and two (out of 23) operational actions of the Operational Action Plans (OAPs) on online payment-card fraud and cyber-attacks respectively. Romania also participates in 29 (out of 66) of the operational actions of the three OAPs as well as in Europol's focal points dealing with these three cybercrime subpriorities (FPs Twins, Cyborg and Terminal).

CERT-RO collaborates with ENISA in programmes supporting national CERTs. Collaboration with ENISA takes the form of participation in working groups, workshops, and cyber-security conferences concerning cooperation between national CERTs and law enforcement agencies, such as the cyber-security exercises (CYBER-EX) in 2012 and 2014. CERT-RO coordinates the calendar with activities conducted nationwide within ECSM (security events in the cyber-security month). The CERT-RO representative attends ENISA board meetings. In addition, representatives of the Ministry of Internal Affairs took part in the cyber-exercise at the Pan-European Cyber-Europe 2014 (EC 2014) event organised by ENISA.

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

According to the Romanian authorities, the capacity of Eurojust to facilitate communication with foreign authorities and accelerate the execution of urgent requests is strengthened by the DIOCT. The possibility of funding from Eurojust is appreciated by practitioners. The support Eurojust can provide is considered very useful in terms of facilitating cooperation with third countries. The assessment of the cooperation between competent authorities in Romania and Eurojust is positive; the cooperation consists in setting up coordination meetings on concrete cases. It is worth mentioning that the national member for Romania at Eurojust is also the Eurojust contact point to Europol/EC3 in The Hague, and is also the Eurojust Contact Point to the Europol Focal Point Terminal on Payment Card Fraud. The practitioners met found it useful for Eurojust to collect best practices and case law from other jurisdictions and disseminate this information to all Member States.

Setting up Europol/EC3 brought added value in terms of preventing and combating cybercrime at European level but also in the Member States. The integrated approach to cybercrime in terms of cyber-attacks, online fraud and child pornography through information systems shows the importance of the three areas and the connections among them, in terms of technical and legal instruments for investigation.

The Romanian authorities noted an improvement in the way the new developments in technology and operating modes are identified and presented to the Member States to take measures and order specific preventive and investigative measures. Analysis reports carried out at the Europol/EC3 level have a high value and contain integrated data from databases. The resources available to the Member States primarily for operational coordination meetings are at high level. Another positive aspect is the greater involvement of Europol/EC3 in cooperation with the private sector but also with third countries. The Romanian authorities underlined that Europol/EC3 should continue the evaluation of new criminal trends and dissemination of its findings to the Member States, as well as the improvement of their capacities on cyber-attacks and computer forensic.

The ENISA programme of supporting operational cooperation of national CERTs with the national law enforcement agencies at national and European level is a good start. This should be continued and focused on the exchange of information. Currently the two sides, national CERTs and law enforcement agencies, do not know each other's tasks, responsibilities and limitations well enough, especially in carrying out prevention and fighting actions. Thus, the capabilities of the national CERT sites are not always used effectively to support the work of law enforcement agencies. According to the Romanian authorities, this could be changed by adjusting the national and European legislation, to introduce express binding obligations of cooperation in order to avoid duplication of efforts and expenditures. ENISA could also develop a standardised format for the statistics analysed by CERT to make the registered alerts comparable and harmonised throughout the EU.

7.1.3 Operational performance of JITs and cyber-patrols

The Romanian authorities reported many cases of cybercrime cooperation with Europol/EC3 in which Romanian citizens were the perpetrators of illegal activities or in which Romanian citizens, authorities or private institutions from Romania were victims of crime. The collaboration involved exchanging data and information, conducting operational meetings with other Member States or

third parties, and participating with Europol mobile office in activities carried out in Romania. For example, a JIT on cybercrime (cyber-attacks and obtaining databases of credit card details) was set up between the UK, Finland, Slovenia, Romania and the US. Investigations were also carried out in joint cases with other EU or non-EU Member States on cybercrime. The experience gained at that time was positive since joint investigations were effectively established, as well as coordination of investigative measures, rapid response in obtaining evidence, etc.

EU funding (Eurojust or Europol/EC3) has been supplied only for supporting the implementation of coordination meetings with EU Member States, and third countries.

Romania participates in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol. The Romanian police is a member of the EU Cybercrime Task Force (EUCTF) and has been participating in its activities since its foundation. The concept of cyber-patrol is one that has many advantages, but for it to function well, it requires certain resources. At the level of CERT-RO a project was developed resulting in several proposals including the implementation of the concept of cyber-patrol in the Romanian police. At present, the concept of cyber-patrol is used within the Romanian police for specific cases, but it is not institutionalised and not carried out at international level. These cooperation tools are useful for several reasons, including establishing and identifying joint cases and obtaining evidence faster. However, in the opinion of the Romanian authorities, they are not effective enough on encryption, anonymous services, the cloud and cooperation with third countries.

7.2 Cooperation between the Romanian authorities and Interpol

The Romanian authorities appreciate events organised by Interpol and the exchange of data and information provided by the National Bureau of Interpol. Following the Interpol invitation, officers of this unit participated in two workshops organised by Interpol within the 'Baseline' project on establishing a list of signatures of files containing pornographic material that presented prepubescent minors that are engaged in sexually explicit activities, this list subsequently to be made available to internet service providers to block the online presence of files with those signatures and inform the competent judicial authorities about entities that initiate the transmission of such activities in their online environment.

Since 2010, the Romanian police through the unit specialising in investigating cases of sexual exploitation of minors via the internet has been granted access to and started using the ICSE Interpol database, carrying out the following activities:

- introducing materials presenting victims identified in Romania;
- cooperating with other users to identify victims of materials introduced in the ICSE, both by introducing materials with unidentified victims and by analysing such materials existing in the ICSE.

In 2011 the same unit began to exploit the ICACOPS and CPS databases containing data and information on entities performing acts of child pornography via computer systems in specific online environments (P2P, Tor etc.).

7.3 Cooperation with third states

International instruments form the legal basis for cooperation with third countries, as well as Interpol channel, 24/7 contact points, the network of liaison officers or established direct contacts. The Romanian authorities pointed out that there are third countries that are suppliers of illegal activities and their lack of reaction in international cooperation makes certain investigations impossible. Europol/EC3 brought added value in cooperation with third countries through the resources available for operational coordination meetings and contacts with these third countries, which can be used to assist the Member States.

International judicial assistance requests made in cases of cybercrime (including bank card frauds) amount to almost 40% of the international judicial cooperation activity of the DIOCT. During 2013-2014, at the DIOCT level there were 262 requests from other countries for international judicial assistance on cybercrimes. In turn, the DIOCT transmitted 397 of such requests to the authorities from other states.

Regarding relations with third countries during that period the following requests were registered.

COUNTRY	*RECEIVED*	*TRANSMITTED*
ALBANIA	1	-
AUSTRALIA	-	6
BELARUS	1	-
BRAZIL	-	2
CANADA	-	5
CHINA	-	4
SOUTH KOREA	1	2
SWITZERLAND	6	7
RUSSIAN FEDERATION	2	2
HONG KONG	-	1
ISRAEL	-	1
JAPAN	1	1
LIECHTENSTEIN	2	-
MALAYSIA	-	2
MEXICO	-	3
NIGERIA	5	-
NORWAY	3	2
NEW ZEALAND	-	2
PALESTINE	-	2
PERU	-	2
ANDORRA PPRINCIPALITY	2	-
DOMINICAN REPUBLIC	-	1
REPUBLIC OF MOLDOVA	-	2
SERBIA	1	-
USA	32	19
TURKEY	2	1
UKRAINE	-	3

7.4 Cooperation with the private sector

The Romanian authorities stated that international cooperation regarding online card fraud for cases with cross-border connections is very important for the success of an investigation. Cooperation is also possible if private companies have their main headquarters in a third state, but it depends on their organisation and functioning. If they cooperate in conformity with their status and legal provisions, the exchange of data and information is faster. The offices of private companies may be the object of investigations and searches.

