Council of the
European Union

Brussels, 5 April 2016
(OR. en)

10953/15
DCL 1

GENVAL 27
CYBER 73

DECLASSIFICATION

of document:	10953/15 UE RESTREINT/EU RESTRICTED
dated:	12 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 Estonia

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, 12 January 2016
(OR. en)

10953/15

RESTREINT UE/EU RESTRICTED

GENVAL 27
CYBER 73

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 Estonia

EVALUATION REPORT ON THE SEVENTH ROUND OF MUTUAL EVALUATIONS

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

REPORT ON ESTONIA

Table of Contents

1. EXECUTIVE SUMMARY

Estonia is an advanced digital country characterised by its high level of internet access and the widespread use of IT both in the public and private spheres. As a country that is largely dependant on the Internet and after the cyber-incidents in 2007, cyber security and the fight against cybercrime have been key priorities for Estonia. At the same time, special attention is paid to the protection of fundamental rights and freedoms and responsible Internet governance.

In recent years, Estonia has invested in the development of "e-Government" with a view to ensuring full transparency of the public administration. Public services are accessible to the general public online through a state portal, which acts as a one-stop-shop for the e-services offered by the various government institutions.

Estonia approved its Cyber Security Strategy 2014-2017 in 2014. The key fields on which the Cyber Security Strategy focuses are ensuring vital services, combating cybercrime more effectively and advancing national defence capabilities. Additional supporting activities to fulfil these objectives include: shaping the legal framework, promoting international cooperation and communication, raising awareness, and ensuring specialist education as well as the development of technical solutions.

There is a robust legal framework in place in Estonia, with substantive criminal law covering the full range of offences related to cybercrime, including the illegal use of another person's identity which is also provided for in the Penal Code. The Penal Code is kept under review and amended as new trends emerge. Estonia has implemented the Freezing Order Framework Decision, the Framework Decision on attacks against information systems and the Confiscation Order and the Directive on combating sexual abuse and sexual exploitation of children and child pornography and expects to ratify the Lanzarote Convention in 2018. Estonia is party to the Budapest Convention, and other relevant Council of Europe Conventions, UN Conventions, EU instruments on MLA.

From a practical point of view, fulfilment of the Cybersecurity Strategy is carried out by different stakeholders, including law enforcement agencies, Ministries of Economic Affairs and Communications, Justice and the Interior as well as other bodies such as the Information System Authority and Information Technology Foundation for Education. Its objectives are also progressed via public-private partnership.

The Estonian Police and Border Guard Board has substantial powers and investigative techniques at its disposal to investigate cyber offences and deal with e-evidence and encryption. E-evidence is treated as ordinary evidence, however, no special rules in place to determine the handling and presentation of such evidence in criminal proceedings.

Private sector enterprises providing critical services are obliged to report cyber attacks and security incidents to the Estonian authorities. On the prevention of child sexual exploitation, Estonia is currently considering the blocking of access to websites containing child pornography although images can already be removed by court order.

Estonia engages with Europol and Eurojust and makes good use of JITs and makes significant efforts to facilitate links with other international partners such as the USA.

Part of the Strategy's objectives is to upskill law enforcement agencies and in this respect different training sessions are provided by CEPOL, the Tallinn University of Technology, CERT, OLAF and the Estonian Forensic Science institute (EFSI). Training for prosecutors on the detection of securing of e-evidence is provided in cooperation with the Police and Border Guard Board, the Supreme Court and the Tallinn University of Technology.

In addition, Estonia, provides awareness-raising and prevention programmes to inform the public and industry about the risks of cybercrime and encourage the safe use of the internet. The evaluators consider that Estonia's use of web constables on the internet is an innovative and useful tool to provide assistance to internet users and act as contact of confidence for both children and adults in the virtual environment.

On the whole, the evaluators could conclude that Estonia is committed to tackling cybercrime and has taken a series of measures to meet this objective. The team was very impressed by the number of key initiatives in place and considers that many of those could serve as models of good practice and could be used by other Member States to bolster their own efforts to tackle cybercrime. In particular, the use of web constables, the use of digital signatures on online transactions and the impressive public-private partnership are worthy of mention.

The team did, however, identify some areas which need further improvement and has made some recommendations to Estonia in this regard (See Chapter 9). The team invites Estonia to implement these recommendations in order to further enhance its efforts to fight against cybercrime

2. INTRODUCTION

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

The choice of cybercrime as the subject for the seventh Mutual Evaluation round was welcomed by Member States. However, due to the broad range of offences which are covered by the term cybercrime, it was agreed that the evaluation would focus on those offences which Member States felt warranted particular attention. To this end, the evaluation covers three specific areas: cyber attacks, child sexual abuse/pornography online and online card fraud and seeks to 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[2] (transposition date 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

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

Moreover, the Council Conclusions on the EU Cybersecurity Strategy of June 2013[1] reiterate the objective of ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[2] of 23 November 2001 as soon as possible and emphasise in their preamble that "the EU does not call for the creation of new international legal instruments for cyber issues". This Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems[3].

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

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

1 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.

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

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

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

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

The experts charged with undertaking the evaluation of Estonia were Mr Tero Toivonen (Finland), Mr Rimvydas Valentukevicius (Lithuania) and Mr José Manuel Sanchez Siscart (Spain). Three observers were also present: Ms Daniela Buruiana (Eurojust), Mr Michele Socco (European Commission) and Mr Philipp Amann (Europol/EC3), together with Ms Nicola Murphy and Ms Monika Kopcheva from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Estonia between 16 and 19 March 2015, and on Estonia's detailed replies to the evaluation questionnaire together with their detailed answers to ensuing follow-up questions.

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

In 2014, the Estonian Government approved the Cyber Security Strategy 2014-2017[1], which serves as the basis for planning Estonia's cyber security and forms part of Estonia's broader Security Strategy. The Strategy assesses threats to Estonia's cyber security, highlights important recent developments to combat cybercrime and presents ideas on how to manage threats effectively.

The key areas on which the Cyber Security Strategy focuses are ensuring critical services, combating cybercrime more effectively and advancing national defence capabilities. The fight against cybercrime focuses on the prevention, detection and the prosecution of cybercrime offences. Measures to be taken include increasing capacity to tackle cybercrime, promoting international cooperation, as well as raising public awareness of cyber-related risks.

The Cyber Security Strategy is closely linked with other strategy documents, such as the 'Digital Agenda 2020 for Estonia' and the 'Guidelines for Development of Criminal Policy until 2018'. In addition, the Strategy is indirectly linked with other strategic papers including the Internal Security Development Plan 2015-2020; Fundamentals of Counter-Terrorism in Estonia (2013); Development Plan for Reducing Violence 2010-2014; Development Plan for Reducing Violence for 2015-2020; National Defence Development Plan 2013-2022 etc.

[1] The English translation of the Cyber Security Strategy 2014-2017 can be found at: https://www.mkm.ee/en/node/2722#cybersecstrat

The Ministry of Economic Affairs and Communications coordinates the implementation of the Cyber Security Strategy through the Cyber Security Council formed under the Government Security Committee. More specifically, policies on combating cybercrime and prevention fall under the responsibility of the Ministries of Justice and the Interior. Cybercrime acts are investigated by the Police and Border Guard Board, the Internal Security Service and the Office of the Prosecutor General. In the field of prevention, the Police and Border Guard Board, the Information System Authority and the Information Technology Foundation for Education also play a key role.

3.2. National priorities with regard to cybercrime

The Cyber Security Strategy sets out three priority sub-goals for enhancing the fight against cybercrime:

1. Enhancing detection of cybercrime

- In order to improve the efficiency of the detection and prosecution of cybercrime, law enforcement capacity will be improved by:

  - clarifying the organisation of work;
  - increasing the number of personnel dealing with cybercrime; and
  - enhancing the capabilities of bodies conducting proceedings relating to digital data carriers.

- In order to develop capabilities, LEAs will cooperate with universities and international centres of excellence.

2. Raising public awareness of cyber risks

- In order to raise public awareness, attention will be given to introducing actions to prevent cyber threats and to provide the knowledge required to identify and respond wisely to incidents. Users of e-services will be directed towards the most secure solutions and will be informed about new technologies and how to use those solutions securely.

3. Promoting international cooperation against cybercrime

- In order to achieve more effective and timely prosecution of cybercrime acts with an international dimension, the exchange of information between Estonia and other countries should be improved. There will be active participation in various initiatives and projects that are part of the international fight against cybercrime.

In addition, the 'Guidelines for Development of Criminal Policy until 2018' emphasise the need to cooperate with the private sector and focus on vulnerable target groups, such as minors or elderly people in order to raise their awareness of the risks associated with use of the internet. More specifically, these guidelines aim to co-ordinate actions taken by state agencies to:

- combat sexual abuse of minors;
- prevent major computer fraud;
- prevent the spreading of computer viruses and hacking;
- raise awareness of vulnerable target groups (minors, elderly people) in cooperation with the private sector;
- ensure a sufficient number of IT specialists in law enforcement agencies.

3.3. Statistics on cybercrime

3.3.1 Main trends leading to cybercrime

As in the rest of the world, the number of criminal offences committed in Estonia with the aid of ICT tools is growing year on year. There has been an increase in both computer-related fraud and crime related to the use of another person's identity on the internet.

The Estonian authorities report that Cybercrime constitutes approximately 2% of all registered crime.

In Estonia, a cybercrime is defined as one which was enabled through the operation of digital devices. The overall statistics on cybercrime are affected by factors such as the distinction between acts classified as criminal offences and as misdemeanours. In computer-related fraud, for instance, the crime statistics are influenced by a recent amendment to the Penal Code which the distinction between a criminal offence and a misdemeanour is whether the damage is above or below EUR 200 as opposed to the previous threshold of EUR 64.

3.3.2 Number of registered cases of cyber criminality

Crime statistics are collected, processed and published by the Ministry of Justice. The sources of cybercrime statistics are the same as for other types of crime. Similarly as with other types of crime, the basis for gathering statistics is through the proceedings information system 'E-toimik' (E-file), which contains information from the police, the Prosecutor's Office and the courts. It is an integrated system that provides consolidated data on all civil, administrative, criminal and misdemeanour proceedings. The contribution of the private sector to crime statistics is indirect and depends on their readiness to report crime. Separate statistics on their activities are also collected by several non-profit organisations, such as the child helpline service ('Lasteabi') and the 'Vihjeliin', a free online service for reporting illegal content (http://vihjeliin.targaltinternetis.ee/en/), created within the framework of a project on wiser internet use ('Targalt Internetis').

Crime statistics for years 2012, 2013 and 2014 are as follows:

Registered criminal offences

Penal Code	Description	2012	2013	2014
§ 157²	Illegal use of another person's identity	62	91	112
§ 175¹	Requesting access to child pornography and watching thereof	0	0	1
§ 177	Use of minors in manufacture of pornographic works	9	0	0
§ 177¹	Use of minors in manufacture of erotic works	0	0	0
§ 178	Manufacture of works involving child pornography or making child pornography available	65	70	68
§ 178¹	Agreement of sexual purpose for meeting with child	9	4	7
§ 179	Sexual enticement of children	63	49	49
§ 206	Interference with computer data	14	12	7
§ 206[1]	Unlawful removal and alteration of means of identification of terminal equipment	2	0	1
§ 207	Hindering of functioning of computer systems	1	6	9
§ 208	Dissemination of spyware, malware or computer viruses	1	0	3
§ 213	Computer-related fraud	456	470	486
§ 216¹	Preparation of computer-related crime	3	13	37
§ 217	Unlawful use of computer system	34	31	22
§ 217[1]	Use of terminal equipment with unlawfully removed or altered means of identification	0	1	3
§ 284	Handing over protection codes	0	0	0