During the evaluation visit it was highlighted that cooperation with Western Union also works very well because of the presence of a contact point in Romania. In addition, Western Union-USA also cooperate well thanks to good relations between the Romanian police and the FBI in the USA. However, the cooperation with money-transferring companies could be improved. During the visit, it was stressed that representatives of the police and the Prosecution Service meet on an *ad hoc* basis with private-sector representatives to go through technical aspects of collecting information, steps to be undertaken to guarantee that this information is admissible in courts, etc.

7.5 Tools of international cooperation

In the field of criminal cooperation, Romania uses multilateral and bilateral instruments to which it is party (Council of Europe treaties, in particular the Convention on Cybercrime, UNTOC, EU-Japan MLA Agreement, Bilateral Treaty with USA, etc.). To ensure immediate and continuous international cooperation in combating cybercrime, a contact point was set up within the Service for Combating Cybercrime from the Prosecutor's Office of the Supreme Court of Justice. These tools are very important for collecting digital evidence and conducting investigative activities in other jurisdictions. Difficulties encountered concern the volatility of digital evidence and problems related to the 'cloud'.

7.5.1 Mutual Legal Assistance

MLA requests for cybercrime cases are executed based on the law on international judicial cooperation in criminal matters (Law No 302/2004) and the provisions of Law No 161/2003. In addition, bearing in mind the constitutional provisions that state that treaties once ratified become part of domestic law, various regional and international treaties can be used as a legal basis for cooperation with EU or third countries. In that case, Law No 302/2004 is applicable to international judicial cooperation in criminal matters only to supplement those instruments in cases not regulated therein. Domestic law this only establishes norms when those norms are not already regulated by the international treaty or to supplement them. Law No 161/2003, which implements the Convention on Cybercrime, provides for specific provisions relating to cybercrime requests.

Depending on the legal instruments applicable, different authorities can be competent for receiving or sending MLA requests in cybercrime investigations. At the EU level, direct contact between issuing and executing judicial authorities is encouraged regardless of the stage at which the request is issued (investigation, prosecution, trial or execution). Thus, prosecutors or judges can and do communicate directly.

In the case of third countries, usually based on the legal treaty applicable, two situations can be encountered in relation to central authorities competent to send/received the MLA request:

- two central authorities: the Prosecution Service, for MLA requests made during investigation and criminal prosecution stage, and the Ministry of Justice, for requests made during the trial and execution stage, or
- one central authority: the Ministry of Justice, if the request has been issued in the absence of a treaty and based on reciprocity or if the treaty applicable designates the Ministry of Justice as the single central authority.

In addition, for requests relating to criminal records, which are registered differently than MLA, the central authority is the Ministry of Internal Affairs.

With reference to channels of communication, at EU level there is a direct channel used between the issuing and executing judicial authorities. In some cases, transmission via central authorities is preferable, especially by those countries that, though parties to the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the Additional Protocol thereto, continue to make use of central authorities. Otherwise, in relation to third countries transmission takes place between central authorities or even via diplomatic missions.

Statistical data on MLA cases dealt with through the Ministry of Justice[25]

Year	Active	Passive
2013	15	11
2014	34	12

MLA requests can be also transmitted through the Prosecutor's Office attached to the High Court of Cassation and Justice and directly between judicial authorities with regard to EU countries. According to the statistics on international judicial assistance relating to cybercrime cases investigated by the DIOCT, Romania received 139 MLA requests and sent 220 requests in 2013 and respectively received 140 and sent 150 in 2014.

Various form of cooperation can be requested via MLA in respect of cybercrime offences, depending on the type of cybercrime that constitutes the illegal conduct. Most of the requests refer to computer-related fraud and forgery, credit-card offences and, most recently, infringements of copyrights by means of computer systems. Consequently, many of the requests refer to providing subscriber information, login data, content data (to a lesser extent), search and seizure of computer systems, production of documents, interviewing witnesses etc.

[25] This relates to requests passed through the Romanian Ministry of Justice as central authority only, as required by international legal instruments.

According to the Romanian authorities, the difficulties resulting from the execution of requests emerge in general from differences in legal systems and from length of time before the request is executed. In many cases the legal instrument applicable or the lack of treaty applicable requires transmission through diplomatic channels, which takes more time and leads to obvious delays.

7.5.2 Mutual recognition instruments

No specific statistics are provided with regard to the application of various mutual recognition instruments. Besides, only a few of them would be applicable to cybercrime cases. For example, statistical data (for June 2014) referring to the application of Framework Decision 2008/909/JHA show that six requests have been received from other Member States in relation to credit-card cloning (three with Italy, one with Belgium, and two with Poland).

7.5.3 Surrender/Extradition

Surrender

The surrender procedure under the Framework Decision on the European Arrest Warrant and surrender procedure between the Member States establishes direct contact between issuing and executing judicial authorities, which has been taken over by the Romanian legislation. The Ministry of Justice as central authority rarely intervenes in the process, playing a merely administrative role. The authorities competent to receive EAWs are the Prosecutor's Offices attached to the Courts of Appeal, while the authorities competent to execute the EAWs are the courts of appeal. Regarding the issuing of an EAW, depending on the type of offence, all Romanian courts may be involved (based on material competence).

Statistical data on European Arrest Warrants issued in cybercrime cases in 2013 and 2014

Court of Appeal	Active	Passive
1.Oradea	4	7
2.Craiova	25	17
3. Ploiești	4	7
4.Pitești	5	7
5. Galați	-	4
6. Bacău	9	8
7. București	48	27
8. Brașov	1	1
9. Suceava	7	1
10. Timișoara	-	4
11. Constanța	4	2
12. Iași	6	70
TOTAL	**113**	**155**

Art. 96 of Law No 302/2004 mentions the list of 32 offences for which the double criminality check is lifted. Cybercrime, sexual exploitation of children and forgery of means of payment are included in that list. This very wide typology allows for a wide range of cybercrime offences as provided for by the Romanian Criminal Code to be included in the list. While observing the limits of the offences criminalising cybercrime and related offences as established by the new Criminal Code, it may be noted that most of the offences comply with the three-year threshold. Moreover, most of the time cybercrime offences are committed with participation in an organised criminal group and therefore the three-year threshold is most likely always met.

Extradition

The authority responsible for sending and receiving extradition requests is the Ministry of Justice. If the legal requirements provided for in the applicable international legal instrument and Law No 302/2004 are not met, the Ministry of Justice is entitled to require supplementary information or to return the requests. In the case of active requests, the Ministry of Justice is responsible for the drafting of the request, based on the annexed documentation provided by the relevant court.

Article 26 of Law No 302/2004 establishes that the seriousness of the offence is the criterion to be taken into account in order to establish whether an offence is extraditable or not. Romania is therefore not operating with a list of offences any more. There are two thresholds established - one of at least one year - if the extradition is sought for a criminal prosecution or trial of a person and one of four months - if the extradition is requested in order to execute a punishment.

Extradition requests and/or EAWs are processed as a matter of urgency, Romanian law establishing strict deadlines in that respect, whether the request is active or passive (corroborated with other legal instruments applicable). For example, in respect of the execution of the EAW, Romanian law establishes a maximum period of 90 days. If the person consents, the surrender decision is pronounced within ten days. On average, surrender based on an EAW takes place in less than one month. As regards extradition, the extradition process in Romania takes place on average two to three months. However, there are variations depending on the legal instrument applicable and deadlines for provisional arrest.

There are no specific procedures that have to be fulfilled to as regards the requests related to cybercrime. There is in general one procedure applicable, irrespective of the offence committed. On the other hand, extradition requests relating to cybercrime or to an EAW issued for cybercrime do have certain particularities that are determined by transnational character. Also on many occasions, positive conflicts of jurisdiction can occur, and in order to avoid such conflicts prior coordination between relevant authorities is needed.

In both cases, when Romania is the executing state in extradition and EAWs, the judicial authorities (the Romanian courts - specifically, the courts of appeal) decide on extradition/surrender.