Number of convicted persons

Penal Code	Description	2012	2013	2014
§ 157²	Illegal use of another person's identity	0	9	26
§ 175¹	Requesting access to child pornography and watching thereof	0	0	1
§ 177	Use of minors in manufacture of pornographic works	0	1	0
§ 177¹	Use of minors in manufacture of erotic works	0	0	0
§ 178	Manufacture of works involving child pornography or making child pornography available	29	36	38
§ 178¹	Agreement of sexual purpose for meeting with child	0	5	4
§ 179	Sexual enticement of children	21	19	12
§ 206	Interference with computer data	2	0	0
§ 206¹	Unlawful removal and alteration of means of identification of terminal equipment	0	0	0
§ 207	Hindering of functioning of computer systems	0	0	1
§ 208	Dissemination of spyware, malware or computer viruses	0	0	0
§ 213	Computer-related fraud	160	133	131
§ 216¹	Preparation of computer-related crime	0	0	15
§ 217	Unlawful use of computer system	2	3	2
§ 217¹	Use of terminal equipment with unlawfully removed or altered means of identification	0	0	0
§ 284	Handing over protection codes	0	0	0

It should be pointed out that several systemic amendments have been introduced in the penal law in the recent years, whereby the necessary elements of a criminal offence have been specified and harmonised. Therefore, §§ 177 and 177[1] of the Penal Code were repealed in 2012 and § 208 was repealed on 1 January 2015, and the activities described therein were criminalised as other abovementioned computer-related crime. § 217 was amended on 1 January 2015 and today it provides for responsibility for the illegal obtaining of access to computer systems. In addition, § 222[1], after entry into force on 1 January 2015, provides for accountability for the infringement of copyright in a computer system. Pursuant to § 315 of the Penal Code, unlawful surveillance activities and covert collection of information (including with the help of computer systems) are also criminalised.

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

The vast majority of the measures taken to prevent and fight against cybercrime is financed through normal budgets of governmental ministries. A more detailed breakdown of budget funds for different national authorities and activities has been presented in the operational programme of the Cyber Security Strategy 2014-2017. The Strategy estimates that almost €16 million will be required over its lifetime to implement the measures contained therein.

Special appropriations have been made for individual prevention projects. For example;

- In 2013 a project was launched as a collaboration between the public and private sector in order to improve the skills and security awareness of smart device users, developers and sellers.
- Systematic funding has been provided for the activities of the Information Technology Foundation for Education (HITSA), which is active, *inter alia*, in raising awareness on internet safety. In addition, the state has funded the launching of various study programmes.

- In 2009, an international Master's programme on Cyber Security accepting 50 students annually was launched in collaboration between the Tallinn University of Technology (hereinafter referred to as 'TUT') and the University of Tartu. A 2CENTRE centre of excellence has been opened and a Master's programme was launched in cooperation with the TUT in 2014.
- The European Commission is financing the implementation of the project 'Estonian Safer Internet Centre: Targalt internetis (Smartly on the Web)', coordinated by the Estonian Union for Child Welfare. The project, aimed at promoting safe internet use, was initiated in 2011 and currently the partners are planning activities under a follow-up project for 2015-2016 (more information on the website of the project: http://www.targaltinternetis.ee/?lang=en).

3.5 Conclusions

It was obvious to the evaluators that Estonia takes cyber security seriously particularly in the aftermath of the 2007 cyber attacks which is further demonstrated by the adopted in 2014 National Cybersecurity Strategy which sets out priorities and the associated governance structure in place.

The team noted, however, that the Strategy does not clearly identify particular tasks or targets for stakeholders so each stakeholders' role is not clear. The team was advised that a separate action plan which sets out these roles exists, however it is confidential so the team was unable to assess its value. The team also noted that prosecution and judiciary were not included in the Strategy.

Similarly, although the team noted that the Strategy estimated that €16m would be required over the 4 year period to fulfil its objectives it was unable to see the specific allocation of funding under each heading due to the confidential nature of the action plan.

Estonia records and maintains up-to-date statistics on cybercrime and is therefore able to monitor any trends in this regard. This is commendable.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecution and courts)

4.1.1 Internal structure

According to Article 1 of the Prosecutor's Office Act the Prosecutor's Office is a government agency under the aegis of the Ministry of Justice which participates in the planning of surveillance necessary to detect and combat criminal offences, directs pre-trial criminal procedure and ensures the legality and efficiency thereof, represents public prosecution in court and performs other duties assigned to the Prosecutor's Office by law.

There is no specialised cybercrime court or prosecutor's office in Estonia. At the same time, certain prosecutors have been assigned to deal with cybercrime (a total of 16 - 17 prosecutors who simultaneously work with other types of crime). An information technology crime prosecution manual has been prepared to assist prosecutors when conducting cybercrime proceedings.

In accordance with Intend 1 of Article 213 of the Code of Criminal Procedure, prosecutors are competent to:

1) perform procedural acts, if necessary;

2) be present at the performance of procedural acts and intervene in the course thereof;

3) terminate criminal proceedings;

4) demand that the materials of a criminal file and other materials be submitted for examination and verification;

5) issue orders to investigative bodies;
6) annul and amend orders of investigative bodies;
7) remove an official of an investigative body from a criminal proceeding;
8) alter the investigative jurisdiction over a criminal matter;
9) declare a pre-trial proceeding completed;
10) demand that an official of an investigative body submit oral or written explanations concerning the circumstances relating to a proceeding;
11) assign the head of the probation supervision department with the duty to appoint a probation officer;
12) perform other duties arising from this Code in pre-trial proceedings.

4.1.2 Capacity and obstacles for successful prosecution

For Estonia, the main obstacle lies in obtaining the information necessary for the proceedings from other countries. A large amount of information and evidence needs to be gathered from abroad and very often there is no reply, or replies arrive with a considerable time delay.

4.2 Law enforcement authorities

The Police and Border Guard Board is the main law enforcement authority in the field of cybercrime. Some selected criminal offences are also dealt with by the Security Police Board. The Security Police Board is tasked with preventing and combating activities aimed at changing the constitutional order and territorial integrity of Estonia.

The Police and Border Guard Board has developed cybercrime investigation capacities in different prefectures as well as centrally in the Central Criminal Police. In the Central Criminal Police, cybercrime is dealt with by the Unit III under the Organised Crime Bureau. The service is responsible for the pre-trial procedure for cybercrime acts, and gathers and analyses intelligence on criminal offences under its procedural powers. In addition, the service supports other units in crime prevention, crime blocking and pre-trial procedure that require special knowledge in information technologies. The Central Criminal Police is also responsible for promoting international cooperation in the field of cybercrime.

Criminal intelligence services have been created in the prefectures (North, South, West and East prefectures), which are responsible, *inter alia*, for the prevention, blocking and pre-trial procedures for cybercrime as well as for internet monitoring analysis. Prefectures also include child protection services that investigate serious offences connected with the sexual abuse of children on the internet and child pornography. The e-evidence services located in the prefectures provide help and assistance in cyber forensics for all three other units.

The Offence Proceedings Bureau under the development department of the Police and Border Guard Board is responsible for capacity building in the light against cybercrime in general. For the most part, cybercrime prevention activities also fall under the responsibility of the Police and Border Guard Board, more specifically the Prevention and Supervision Bureau of the Development Department. The main spokespersons on internet security are the web constables (currently three) employed in the Information Analysis Service of the Information Management Bureau under the Information Management and Proceedings Department of the Police and Border Guard Board.

The web constables are authorised to communicate directly in various social media channels (e.g. Facebook, lapsemure.ee, perekool.ee, Vk.com, Rate.ee, Twitter, Odnoklassniki.ru, e-mail, soon narko.ee). They provide counselling, distribute information and forward alerts, as well as receiving information and tips. If needed, they forward information to a police station for information or processing (e.g. information about possible child abuse to the regional child protection services of the police, as web constables do not process offences), collaborate with networks of hotlines and helplines, monitor public internet content and assist colleagues in finding information from the virtual environment, taking and saving digital evidence as well as drawing up reports about accounts with inappropriate content in order to block and delete them.

4.3 Other authorities/institutions/Public Private Partnership

The Cyber Security Council (under the Government Security Committee) provides strategic support for inter-agency cooperation and supervises the implementation of the goals of the Cyber Security Strategy. There are several examples of good Public Private Partnership in this regard.

1. The Cyber Unit of the Estonian Defence League ('Cyber Defence League') was created in cooperation with the public, private and third sector. It assembles volunteers whose knowledge is implemented during exercises, testing solutions, training courses and through other forms of coordinated aid to improve cyber defence in both the private and public sector. The Cyber Unit of the Estonian Defence League is an important element in ensuring the State's cyber security and it collaborates with the agencies responsible for internal security as well as with the Information System Authority.

2. The Information System Authority supervises the information systems used for providing critical services and the continuous implementation of the security measures of related information assets; organises activities in connection with the information security of the state's information system and Estonian critical information infrastructure; handles security incidents in Estonian computer networks; and supervises implementation of the legislation regulating the management of the state's information system.

3. The cyber lab of the Estonian Defence Forces was created to support cyber defence training, run cyber exercises, and organise domestic exercises and study activities in higher education establishments.

4. The digital forensics and cyber security centre at the Tallinn University of Technology was established in autumn 2014.

The private sector is involved mostly in cases where security flaws of widely used and/or important systems occur. In such instances, the aim of the cooperation is to block and prevent attacks to the resources bearing the security flaw. The Estonian authorities also forward information to internet service providers and hosting service providers on malware-infected customers and break-ins to websites and encourages victims to turn to the police if damage has been caused in connection to a malware or a break-in to a website.

4.4.Cooperation and coordination at national level

4.4.1 Legal or policy obligations

In Estonia, private sector enterprises providing critical services are obliged to report cyber attacks and security incidents that have a significant impact. The obligation to notify is provided for in § 37 (3) of the Emergency Act which lays down that a provider of a critical service is obliged to immediately notify the authority organising the critical service or the authority appointed thereby of an event significantly disturbing the continuous operation of the critical service or of an impending risk of the occurrence of such an event.

§ 40 (2) of the Emergency Act is the legal basis for Regulation No 43 of the Government of the Republic: 'Security measures for critical service information systems and for related information assets', which imposes an obligation on a provider of a critical service to immediately notify the Information System Authority of important security incidents. Security incidents are notified by forwarding a report developed by the Information System Authority. Important security incidents are defined as events that entail a loss of availability, integrity or confidentiality of data or other information assets or a risk of their loss.

As a rule, banks report any suspicious transactions in their systems. There is also well-functioning cooperation between banks, the Financial Intelligence Unit and law enforcement authorities. Advanced security measures are used for the authorisation of internet transactions and a hardware-based security measure (ID card) is used in addition to passwords.

The Electronic Communications Act imposes legal obligations on communications providers concerning the methods and time limits for the retention of data. In addition to logs, private providers are obliged to provide data during a criminal procedure. Private providers are therefore obliged to provide information to investigative bodies. The Estonian authorities have enjoyed good cooperation with the private sector to date and no separate agreements have been required. As a rule, requests are answered within two weeks or faster if necessary. The provision of data is regulated by § 90 of the Code of Criminal Procedure.