7.6 Conclusions

- Romania seems to make wide use of the services offered by Eurojust and Europol and the possibilities for cooperation and coordination with regard to cybercrime. Romania acknowledges the support provided by Eurojust in facilitating communication with foreign authorities and in accelerating the execution of urgent requests to or from EU countries, exchanging data and information, and conducting operational meetings with other Member States or third parties. However, the practitioners met during the on-site visit raised the point that Eurojust could have a role in assisting practitioners by collecting best practices and case-law from other jurisdictions and disseminate that information to all Member States.

- The authorities met, in particular from the police, are very well aware of Europol/EC3. The Romanian police attend meetings of the Europol/EC3 Board and appreciate in particular the analysis reports carried out by Europol/EC3, and Europol/EC3's cooperation with private sector and third countries. The support provided by Europol's mobile office for the activities carried out in Romania and its integrated approach to cybercrime within Europol/EC3 in terms of cyber-attacks, online fraud and child pornography through information systems was also praised by practitioners.

- Romania's experience in cybercrime is thus a valuable asset in the fight against the cyber-related crimes identified by the EU as priorities. As an example, Romania took the role of a driver in online payment card fraud at the very beginning of the EU Policy Cycle (EMPACT) in 2012; subsequently it became co-driver for cyber-attacks in 2014 and 2015 and participant with regard to online child sexual exploitation in 2014 and 2015.

- There is a wide range of collaborative examples of CERT-RO with ENISA, such as on the programmes run by the latter, on supporting national CERTs and identifying their capabilities to support the work of law-enforcement agencies; participation in working groups and workshops, cyber-security conferences and cyber-exercises (Cyber-Europe 2012 and 2014), attendance at ENISA board meetings, etc. However, ENISA could develop a standardised format for the statistics analysed by CERT to make those statistics more comparable and harmonised across the EU.

- Romania is a member of EU Cybercrime Taskforce (EUCTF) and has been actively participating in the EUCTF activities and at the meetings. Cooperation with Interpol seems to be good. Romania takes advantages of services provided by the Interpol such as the ICSE database to identify victims of child abuse.

- Romania is open to cooperation with third countries, being a party to many international instruments providing a basis for legal assistance. Use is made most frequently of bilateral agreements (mostly with USA and Canada), multilateral agreements (Convention on Cybercrime, 1959 Convention and its two additional protocols, UNTOC, EU-Japan MLA Agreement, Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union), or bilateral agreements in conjunction with multilateral agreements (Bilateral Treaty with USA in conjunction with 2001 Budapest Convention or Bilateral Treaty with USA in conjunction with UNTOC and 2001 Budapest Convention). For the purpose of smooth cooperation Romania uses Interpol channels, 24/7 contact points, the network of liaison officers or established direct contacts.

- With regard to European Arrest Warrants (EAWs) Romania bases its cooperation on direct contacts between judicial authorities. The Ministry of Justice as central authority rarely intervenes in the process, playing a merely administrative role. There are statistics showing a tendency to apply EAWs also to cybercrime cases.

8 TRAINING, AWARENESS - RAISING AND PREVENTION

8.1 Specific training

Romania provides training on cybercrime targeted at specific groups of practitioners such as judges, prosecutors, police officers and IT experts but also the general public.

The National Institute of Magistracy (NIM) provides cybercrime training for judges and prosecutors. The training activities seek to familiarise judges and prosecutors with the methods for investigating crime in this area, providing magistrates with knowledge on the new *modi operandi* and on the information that can be obtained from private companies useful for conducting investigations or while handling files. The NIM organises approximately 2-3 seminars each year pertaining to cybercrime trends in Romania and including importance of the forensic investigative work relating to the new features and functions of mobile devices; digital evidence; the impact of cybercrime on the electronic payment system, trends and methods of investigation; cooperation of private companies with law enforcement institutions; the rules for conducting computer searches; and special investigative resources. In 2011 the NIM and Europol developed a project that included three two-day seminars in Cluj, Brasov and Bucharest for magistrates. Approximately 25 judges and prosecutors are invited to attend each seminar.

In addition, a 'Justice and Cybercrime conference is organised each year as decentralised continuous training with the support of Gorj Court. There are also regional events on cybercrime organised by judges themselves, such as the one held in Targu Jiu Court (for the past seven years) with the participation of judges, prosecutors and police officers. Trainers also included private-sector representatives.

CERT-RO is another institution very active in promoting the fight against cybercrime. Within the 'National System for Combating Cybercrime' project conducted by CERT-RO supported by a grant from the Administrative Capacity Development SOP 2007-2013, a training programme in preventing and combating cybercrime was developed. The training programme was divided into four modules:

Module I -	Legal aspects and public policies on cyber-security (40 participants) 27.01.2014 - 31.01.2014 5 days, 2 series of 20 persons each - simultaneously
Module II -	Certified Ethical Hacking (20 participants) 03.02.2014 - 07.02.2014 (first series) 10.02.2014 - 14.02.2014 (second series) 5 days, 2 series of 10 persons each
Module III -	Computer Hacking Forensic Investigator (20 participants) 03.03.2014 - 07.03.2014 (first series) 10.03.2014 – 14.03.2014 (second series) 5 days, 2 series of 10 persons each Malware analysis (10 participants, depending on results after evaluation) 07.04.2014 - 11.04.2014 5 days, 1 series of 10 participants
Module IV-	Cyber-type exercise (40 participants) 07.05.2014 – 09.05.2014 3 days, 1 series of 40 participants

The overall objective of the project was to create a suitable framework to increase capacity for the formulation and implementation of policies and for better regulation and strategic planning, by strengthening partnerships both at the inter-institutional level and between public institutions and representatives of other areas interested in fighting cybercrime.

Furthermore, intra- and extra-curricular activities include materials produced in the *Sigur.Info* project as well as resources developed by other projects that address this topic. The *Sigur.Info* project also includes a training component, so there is a resource person (teacher / inspector) in each county who has been trained under the project. Training sessions for volunteers on the topic of online safety are also organised.

In addition, the role of the Ministry of Education in training relating to cybercrime should also be highlighted. The Ministry's 'Developing managerial components of the teaching staff with competences in management, guidance and control from the undergraduate system in the knowledge society - OSCINT 2009 ID – 63376' is addressed to county school inspectorates and educational institutions. The general objective of the project is popularisation among teachers in positions involving management, guidance and control from the education system, with respect to the major conceptual landmarks within the OSCINT, Competitive Intelligence and Knowledge Management areas; knowledge of the OSCINT organisation - human resources, legal framework and OSCINT skills; the rationale for knowledge intelligence and knowledge management in undergraduate education; understanding the context in which knowledge / information is created, managed and used; familiarisation with the principles of collaborative intelligence and OSCINT collaborative working tools - TTP platform.

Training of police officers on cybercrime is provided through the National Annual Training Plan, which includes topics of interest, and also through other events organised with public institutions, foreign authorities or private partners. Individual participation in training courses by police officers is another way to ensure the level of knowledge required. The Annual Training Course on 'Searching information systems' was organised in 2014 at the ISPO for police officers working in organised crime structures. The course curriculum included presentations of procedures specific to searching information systems; legal and procedural issues concerning computer searches; identification, securing and collection of digital evidence, copying data storage media - procedural aspects and applications; presentation of software used in information system search activities; an overview of the basic features and configuration of EnCase Forensic software; and many other topics.

There are also specialised education modules in place aimed at IT-forensic examiners and cybercrime investigators. In the Service for Combating Cybercrime within the Romanian police training sessions are run periodically, or whenever needed, for police officers that operate in the computer forensic field. These courses are conducted by trainers from the Service for Combating Cybercrime for new or territorial officers to cover the need for training on the new IT developments.

Romania also participates in the European Cybercrime Training and Education Group (ECTEG) and contributes to new classes that are identified and developed. Thus, at the end of 2014, under the coordination of ECTEG and the University College Dublin, Romania participated in a European project which aimed to update three specific training courses in the field of cybercrime. The police officers also attended specialised training of personnel from law-enforcement agencies, organised by the European Police College (CEPOL) together with Europol, on: cybercrime forensics and digital evidence, in Tallinn, Estonia, in November 2014; cybercrime vs. cybersecurity, in Tampere, Finland, in October 2014; child abuse in cyberspace, in Barcelona, Spain, in April 2014; and a course on combating sexual exploitation of children on the internet, in Selm, Germany, in October 2014.