4.4.2 Resources allocated to improve cooperation

The Estonian authorities are satisfied that they have the necessary IT infrastructure to respond to the cyber threat but are aware of the need to increase human resources and enhance training. In this regard, they are planning to build cybercrime prosecution capacities with the help of the European Union Internal Security Fund. Funding from the European Union Internal Security Fund has also been requested to build e- evidence processing capacities. In order to speed up and improve the processing of e-evidence in criminal matters, it is also considered necessary to purchase additional necessary software, ensure the certification of officials and, with the help of a shared network and server solution, ensure that information is exchanged between relevant authorities as efficiently as possible.

Regular activities have been performed under the guidance of the Information System Authority (both from the budget of the Information System Authority as well as through programmes with the help of Structural Funds) with the aim of raising awareness and improving know-how. The objective of these activities is to support the understanding and skilled management of technology-related risks as well as to support the principle of information society development to ensure the mitigation of unacceptable risks in information and communications systems, taking into account security requirements in designing the systems and throughout their entire life cycle.

4.5 Conclusions

- The team welcomed the fact that Estonia has several dedicated prosecutors who specialised in cybercrime, but noted that there is no specific role or training provided to judges and no specialised courts.

- Estonia like many other Member States expressed the challenges faced when obtaining evidence from foreign jurisdictions and particularly when getting information from the 'cloud'. It recommended that these difficulties be addressed at EU level.

- The Estonian authorities clearly enjoy good cooperation with industry. The team was advised that there is mandatory reporting for banks to the relevant authorities which works effectively. However, the team was not sure how good the cooperation between industry and prosecutors are during criminal investigations and how willing the private sector is to share information with prosecutors.

- The team was pleased to note that Estonia makes use of EU funding for the purposes of enhancing IT capabilities to tackle the phenomenon and supports its efforts in this regard.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on cybercrime

Estonia ratified the convention in 2003. It was also decided during the revision of the Penal Code (which entered into force on 1 January 2015) to specify the wording of the necessary elements of cybercrime acts contained in the Penal Code in order to improve legal clarity and simplify the prosecution of cybercrime acts.

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

Estonia has transposed into its national law Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

Criminal offences in connection with information systems are provided for in the Penal Code (e.g. §§ 206, 207, 208, 213).

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

The Directive has been transposed and the corresponding amendments have been made in the Penal Code.

C/ Online Card fraud

According to Estonia, generally smaller incidents of card fraud are left unreported, but more important and repeated incidents are reported. The reasons why incidents are not reported probably depend on the specific person and situation. It can be assumed that incidents are left unreported because participation in the proceedings is considered too burdensome.

Cooperation with banks is effective and magnetic stripe cards are no longer used. As a rule, banks report any suspicious transactions in their systems. There is also well-functioning cooperation between banks, the Financial Intelligence Unit and law enforcement authorities. Advanced security measures are used for the authorisation of internet transactions and a hardware-based security measure (ID card) is used in addition to passwords.

D/ Other Cybercrime phenomena

The Penal Code also provides for a serious or other offences related to data as set out below:

- Illegal use of another person's identity;
- Interference with computer data;
- Unlawful removal and alteration of means of identification of terminal equipment;
- Hindering of functioning of computer systems;
- Preparation of computer-related crime;
- Illegal obtaining of access to computer systems;
- Manufacture of works involving child pornography or making child pornography available;
- Agreement of sexual purpose for meeting with child.

The Penal Code also provides for offences in relation to negligence, aiding and abetting and also for liability of legal persons in relation to cybercrime offences.

5.2.1 Investigative Techniques

Search is provided for in § 91 (Search) of the Code of Criminal Procedure. § 86 (Inspection of document, other object or physical evidence) of the Code of Criminal Procedure may also be applied.

In the investigation of cybercrime, the first step is to identify the locations where the evidence is held in order to make urgent requests to acquire the log data or request its storage. International channels such as Europol and Interpol are used to compare similar cases in nearby countries. The aim is to establish any links between cases.

In Estonia it is also possible to use surveillance activities to investigate cybercrime. § 126^2 (2) of the Code of Criminal Procedure contains a list of Penal Code provisions which provide for surveillance activities to be conducted. In cybercrime investigation, for instance, surveillance activities may be used for the monitoring of computer traffic and the inspection of computers. The above investigative techniques are also used for the processing of other criminal offences.

According to Intend 1 of Article 91 of the CCP, a search can be carried out to locate any object which may be used as physical evidence in a building, room, vehicle or enclosed area.

A search is authorised at the request of a Prosecutor's Office on the basis of an order of an investigating judge or on the basis of a court ruling (Intend 2 Article 91 of the CCP).

As an exception, a search is authorised on the basis of an order of a Prosecutor's Office if there are reasons to believe, that the location was used to prepare or commit a criminal offence or the suspect used the location at the time of the commission of a criminal act or during the pre-trial proceedings (Intend 2 and 2-1 of Article 91 of the CCP). In urgent cases a search may be conducted on the basis of an order of an investigative body once post authorisation of the search by an investigating judge/the Prosecutor´s Office is granted within 24 hours of the search conducted (Intend 3 of Article 91 of the CCP).

Separate authorisation is required for entering the location against the will of the owner. (Article 91-1 of the CCP).

Guidelines on the use of these measures have been included in the IT crime prosecution manual. This document is designed for internal use in the Police and Border Guard Board. It aims to provide guidelines to police officers for the pre-trial procedure for computer related crime and criminal offences committed with the help of digital tools as well as for taking e-evidence. The manual contains a selection of frequently used IT terms together with information on existing case law and best practice models.

Physical evidence is immediately returned to the owner or former lawful possessor if this does not hamper the criminal procedure (Intend 3 of Article 124 of the CCP). If the evidence is retained, it is stored in a criminal file either using the storage facility of a body conducting the proceedings or in another premises in the possession of or territory guarded by the body or in a forensic institution (Intend 1 of Article 125 of CCP), or deposited into storage with liability on the basis of a contract. A person with whom physical evidence is deposited has responsibility to ensure the inviolability and preservation of the evidence (Intend 2 and 3 of Article 125 of CCP).

Traffic data

Based on authorisation from a Prosecutor's Office (in pre-trial procedure) or a court (in court proceedings) a body conducting proceedings may make enquiries to telecommunications service provider (TSP) about traffic data (Intend 2 of Article 90-1 of CCP).

Subscriber data

The body conducting the proceedings may make enquiries to TSP about subscriber data (Intend 1 of Article 90-1 of CCP). Enquiries regarding traffic/subscriber data may be made only if this is unavoidably necessary for the achievement of the objectives of criminal proceedings (Intend 3 of Article 90-1 of CCP).

Surveillance activities are permitted for a limited number of criminal activity (Intend 2 of Article 126-2 of CCP). Cybercrime acts are included in the list of offences for which surveillance activities may be conducted.

Surveillance activities are ultima ratio and permitted only if collection of data by other activities or taking of evidence by other procedural acts is impossible, is not feasible in the available time or is especially complicated or if they could damage the criminal proceedings (Intend 2 of Article 126-1 of CCP).

The gathering of information via surveillance activities is subjected to strict rules regarding it's requirements. In fact, such information can only be used as evidence if it was collected in absolute compliance with those requirements (Intend 4 of Article 126-1).

The surveillance activity is subject to written authorisation either by a Prosecutor´s Office or an investigating judge depending on the case (Intend 1 of Article 126-4 of CCP). In urgent cases surveillance activities requiring written authorisation of a Prosecutor's Office may be conducted with verbal authorisation which should be reproduced in writing and formalised as a written authorization within 24 hours (Intend 2 of Article 126-4 of CCP). Surveillance activities requiring written authorisation of an investigating judge may only be conducted with verbal authorisation which can be reproduced in writing, if there is immediate danger to the life, physical integrity or physical freedom of a person or to proprietary benefits of high value and requesting a permission or execution thereof on time is impossible. Again, the written authorisation must be formalised within 24 hours (Intend 3 of Article 126-4 of CCP).

If covert entry into a building, premises, vehicle, enclosed area or computer system is necessary to conduct surveillance activities or in order to install or remove technical appliances necessary for surveillance, the Prosecutor's Office shall apply for a separate permission of an investigating judge for such purpose (Intend 5 of Article 126-4 of CCP).

Real-time collection of traffic data:

Covert surveillance of persons, things or areas, covert collection of comparative samples and conduct of initial examinations and covert examination or replacement of things may be authorised by the Prosecutor's Office for up to two months (extendable two months at a time).

Real-time interception/collection of content data:

Recording of information obtained by wire-tapping or covert observation of messages or other information transmitted by the public electronic communications network or communicated by any other means can be authorised by an investigating judge for up to two months (extendable two months at a time).

Qualified persons/specialists and experts from a forensic institution, as appropriate, are involved in evidence taking. In performing their tasks, experts follow the rules provided for by the forensic institution and all the work methods are accredited. After the confiscation of a device or data medium the data medium is handed over for inspection to the IT crime specialists in the prefecture or the proceedings bureau of the Police and Border Guard Board or sent to IT expert assessment unit in the Estonian Forensic Science Institute.

5.2.2 Forensic and Encryption

The Estonian Forensic Science Institute (EFSI) does not currently perform electronic or remote forensic examination. In future, once a central server (an AccessData device) is installed it is planned to provide the IT investigators of the Police and Border Guard Board access via weblink to e-evidence saved in the central server (original copies of hard disks).

The EFSI currently performs IT examinations. The aim of an IT examination is to examine various devices and data media that contain digital information. The main purpose is to find relevant information in connection with the criminal offence and submit it in an understandable form. The objects include any data media, electronic devices, computers or any other technical equipment. There are a total of five specialists performing information technology examination in the EFSI.

Estonia has found encryption quite problematic. The possibilities offered by hardware and software for managing encryption are very limited.

The EFSI has been developing the necessary IT expertise to improve this situation. Its experience thus far shows that the AccessData PRTK software has made it possible to unlock data in some individual cases. In most cases, however, it has not been possible to examine data within a reasonable period of time and the matter has been returned.

Practical cooperation is established between investigative bodies in daily criminal proceedings. Objects containing encrypted data are sent by the Police and Border Guard Board to the EFSI to be processed. The Internal Security Service independently performs any operations with regard to encryption for criminal offences that fall within its investigative jurisdiction.

The standard requirements for devices and software acquired for forensic institutions are currently being specified by the Estonian authorities. An assessment of the requirements is currently being undertaken by the IT and development centre (SMIT) of the Ministry of the Interior and by the Centre of Registers and Information Systems (RIK).

5.2.3 E - e v i d e n c e

Until now, there has been no need to define the term e-evidence in Estonian legislation. The terms used in the Convention on Cybercrime of the Council of Europe and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA serve as a reference.

No separate rules have been established in Estonia for the admissibility of e-evidence. According to its legislation, the admissibility rules for e-evidence are the same as for other evidence. In addition, there are no specific provisions on gathering of e-evidence and general rules and principles on gathering of evidence are applied.

According to Intend 1 of Article 64 of the CCP evidence shall be taken in a manner which is not prejudicial to the honour and dignity of the persons participating in the taking of the evidence, does not endanger their life or health or cause unjustified proprietary damage. Evidence shall not be taken by torturing a person or using violence against him or her in any other manner or by means affecting a person's memory capacity or degrading his or her human dignity.

There are specific provisions on the usage of tools and expertise in the course of gathering of evidence.

- Intend 3 of Article 64 of the CCP foresees usage of technical equipment in the course of gathering of evidence.