Professional training in cybercrime is the responsibility of public authorities competent in preventing and combating this phenomenon. The first national project for joint training of the police, prosecutors and judges - the Centre of Excellence in Cybercrime (CYBER-EX) was initiated by the Romanian police in cooperation with the DIOCT, the National Institute of Magistracy and others. At present specific actions are being taken to allow the centre to become operational and therefore to provide specific training starting from the second quarter of 2015 (courses, training sessions, etc.) that will facilitate the promotion, development and implementation of horizontal methods and tools to combat cybercrime. Nonetheless, it is worth mentioning that at the time of the on-site visit some events involving the participation of police officers, prosecutors and judges had been already organised.

8.2 Awareness-raising

The Decision on 30.09.2014 of the Supreme Council of National Defence mentions the inclusion of courses in the field of cyber-security in school training. To achieve this objective, the private sector has an important role to play in developing outreach campaigns and awareness events, especially for young people, on online threats and on the need to respect computer security measures. The private sector has been involved in outreach and awareness events such as Safer Internet Day and Cyber-Security Month.

On Safer Internet Day 2014, the eSafety Label was launched in Romania, a free online platform that supports ICT specialists and teachers in creating a safe school environment in terms of accessing the online environment. The platform provides several worksheets on topics such as cyber-bullying and online incident management, a forum where teachers can share experiences with other teachers across Europe, and which provides direct communication with eSafety experts, who will answer their questions through the platform. After completing an evaluation form of 30 questions, covering issues related to infrastructure, policies and practices, the school representative may download a customised action plan. This presents concrete measures to improve eSafety in their school. This unique European label shows parents and institutions that eSafety principles are taken seriously and that they are essential in the education of the young generation.

The 'Me and the internet' contest is a part of Safer Internet Day 2014; in it hearing-impaired children help creating a safer environment for themselves and for other hearing impaired children. The participants create a PhotoVoice gallery with ten representative photos that capture their online activity and their attitude to the internet gained in the eSign project, enrolling a collection of resources for hearing-impaired persons (selection of educational sites and blogs, electronic resources, videos, artwork, discussion groups, etc. specifically for hearing impaired persons).

Recently, the Commission for Education within the Chamber of Deputies of the Romanian Parliament discussed with representatives of public institutions, the private sector and NGOs the creation of a course on cybercrime to be introduced in schools, an activity which is in progress. School courses should present topics related to the submission of personal data over the internet, online child safety and cyber-threats.

8.3 Prevention

The National Strategy on Security and Public Order postulates a need for institutional consolidation to prevent and combat crime, while the police action plans provide concrete measures to improve prevention. It is also developed by Law No 161/2003 regulating the prevention and the fight against cybercrime through specific measures of prevention, detection and punishment of offences committed through computer systems, ensuring respect for human rights and personal data protection. It stipulates that public authorities, service providers, NGOs and other representatives of civil society undertake joint activities and programmes to prevent cybercrime to ensure the security of information systems and personal data protection. Therefore, they are expected to organise information campaigns on cybercrime and on the risks the users of information systems are exposed to.

Protection of children against abuse exercised via the internet is circumscribed in terms of the regulatory framework for the protection of child rights, general to the provisions of the specific law on child protection against all forms of abuse, neglect, exploitation. According to Law 272/2004 on the protection and promotion of children's rights, the child has the right to be protected from abuse, neglect, exploitation, trafficking, illegal migration, kidnapping, violence, pornography via the internet, and any forms of violence. Any natural person, including a child, may notify the General Directorate of Social Assistance and Child Protection from the county / district of domicile for it to take appropriate measures to protect them against all forms of violence, including sexual violence, harm or physical or mental abuse, ill treatment or exploitation.

At the same time, the National Strategy for the Protection and Promotion of Children's Rights, which covers the period 2014-2020, refers to the prevention and combating of all forms of violence and to the implementation of awareness actions including measures lowering children's exposure to violence in the media and in the online environment. The Romanian authorities indicated that in order to achieve this goal, the legislation on child protection against the forms of violence should be amended.

The other initiative, called *Together we make the internet better*, conducted within *Sigur.Info,* is a project that seeks to involve children, young people, parents and teachers in shaping ideas through which users can build a better internet together, by moderating their own behaviour, by modelling positive behaviours to other users, by reporting illegal, inappropriate or harmful content and by creating opportunities for collaboration, teamwork and knowledge sharing. The theme of the 2014 competition focused on the responsibility that society (including children, parents, teachers, educators and politicians) must take for making the internet a better and safer place. Moreover, this competition seeks to raise awareness among children, young people, teachers and parents regarding the opportunities that the internet offers and to identify behaviours by means of which users can create a better online environment, proposing innovative ways whereby users, representatives of the industry (Facebook, Google, etc.) and public institutions can contribute to this end. The competition is open to all schools, youth clubs and children. The *Together we make the internet better* competition also has special categories, awarding the individuals and institutions that are most involved in promoting and ensuring a responsible online activity in 2013:

•The teacher of the year - the teacher most involved in activities to promote and raise awareness of online safety among students and community;

•The school of the year - the school with the highest number of activities to promote and raise awareness on online safety among students;

•The kindergarten of the year- the kindergarten showing most clearly and creatively the national competition topic *Together we make the internet better!* in a team project;

•*Sigur.Info* volunteer of the year - the most active *Sigur.Info* volunteer, who has promoted online safety amongst target groups and initiated his/her own projects and activities to ensure responsible behaviour in using the internet.

The Romanian authorities also gave examples of the most important events on cybercrime prevention held in 2014, on:

- cyber-security, to build an interactive platform for dialogue between decision-makers and IT specialists on 2 October 2014;
- cyber-risks in financial services, on 9 October 2014;
- NEC technological seminar, on 14 October 2014 - organised by the NEC Corporation and CERT-RO;
- the future and safety of electronic payment services, on 16 October 2014 - organised by Romanian Banking Association (ARB), National Association for Information Systems Security (ANSSI) and CERT-RO;
- UTI Cyber-Security, on 29 October 2014 (included in the ENISA's cyber-security month series);
- New Global Challenge to Cyber-Security, on 3 November 2014;
- "CYBERTHREATS" conference, on 13 November 2014.

The Romanian Banking Institute (RBI) held the seventh edition of their 'Cyber-threats' conferences, in partnership with the CIO Council Romania, and with contributions from officials of the Intelligence Service, CERT-RO, Romanian National Bank (BNR) and the ARB, financial institutions and government institutions, as well as audit firms and technology and security companies. This edition focused on the major risks from old and new threats, and methods to keep up with both technological and procedural principles and methods of crisis management.

Within the cybercrime project 'The National System of Combating Cybercrime, conducted by the CERT-RO, four sets of policy proposals were developed, aiming at improving the working environment so as to strengthen the capacity to formulate public policies and to achieve better regulation and strategic planning by consolidating partnerships both at inter-institutional level and between public institutions and representatives of other fields interested in fighting cybercrime.

8.4 Conclusions

- The National Institute of Magistracy provides cybercrime training for judges and prosecutors, whereas the Police Academy for police officers. In addition, the concept of 'joint training' for police officers, prosecutors and judges has been already used in various events organised by the Romanian authorities.

- This initiative should furthermore be strengthened when the Cybercrime Centre of Excellence (CYBER-EX) becomes fully operational, which is expected to happen in 2016. The opening of the CYBER-EX should facilitate the promotion, development and implementation of horizontal methods and tools to combat cybercrime. This possibility is likely to be a particular asset for the judicial sector in enhancing its expertise in cybercrime. CYBER-EX could also provide expert advice and a contact point for cybercrime-related issues, notably for judges dealing with cybercrime cases, since there are no specialist judges in this field, unlike the case with the police and prosecutors.