- Intend 3 of Article 83 of the CCP foresees participation of a qualified person in procedural act of inspection for the purposes of helping "to ensure the thoroughness, comprehensiveness and objectivity of the inspection".

- Intend 2 of Article 109-1 of the CCP foresees participation of a qualified person in all the other procedural acts. The statements made by the qualified person in connection with the detection and storage of evidence shall be recorded.

If evidence has been obtained from a foreign state, its use is allowed on condition that the evidence has been duly taken pursuant to the legislation in force in the foreign state and that the procedural acts performed in order to obtain the evidence are not in conflict with the principles of the Estonian criminal proceedings. As a rule, it is done through a request for legal assistance.

5.3 Protection of Human Rights/Fundamental Freedoms

Any limitation of fundamental rights takes place on the same grounds as in other types of crime. This limitation normally only arises when surveillance activities are used. § 126^2 (2) of the Code of Criminal Procedure contains a list of Penal Code provisions that enable surveillance activities to be conducted.

5.4 Jurisdiction

5.4.1 Principles applied to investigate cybercrime

§ 6 of the Penal Code provides a general rule that the penal law of Estonia applies to acts committed within the territory of Estonia.

At the same time, it is important to note that according to § 7 of the Penal Code, the penal law of Estonia also applies to an act committed outside the territory of Estonia if such an act constitutes a criminal offence pursuant to the penal law of Estonia and is punishable at the place of commission of the act, or if no penal power is applicable at the place of commission of the act and if:

1) the act is committed against a citizen of Estonia or a legal person registered in Estonia; or

2) the offender is a citizen of Estonia at the time of commission of the act or becomes a citizen of Estonia after the commission of the act, or if the offender is an alien who has been detained in Estonia and is not extradited.

The provisions of §§ 6, 8 and 11 of the Penal Code are also relevant:

- According to § 6 of the Penal Code, the penal law of Estonia applies to acts committed within the territory of Estonia.
- According to § 8 of the Penal Code, regardless of the law of the place of commission of an act, the penal law of Estonia applies to any acts committed outside the territory of Estonia if the punishability of the act arises from an international obligation binding on Estonia.
- According to § 11 of the Penal Code, an act is deemed to be committed at the place where:

1) the person acted;
2) the person was legally required to act;
3) the consequence which constitutes a necessary element of the offence occurred; or
4) according to the assumption of the person, the consequence which constitutes a necessary element of the offence should have occurred.

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

Estonia has had no such experience to date. The decision to bring together proceedings that are conducted in parallel in different Member States is made in cooperation with the authorities of the Member State concerned.

According to § 436[1] (Prohibition on parallel proceedings of criminal offences) of the CCP, which entered into force on 1 January 2015, the opening of criminal proceedings with respect to the same persons and the same circumstances relating to a criminal offence in several Member States of the European Union is to be avoided, and in the event of such parallel proceedings taking place, Member States must contact each other and decide on bringing the proceedings together.

Jurisdiction is usually agreed upon in the framework of joint investigation teams (JITs). Framework Decision 2009/948/JHA was transposed into Estonian law on 1 January 2015. To date, Estonia has no experience in applying that Framework Decision.

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

One of the main practical problems Estonia faces relates to obtaining data from the 'cloud', i.e. from data centres and servers located in other countries. There are two possibilities for obtaining data: either it is provided voluntarily by the suspect, or the location of the information has to be identified and a request for legal assistance submitted to the corresponding state. In doing this, identifying the physical location is one of the greatest challenges. As a solution to this problem, Estonia suggests that it would be useful to be able to make virtual searches in data centres located in other countries without having to first identify the physical location of the server. One possibility would be to impose certain cooperation rules on data operators who would, under certain circumstances, give the law enforcement authorities the passwords necessary for accessing data, thus making it possible to copy the data without identifying the physical location.

5.4.4 Perception of Estonia with regard to legal framework to combat cybercrime

In Estonia's view the existing legal framework is not sufficient for the investigation and prosecution of cybercrime acts committed outside its territory. A large amount of information and evidence needs to be gathered from abroad and very often there is no reply, or replies arrive with a considerable time lag. Cybercrime-related evidence is located in numerous countries across the world where different rules apply, and submitting requests for legal assistance is a complex and time-consuming process. Since log files are preserved for a short time, they are often deleted by the time a request for legal assistance is received. It can be said, based on the practice of solving incidents and gathering technological information, that incidents in cyberspace tend to have a cross-border element and can simultaneously include different resources (DNS, IP space) on different countries and even different continents. The principal solution is to broaden standardisation and establish requirements at international level.

5.5 Conclusions

- The substantive criminal law is comprehensive and flexible. Estonia provides for a range of offences and covers legal liability aiding and abetting, negligence and legal liability. It also provides for an offence of the illegal use of identity.

- The situation differs slightly regarding procedural law especially in terms of gathering e-evidence spread around the world, data located in the cloud and difficulties finding the physical location of the data. Here the team noted that no special rules exist with regard to e-evidence.

- The Police and Border Guard Board has substantial powers of investigation and tools at its disposal. The team was satisfied that fundamental rights are respected in Estonia and appropriate judicial oversight is applied to any surveillance or special investigation technique.

- Forensic examinations are performed by the EFSI. Plans are underway to develop a central server to allow the EFSI to perform electronic or remote forensic examinations, however, in the meantime this is not possible. The team encourages Estonia to continue to work on this central server to increase Estonia's capability to gather evidence as efficiently as possible.

- The team noted the suggestions put forward by Estonia to access data held in the cloud such as providing the possibility to make virtual searches in data centres located in other countries without having to first identify the physical location of the server and/or to mandate the data service providers to provide passwords to LEAs to enable them to access the data.

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1 Nature of cyber attacks

The annual report of the Cyber Security Branch of the Estonian Information System Authority[1] provides details on the volume and nature of reported cyber attack incidents in Estonia.