- Therefore, the evaluators believe that the setting up of CYBER-EX to organise training for all authorities involved in the investigation, prosecution and adjudication of cybercrime cases, and with trainers from all sectors should be considered as an example of best practice.

- The evaluation team was also informed that judges are organising themselves in terms of training on cybercrime, e.g. the Targu Jiu Court. Trainers from the private sector were also involved. The evaluators believe that the fact that judges have been taking the initiative to organise more training opportunities on cybercrime matters, and in liaison with police and prosecutors is an example of best practice to follow. In the opinion of evaluators, establishing a network of magistrates specialised in cybercrime matters could also spread knowledge of cybercrime.

- It should also be mentioned that many other institutions are organising training for lawyers and IT experts. Cybercrime training is provided by ECTEG and Europol, among other organisations. That training, however, increasingly focuses on e-learning and open-source tools rather than commercial tools. Although Romania successfully uses the resources offered by Eurojust, Europol and ENISA, not much training is provided to practitioners on the possibilities offered by those institutions.

- Since Romania is a relatively large country it may be challenging to provide training to geographically dispersed units. In the evaluators' view, implementation of e-learning for some types of training (first-responder training, open-source intelligence, scripting, introduction to static malware analysis etc.) could lead to more effective learning and improve use of resources. Either the training materials could be provided by ECTEG, or courses could be developed in-house or in cooperation with UCD or Romanian University.

- The CERT-RO is also very active in training and awareness campaigns. It organises mini TV series, technical seminars and conferences, and issues high-impact alerts on the CERT website.

- The Ministry of Education is very involved in the prevention of cybercrime and cyber-security. It supports awareness-raising initiatives, also in good cooperation with relevant actors from the private sector, in particular hotlines and similar institutions (Child Helpline Association), especially in the field of child abuse. It also develops learning materials for primary schools and organises different events to create awareness on cyber-security. They seek (rather like the *Sigur.info* project) to prevent citizens from becoming victims of cybercrime (training for teachers, students and parents). This type of awareness-raising campaigns and education provided to society should be regarded as an example of best practice.

- The private sector is also involved in organising awareness-raising campaigns and in the joint training courses with the law-enforcement authorities. According to the Romanian authorities, collaboration with the private sector in the field of preventing and combating cybercrime takes place in good conditions. However, organising regular meetings or a structure to discuss incidents, trends and developments with regard to cybercrime could strengthen this cooperation.

- The prevention of crimes committed through and on the internet could benefit from enhanced and more targeted activity from relevant public authorities and the development of private / public partnership. This could include awareness-raising activities on fraud and cyber-security as well as preventive measures taken by the private sector, such as ISPs and the banking sector.

9 FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Romania

Crime and cyber-security are major concerns for the Romanian Government due to the fact that Romania is confronted with cross-border organised crime, including cybercrime. From the Romanian perspective, the cross-border nature of the criminal activity pertaining to cybercrime and the difficulties linked to obtaining evidence through international cooperation, or obtaining identifications for IP addresses or other data are among the main obstacles hampering the successful countering of cybercrime. Moreover, institutional capacity-building, harmonisation of legislation and allocation of financial resources must be conducted in accordance with international standards and developments.

Romania wishes to continue to support the efforts of the international community to combat cybercrime.

9.2 Recommendations

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

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

The evaluation team thought fit to make a number of suggestions for the attention of the Romanian authorities. Based on various good practices, related recommendations to the EU, its institutions and agencies, Eurojust, Europol and ENISA, are also put forward.

9.2.1 Recommendations to Romania

1. Romania should work out a method for collecting standardised and overall statistics on investigations, prosecutions and convictions relating to cybercrime, broken down into specific cybercrime areas, preferably those identified at EU level, namely online child sexual abuse, online card fraud and cyber-attacks; (cf. 3.3, and 3.5)

2. Romania should enhance the work of CERT-RO by increasing the number of staff to reach the budgeted staff complement; (cf. 3.1, 4.3, 4.4.2 and 4.5)

3. Romania should regulate the concept of Cyber-Infrastructures of National Interest (CINI) and establish a national legal instrument that stipulates specific tasks for operators of CINIs, including private companies with responsibility for critical infrastructures in the event of a cyber-attack, and organise a structure allowing information about developments and incidents to be shared; (cf. 4.3 and 4.5)

4. Romania should consider strengthening the role of the Operational Council of Cyber-Security (OCCS) as a body coordinating efforts of public institutions involved in cyber-security, and explore the possibility of including other bodies in its composition (such as the Ministry of Education) and establishing a mechanism to facilitate private-sector contributions to the Cyber-Security National System; (cf. 4.4.1 and 4.5)

5. Romania should fully implement Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and the sexual exploitation of children and child pornography; (cf. 5.1.2 and 5.5)

6. Romania should consider constituting a common concept of cybercrime to be shared by all stakeholders tackling cybercrime; (cf. 5.1.2 and 5.5)

7. Romania should consider organising regular meetings or a structure to discuss incidents, trends and developments with representatives of the private sector (from banks, ISPs and IT companies) on cybercrime; (cf. 6.1.2 and 6.4)

8. Romania should consider developing and using specific tools to filter websites for child pornographic content, to complement the possibilities of using to its full potential the legal obligation for internet service providers to remove illegal materials involving minors; (cf. 6.2.4 and 6.4)

9. Romania should be encouraged to continue training activities involving police, prosecutors and judges and to include in these training activities information on the support which may be offered to national authorities by Eurojust, Europol and ENISA; (cf. 8.1 and 8.4)

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

1. Member States should explore any possibilities available, inter alia by reference to Directive 2002/58/EC, and engage in dialogue with the private sector, to seek possibilities for retaining data; (cf. 3.2, 3.5 and 5.5)

2. Member States should consider exploring cooperation between law-enforcement agencies and national intelligence services in the fight against cybercrime, such as that existing in Romania, specifically in obtaining and processing digital evidence; (cf. 4.3 and 4.5)

3. Member States should consider engaging in dialogue with the private sector to discuss methods of ensuring that information-gathering takes place in such a way that it is admissible in courts; (cf. 5.2 and 5.5)

4. Member States should seek a legal solution to cover the gap resulting from the lack of legal solutions allowing for location and access to data in the cloud; (cf. 5.4.3, 5.4.4 and 5.5)

5. Member States should consider providing practitioners with standard operating procedures to support the implementing of legislation on cybercrime, similar to those prepared by the Romanian police; (cf. 6.1.2 and 6.4)

6. Member States should make the best possible use of the services offered by Eurojust and Europol with regard to cybercrime, and provide close cooperation between their national CERTs and ENISA; (cf. 7.1.2 and 7.6)

7. Member States should be encouraged to involve a wide range of actors and programmes in preventing cybercrime, including institutions responsible for the education of pupils and students, along the lines of the actions undertaken by the Romanian Ministry of Education; (4.3, 4.4.1, 4.4.2, 6.2.3, 8.1, 8.3 and 8.4)

8. Member States should explore the feasibility of carrying out joint cybercrime training (covering the life-cycle of cybercrime cases) for police officers, prosecutors and judges, and using for that purpose a platform like CYBER-EX in Romania, involving representatives of police, prosecutorial and judicial authorities and the private sector as participants and speakers; (cf. 8.1 and 8.4)

9. Member States should encourage and support judges taking initiatives to organise more training opportunities to raise awareness of cybercrime in liaison with police and prosecutors; (cf. 8.1 and 8.4)

10. Member States should consider establishing a network of magistrates specialising in cybercrime matters, inter alia with a view to facilitating the spreading of best practices amongst practitioners; (cf. 8.1 and 8.4)

11. EU institutions should encourage and further support initiatives to organise training to cover the whole life-cycle of cybercrime cases, targeting police, prosecutors and judges; (cf. 8.1 and 8.4)

12. EU institutions should address the issue of data retention as soon as possible; (cf. 3.2 and 3.5)

9.2.3 Recommendations to Eurojust/Europol/ENISA

1. ENISA should explore how to standardise the concept of cyber-alerts collected and transmitted by automated systems, which would allow the statistics on these alerts to be comparable and harmonised throughout Member States; (cf. 7.1.2 and 7.6)

2. Eurojust should consider collecting and disseminating best practices at national level identifiable from national and Eurojust casework, in particular when judicial cooperation in criminal matters is involved; (cf. 7.1.2 and 7.6)

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

Monday, 19 January 2015, Bucharest		Participants
	Arrival of the delegation	
17h30 – 19h00	Informal meeting at the hotel bar	Romanian Police, Ministry of Justice, Public Ministry
Tuesday, 20 January 2015, Bucharest (The National Police headquarters)		
9h00- 10h00	Welcoming remarks	High-level officials from the Ministry of Internal Affairs, Romanian Police, Ministry of Justice, Public Ministry, Romanian Intelligence Service, CERT-RO, Ministry of National Education
Short break		
10h00-10h45	Introduction from the evaluation team and general discussion	Representatives from the Ministry of Internal Affairs, Romanian Police, Ministry of Justice, Public Ministry, Romanian Intelligence Service, CERT-RO, National Authority on the Protection of Children, Ministry of Education
10h45-11h00	*Coffee break*	
11h00-11h15	Presentation of the relevant substantive law provisions on cybercrime	Ministry of Justice
11h15-11h30	Presentation of the procedural law provisions on cybercrime	Directorate for the Investigation of Organised Crime and Terrorism (DIOCT) within the Public Ministry - the Service for the Prevention and Fight against Cybercrime
11h30 – 12h30	Discussion	Representatives of the Ministry of Justice, Public Ministry and Romanian National Police
12h30-14h00	*Lunch break*	
14h00-14h10	Transfer to the Public Ministry	
14h10-15h10	Meeting with DIOCT	Representatives of the Service for the Prevention and Fight against Cybercrime and representatives of the International Cooperation Service
15h10-15h30	Transfer to the Romanian National Police	
15h30-17h00	Visit to the Romanian Cybercrime Unit Discussion on: organisation, responsibilities, inter-agency cooperation, cooperation with the private sector and international cooperation	Representatives of the Cybercrime Unit from the Romanian National Police
17h00	Closing and transfer to the hotel	

Wednesday, 21 January 2015, Bucharest		
9h00-9h30	Transfer to CERT-RO	
9h30-10h30	Meeting at CERT-RO Discussion on: organisation, responsibilities, running projects, inter-agency cooperation, international cooperation	Representatives of CERT-RO
10h30-11h00	Transfer to the Romanian Intelligence Service	
11h00-12h00	Meeting with the Romanian Intelligence Service Discussion on: organisation, responsibilities, the cyber security strategy, inter-agency cooperation, international cooperation	Representatives of the Romanian Intelligence Service
12h00-14h00	*Lunch break*	
14h00-14h30	Transfer to SELEC	
14.30-15.30	Meeting with SELEC	Representatives of Southeast European Law Enforcement Centre (SELEC)
15h30-16h00	Transfer to C-PROC	
16h00-17h30	Meeting with C-PROC	Representatives of the Council of Europe's Office on Cybercrime
19h30-22h00	*Dinner*	
Thursday, 22 January 2015, Craiova		**Participants**
8h00-11h00	Travel from Bucharest to Craiova	
11h00-13h00	Meeting at Prosecutor's Office and Police Cybercrime Unit from Craiova Discussion on: organisation, responsibilities, cases, cooperation	Representatives of the Prosecutor's Office, the Police Cybercrime Unit (Craiova),
13h00-14h30	*Lunch break*	
14.30-17.30	Travel from Craiova to Bucharest	

Friday, 23 January 2015, Bucharest (The National Police)		Participants
9h00-9h30	Transfer to the Romanian National Police	
9h30-10h00	Overview of the evaluation visit	Representatives from the Ministry of Internal Affairs, Romanian Police, Ministry of Justice, Public Ministry, Romanian Intelligence Service, CERT-RO, National Authority on the Protection of Children, Ministry of Education
10h30-10h45	*Coffee break*	
10h45-12h00	General remarks and conclusions	
12h00	*Lunch and departure of the experts*	
End of the visit		

-/-

ANNEX B: PERSONS INTERVIEWED/MET

MEMBERS OF THE DELEGATIONS			
	Name	**Institution**	**Contact details**
ROMANIA	**Ministry of Internal Affairs**		
	Ms Claudia VIŞOIU	Deputy Director Directorate for European Affairs and International Relations	claudia.visoiu@mai.gov.ro
	Ms Simona ŞTEFAN	Head of Service Directorate for European Affairs and International Relations	
	Ms Diana BĂDESCU	Expert Directorate for European Affairs and International Relations	sae@mai.gov.ro
	The General Inspectorate of the Romanian Police		
	Mr Virgil SPIRIDON	Deputy Inspector-General General Inspectorate of the Romanian Police	virgil.spiridon@root.ro
	Mr Marius ROMAN	Director Directorate for European Affairs, Missions and International Relations	marius.roman@mai.gov.ro
	Mr Marcel PATATU	Head of Service Service for Combating Cybercrime Directorate for Combating Organised Crime	cybercrime@politiaromana.ro
	Mr Andrei LINŢĂ	Head of Office European Affairs Unit Directorate for European Affairs, Missions and International Relations	integrare@politiaromana.ro
	Ms Mihaela RADU	Specialist officer European Affairs Unit Directorate for European Affairs, Missions and International Relations	mihaela.radu@politiaromana.ro

	Mr Daniel FILIP	Head of office Service for Combating Cybercrime Directorate for Combating Organised Crime	Dl. Daniel FILIP
	Mr Paul ROMAN	Head of Office Service for Combating Cybercrime Directorate for Combating Organised Crime	Dl. Paul ROMAN
	Mr Silviu CRIŞAN	Head of Office Service for Combating Cybercrime Directorate for Combating Organised Crime	Dl. Silviu CRIŞAN
	Mr Bogdan BADIU	Head of Office Service for Combating Cybercrime Directorate for Combating Organised Crime	Dl. Bogdan BADIU
	The Public Ministry Directorate for the Investigation of Organised Crime and Terrorism (DIOCT) Service for the Prevention and Fight against Cybercrime		
	Ms Ioana ALBANI	Chief Prosecutor	albani_ioana@mpublic.ro
	Ms Camelia STOINA	Prosecutor	
	Mr Viorel BADEA	Chief Prosecutor	
	Mr Cătălin CAMBURI	Chief Prosecutor	
	Ms Silvia POPA	Prosecutor	
	Ms Elena DINU	Prosecutor	
	Mr Marius CRIVAT	Prosecutor	

	Ministry of Justice		
	Ms Viviana ONACA	Director Directorate for International Law and Judicial Cooperation	vonaca@just.ro
	Ms Cristina SCHULMAN	Legal adviser having the status of judge/prosecutor Treaties, International Relations and Liaison Magistrates Unit Directorate for International Law and Judicial Cooperation	cschulman@just.ro
	Ms Raluca SIMION	Legal adviser having the status of judge/prosecutor Service for Judicial Cooperation in Criminal Matters Directorate for International Law and Judicial Cooperation	rsimion@just.ro
	Ms Mihaela MEREUȚĂ	Counsellor for European Affairs Directorate for European Affairs and Human Rights	mihaela.mereuta@just.ro
	Romanian Intelligence Service		
	Mr Florin COSMOIU	Colonel	florin.cosmoiu@cyberint.ro
	Mr Gabriel MAZILU	Colonel	
	Mr Lucian MARINESCU	Captain	
	Mr Cristian CONDREA	Colonel	
	Ms Luiza IORDACHE	Major	
	CERT-RO		
	Mr Augustin JIANU	Director-General	
	Mr Mircea GRIGORAS	Deputy Director-General	
	Mr Dan TOFAN	Technical Director	
	Mr Daniel IONITA	Head of the Legal, Analyses and Policies Department	daniel.ionita@cert-ro.eu

	National Authority on the Protection of Children		
	Mr Octavian CIOBA	Senior Counsellor	octavian.cioba@anpdca.ro
	Ministry of Education and Scientific Research		
	Mr Eugen STOICA	Department for Education and Lifelong Learning	eugen.stoica@medu.edu.ro
	Ms Megdonia PĂUNESCU	Counsellor Department for Education and Lifelong Learning	megdonia@gmail.com megdonia.paunescu@medu.edu.ro
	Ms Daniela CĂLUGĂRU	General Inspector Department for Education and Lifelong Learning	calugaru.daniela@gmail.com daniela.calugaru@medu.edu.ro

-//-

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ROMANIAN ACRONYM OR ACRONYM IN ORIGINAL LANGUAGE	ROMANIAN ACRONYM OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
AFP	*AFP*		Australian Federal Police
BCEAR	*BCEAR*		Bucharest Centre for Educational Assistance and Resources
CCEAR	*CCEAR*		County Centre for Educational Assistance and Resources
CEPOL	*CEPOL*		European Police College
CERT-RO	*CERT-RO*		Romanian National Computer Security Incident Response Team
CINI	*CINI*		Cyber-Infrastructures of National Interest
CPC	*CPC*		Criminal Procedure Code
C-PROCMSINF	*C-PROC*		Cybercrime Programme Office of the Council of Europe
CSAT	*CSAT*		Supreme Council of National Defence
	CSNS		Cyber-Security National System
CYBER-EX	*CYBER-EX*		Cybercrime Centre of Excellence
DIOCT	*DIOCT*		Directorate for Investigating Organised Crime and Terrorism
DIPI	*DIPI*		Department for Information and Internal Protection
ECTEG	*ECTEG*		European Cybercrime Training and Education Group

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ROMANIAN ACRONYM OR ACRONYM IN ORIGINAL LANGUAGE	ROMANIAN ACRONYM OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
EWS	*EWS*		Early Warning and real-time information System
ISF	*ISF*		Internal Security Funds
MSINF	*MSINF*		Ministry for the Information Society
NACPA	*NACPA*		National Authority for Child Protection and Adoption
NFSI	*NFSI*		National Forensic Science Institute
OCCS	*OCCS*		Operational Council of Cyber-Security
RIS	*RIS*		Romanian Intelligence Service
RNP	*RNP*		Romanian National Police's Service for Combating Crime
SCND	*SCND*		Supreme Council of National Defence

-//-

ANNEX D: ROMANIAN LEGISLATION

The relevant crimes are criminalised under the following chapters in the **Criminal Code**:

Title II. Offences against property. Chapter IV - Fraud perpetrated using computer systems and electronic payment methods

Title VI. Forgery offences. Chapter III - Counterfeiting documents

Title VII. Offences against public security. Chapter VI - Offences against the security and integrity of computer systems and data

Title I. Offences against individuals. Chapter VIII- Offences against sexual freedom and integrity

Title VIII. Offences that harm social cohabitation relationships. Chapter I - Offences against public order

Title II. Offences against property. Chapter IV- Fraud perpetrated using computer systems and electronic payment methods

Article 249 - Computer fraud

Entering, altering or deleting computer data, restricting access to such data or hindering in any way the operation of a computer system in order to obtain a benefit for oneself or another, if it has caused damage to a person, shall be punishable by no less than two and no more than seven years of imprisonment.

Article 250 - Making fraudulent financial operations

(1) Making cash withdrawal operations, loading or unloading of an electronic money instrument or a fund transfer instrument, by using, without the consent of the owner, an electronic payment instrument or the identification information that allows its use, shall be punishable by no less than two and no more than seven years of imprisonment.

(2) The same penalty is applicable to the operations referred to in paragraph (1), performed by means of the unauthorised use of any identification information or by using false identification data.

(3) The unauthorised transmission to another person of any identification information, in order to perform one of the operations referred to in paragraph (1), shall be punishable by no less than one and no more than five years of imprisonment.

Title VI. Forgery offences. Chapter III - Counterfeiting documents

Article 325 - Computer data forgery

Unauthorised input, alteration or deletion of computer data, or unauthorised restriction of access to such data, resulting in inauthentic data to be used to produce legal consequences, constitutes an offence and shall be punishable by no less than one and no more than five years of imprisonment.

Title VII. Offences against public security. Chapter VI - Offences against the security and integrity of computer systems and data

Article 360 - Illegal access to a computer system

(1) Unauthorised access to a computer system shall be punishable by no less than three months and no more than three years of imprisonment or by a fine.

(2) The act referred to in paragraph (1), perpetrated in order to obtain computer data, shall be punishable by no less than six months and no more than five years of imprisonment.

(3) If the act referred to in paragraph (1) was perpetrated a computer system to which, through processes, devices or specialised programmes, access is restricted or prohibited for certain categories of users, it shall be punishable by no less than two and no more than seven years of imprisonment.

Article 36 - Illegal interception of computer data transmissions

(1) Unauthorised interception of a computer data transmission which is not public and which is intended for a computer system, originates from such a computer system or is carried out within a computer system shall be punishable by no less than one and no more than five years of imprisonment.

(2) The same penalty shall apply to the unauthorised interception of electromagnetic emissions from a computer system containing computer data which is not for public information.

Article 362 - Altering computer data integrity

Illegally altering, deleting or damaging computer data or restricting access to such data shall be punishable by no less than one and no more than five years of imprisonment.

Article 363 - Disruption of the operation of computer systems

The act of seriously disrupting, without authorisation, the operation of a computer system by inputting, transmitting, modifying, deleting or damaging data, or by restricting access to data, shall be punishable by no less than two and no more than seven years of imprisonment.

Article 364 Unauthorised transfer of computer data

The unauthorised transfer of computer data from a computer system or from a data storage device shall be punishable by no less than one and no more than five years of imprisonment.

Article 365 Illegal operations with devices or software

(1) Any person who illegally produces, imports, distributes or makes available in any form:

(a) devices or software designed or adapted for the purpose of perpetrating any of the offences referred to in Articles 360 - 364;

(b) passwords, access codes or other such computer data allowing full or partial access to a computer system for the purpose of perpetrating any of the offences referred to in Articles 360 - 364shall be punishable by no less than six months and no more than three years of imprisonment or by a fine.

(2) Illegally owning a software program, password, access code or other data as mentioned in paragraph (1), with the purpose of perpetrating any of the offences referred to in Articles 360 - 364, shall be punishable by no less than three months and no more than two years of imprisonment or by a fine.

Title VIII. Offences that harm relationships of social cohabitation. Chapter I - Offences against public order

Article 374 - Child pornography

(1) The production, possession for display or distribution, purchase, storage, display, promotion, distribution and provision, in any manner, of child pornography shall be punishable by no less than one and no more than five years of imprisonment.

(2) If the acts referred to in paragraph ?? are perpetrated via a computer system or other means of data storage, they shall be punishable by no less than two and no more than seven years of imprisonment.

(3) The act of unlawfully accessing child pornography through computer systems or other means of electronic communication shall be punishable by no less than three months and no more than three years of imprisonment or by a fine.
(4) Child pornography means any material that shows a minor displaying sexually explicit behaviour or that, even if not showing a real person, simulates in a credible manner a minor displaying such behaviour.
(5) Any such attempt shall be also punished.

Article 6 of Law No 365/2002 (republished) sets out the legal conditions for transmitting commercial communications via electronic mail, i.e commercial communications via electronic mail are forbidden, except where the recipient has expressed his or her agreement to receiving such communications.
Infringement of this rule is considered a contravention, pursuant to Article 22, indent 1, item a, of Law No 365 (republished).
In practice, however, depending on the content or the amount of communications, the act of transmitting commercial communications via electronic mail may constitute an actual offence, either as committed by a perpetrator (Article 363 of the Criminal Code or Article 325 of the Criminal Code) or by an accomplice to one or more computer offences.

Trafficking in underage persons (Article 211)
(1) Recruitment, transportation, transfer, harbouring or receipt of a minor for the purpose of his her exploitation shall be punishable by no less than three and no more than 10 years of imprisonment and a ban on the exercise of certain rights.
(2) If such act was perpetrated under the terms of Article 210 paragraph (1) or by a public servant while fulfilling his or her professional duties and prerogatives, it shall be punishable by no less than five and no more than twelve years of imprisonment and a ban on the exercise of certain rights.
(3) The consent of an individual who is a victim of trafficking does not represent grounds for justification of the act.

Exploitation of persons **(Article 182)**

Exploitation of persons means:

(a) forcing a person to carry out work or tasks;

(b) enslavement or other similar procedures implying deprivation of freedom;

(c) forcing persons into prostitution, pornography - with a view to obtaining and distributing pornographic material - or any other types of sexual exploitation;

(d) forcing persons into mendicancy;

(e) illegal collection of body organs, tissues or other cells.

Rape **(Article 218)**

(1) Sexual intercourse, oral or anal intercourse with a person, perpetrated by constraint, by rendering the person in question unable to defend themselves or to express their will, or by taking advantage of such state, shall be punishable by no less than three and no more than 10 years of imprisonment and a ban on the exercise of certain rights.

(2) The same penalty shall apply to any act of vaginal or anal penetration perpetrated under paragraph (1).

(3) It shall be punishable by no less than five and no more than twelve years of imprisonment and a ban on the exercise of certain rights, when:

(a) the victim is entrusted to the perpetrator for care, protection, education, safeguarding or treatment;

(b) the victim is a first degree relative, i.e. brother or sister;

(c) the victim has not reached the age of 16 years;

(d) the act was perpetrated for the production of pornography;

(e) the act resulted in bodily injury;

(f) the act was perpetrated by two or more individuals, acting together.

(…)

Sexual assault **(Article 219)**

(1) An act with a person that is sexual in nature, other than the acts referred to in Article 218, and is perpetrated by constraint, by rendering the person in question unable to defend themselves or to express their will or by taking advantage of such state, shall be punishable by no less than two and no more than seven years of imprisonment and a ban on the exercise of certain rights.

(2) It shall be punishable by no less than three and no more than 10 years of imprisonment and a ban on the exercise of certain rights, when:

(a) the victim is entrusted to the perpetrator for care, protection, education, safeguarding or treatment;

(b) the victim is a first degree relative, i.e. brother or sister;

(c) the victim has not reached the age of 16 years;

(d) the act was perpetrated for the production of pornography;

(e) the act resulted in bodily injury;

(f) the act was perpetrated by two or more individuals, acting together.

(…)

Sexual intercourse with a minor **(Article 220)**

(1) Sexual intercourse, oral or anal sex, as well as any act of vaginal or anal penetration perpetrated against a minor aged 13 to 15 years old, shall be punishable by no less than one and no more than five years of imprisonment.

(2) The acts referred to in paragraph (1), perpetrated against a minor who has not reached the age of 13, shall be punishable by no less than two and no more than seven years of imprisonment and a ban on the exercise of certain rights.

(3) The acts referred to in paragraph (1), perpetrated against a minor aged 13 to 18 by a person of the age of majority who abused their authority or influence over the victim, shall be punishable by no less than two and no more than seven years of imprisonment and a ban on the exercise of certain rights.

(4) The acts referred to in paragraphs (1) to (3) shall be punishable by no less than three and no more than 10 years of imprisonment and a ban on the exercise of certain rights, when:

(a) the minor is a first degree relative, i.e. brother or sister;

(b) the minor is entrusted to the perpetrator for care, protection, education, safeguarding or treatment;

(c) the act was perpetrated for the production of pornography.

(…)

Sexual corruption of minors **(Article 221)**

(1) Perpetrating an act that is sexual in nature, other than the acts referred to in Article 220, against a minor who has not reached the age of 13, as well as forcing a minor to endure or carry out such an act, shall be punishable.

(4) Child pornography means any material which shows a minor displaying sexually explicit behaviour or which, even if not showing a real person, simulates in a credible manner a minor displaying such behaviour.

(5) Any such attempt shall be also punished.

Note: Romania penalises the transmission of pornographic material involving minors irrespective of the manner in which such material is transmitted (for example, via mobile phone).

Harassment (Article 208)

(1) The act of an individual who repeatedly, with or without a legitimate interest, pursues an individual or observes their domicile, workplace or other places frequented by them, thus provoking a state of fear in them, shall be punishable by no less than three and no more than five years of imprisonment.

(2) It shall be punishable by no less than two and no more than seven years of imprisonment and a ban on the exercise of certain rights, when:

(a) the minor is a first degree relative, i.e. brother or sister;

(b) the minor is entrusted to the perpetrator for care, protection, education, safeguarding or treatment;

(c) the act was perpetrated for the production of pornography.

(3) A sexual act of any nature, perpetrated by a person of the age of majority in the presence of a minor who has not reached the age of 13, shall be punishable by no less than six months and no more than two years of imprisonment or by a fine.

(4) Where a person of the age of majority forces a minor who has not yet reached the age of 13 to witness the perpetration of acts that are exhibitionist in nature or shows or performances in which sexual acts of any kind are perpetrated, and makes available to the minor materials that are pornographic in nature, such act shall be punishable by no less than three months and no more than one year of imprisonment or by a fine.

(5) The acts referred to in paragraph (1) shall not be punished if the age difference does not exceed three years.

Recruitment of minors for sexual purposes **(Article 222)**

The act of an individual of the age of majority proposing to a minor who has not yet reached the age of 13 to meet for the purposes of the perpetration of one of the acts referred to in Article 220 or Article 221, including when such proposal has been made using remote means, shall be punishable by no less than one month and no more than one year of imprisonment or by a fine.

The following definitions are used in Romanian law:

Article 35 of Law No 161/2003

(1) In this title, the following words and expressions have the following meaning:

(a) 'computer system' means any device or group of interconnected or related devices, of which one or more ensure the automatic processing of data by using a computer program;

(b) 'automatic data processing' means the process by which data from a computer system are processed through a computer program;

(c) 'computer program' means a set of instructions that can be performed by a computer system to achieve a specific result;

(d) 'computer data' means any representation of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can determine performance of a function by a computer system;

(e) 'service provider' shall mean:

1. any natural or legal person that offers users the ability to communicate through computer systems;

2. any other natural or legal person that processes or stores data for the persons referred to under point 1 and for users of services provided by them;

(f) 'data on traffic information' shall mean any computer data related to a communication made via a computer system and its products, which is part of the communication chain, indicating the origin, destination, route, time, date, size, volume and duration, and type of service used for communication;

(g) 'user data' shall mean any information that may lead to the identification of a user, including type of communication and service used, address, geographical location, phone numbers or any other access numbers and manner of payment of that service, and any other data that may lead to identification of the user;

(h) 'security measures' shall mean the use of procedures, tools or specialised computer programmes by which access to a computer system is restricted or prohibited for certain categories of users;

(i) 'child pornography' shall mean any material that shows a minor displaying explicit sexual behaviour or an adult who is presented as a minor displaying explicit sexual behaviour or images which, while not representing a real person, simulates in a credible manner a minor displaying explicit sexual behaviour.

(2) Within the meaning of this Title, persons in one of the following situations are deemed to act illegally if:

(a) they are not authorised by law or a contract;

(b) they exceed the limits of authorisation;

(c) they do not have permission from the person or entity responsible, by law, to grant, use, manage or control a computer system or to conduct scientific research or perform any other operation in a computer system.

The Criminal Code

Article 181 - Computer systems and electronic data

(1) 'Computer systems' means any device or group of (functionally) interconnected devices, where one or several of such systems ensure automatic processing of data, using a computer program.

(2) 'Electronic data' means any representation of acts, information or concepts in a manner which allows processing by means of a computer system.

The Criminal Procedure Code

Article138

(4) A 'computer system' is any device or combination of devices interconnected between them or in a functional relationship, one or more of which provide automatic data processing by means of a computer program.

(5) 'Computer data' is any representation of facts, information or concepts in a form appropriate for processing in a computer system, including a program able to determine the performance of a function by a computer system.