Estonia reported several different types of cyber attacks including phishing campaigns, and a series of cyber attacks against school websites in 2013. For example, one case involved the phone system of an educational establishment which was hacked into and as a result hundreds of long distance calls were made. Also a new phenomenon has emerged in Estonia in recent years - a voice phishing wave. A person introducing himself as a representative of Microsoft encouraged non-suspecting computer users to download a program and/or disclose passwords that would enable the impostor to access the victim's computer and, through that, their bank account.

6.1.2 Mechanism to respond to cyber attacks

In Estonia, the Emergency Act has been in force since 2009. It regulates, *inter alia*, arrangements for preparing emergency response plans to cyber attacks. Emergency response plans are prepared on the basis of Order No 208 of the Government of the Republic of 25 April 2013 (list of emergencies for which risk analysis and a response plan are prepared and the appointment of the competent authorities of the executive power to prepare the emergency risk assessment and emergency response plan).

[1] (https://www.ria.ee/2013-annual-report-cyber-security-branch / https://www.ria.ee/ria-kuberturbe-kokkuvote-2013)

All the emergency response plans prepared and in force in Estonia have been prepared on the basis of the inter-agency and situation-based principle. This means that the focus is on the emergency that needs to be resolved, and the roles of different agencies in completing the corresponding tasks are set out accordingly.

Other existing regulations serve as a basis for setting out the role of each stakeholder. The plan currently in force is the 'Emergency response plan for a large scale cyber attack', established by Order No 372 the Government of the Republic of 25 August 2011. The plan sets out that the Information System Authority shall manage any cyber emergency and establishes the obligation for the victims of the cyber attack, the providers of critical services, the Ministry of the Interior, and, if applicable, the Prosecutor's Office, the Police and Border Guard Board, the Security Police Board and the Cyber Unit of the Estonian Defence League to participate as stakeholders in the emergency response.

The Information System Authority is the main agency in emergency response at national level and has to ensure the coordination of the emergency response. CERT-EE and GovCERT are also part of the Information System Authority. The other abovementioned agencies are involved in different tasks set out in the emergency response plan, based on the acts and statutes that regulate those agencies. The activities of the involved agencies include, by way of example, gathering information on threats, blocking cyber attacks, information exchange and analysis, etc.

6.2 Actions against child pornography and sexual abuse online

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

In Estonia, there is no special national database to identify victims. However, data is entered in the International Child Sexual Exploitation (ICSE) Interpol. Plans are underway to develop a similar national database in the future.

Images of child pornography and other media are usually destroyed by court judgment. In the event where, in procedural acts under criminal proceedings, data media containing files which depict sexual abuse of children are found and confiscated from a person, the court in its judgment prescribes how to treat the data. The usual practice is to destroy the data media or to delete files in their entirety from the data media.

In Estonia, there is no national hash-database of images and videos depicting sexual abuse of children, which would make it possible, through the comparison of hashes, to identify and categorise the material depicting sexual abuse of children on data media more rapidly and with less emotional damage to the persons conducting proceedings (because of repeated observation).

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

In procedural practice, each case is dealt with separately and through the necessary procedural possibilities.

If the necessary elements of a criminal offence are identified, it will be followed by criminal proceedings led by the Prosecutor's Office. Prevention activities are also used – youth police officers give prevention lectures in schools. In addition, articles are regularly published in the press.

The blocking of access to websites containing child pornography is currently being discussed in Estonia with the aim of ensuring the implementation of requirements contained in Article 25 of the Directive on combating the sexual abuse and sexual exploitation of children and child pornography (Directive 2011/93/EU).

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

The information on abusers communicated through Interpol and Europol channels is systematically compared with national databases and contributions are made to international operations.

In 2014, the Police and Border Guard Board participated in Europol's RAVEN/HAVEN operation. One of the aims of the operation was to map potential sex tourists in all Member States.

Data on potential sex tourists who have been convicted of sexual crimes against children and are believed to travel between different countries are entered in Europol's Information System (EIS) database.

Advertising child pornography is prohibited and punishable as an offence. Victims are offered help and support before, during and after criminal proceedings (victim support). Estonia plans to transpose the Victims Rights Directive[1] later this year. The Penal Code contains several provisions on trafficking in human beings (§ 133 to § 133^3; buying sex from minors – § 145^1 ; human trafficking in order to take advantage of minors – § 175).

Estonia has also signed the Lanzarote Convention ('Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse). It expects to ratify the Convention in 2018.

[1] Ref to Victims Directive

Estonia has made it possible to make reports online through a hotline; more details are available on the website vihjeliin.ee. Information is also provided in the framework of the activities of the Estonian Union for Child Welfare and its cooperation partners as well as web constables. The hotline is part of a project on wiser internet use ('Targalt Internetis').

The hotline www.vihjeliin.ee enables internet users to report websites which contain material in breach of children's sexual self-determination. The hotline may be used also to report other material on the internet that is inappropriate for children.

For the safe use of the internet, children and parents are offered advice and information by the child helpline telephone 116111 (www.lasteabi.ee) as well as on email (contact address: info@lasteabi.ee) and by chat tools (activities under the project on wiser internet use ('Targalt Internetis')). The authorities also work in cooperation with various interest groups in Estonia and Europe. Estonia also participates in the INHOPE and INSAFE cooperation networks.

The web constables of the Police and Border Guard Board are easily reachable confidants for both children and adults in the virtual environment. Information about them is available on the website of the Police and Border Guard Board, in the social media as well as on the websites of partners. Web constables provide assistance in Estonian, Russian and English.

'Targalt Internetis' was launched with funding provided by the European Commission. It includes training sessions and seminars on the risk facing children on the internet for children, parents, teachers and social workers as well as awareness raising events for the general public. Training and information material is provided to children, teachers and parents, and creative competitions are organised for pupils to encourage them to explore the topic further.

6.2.4 Actors and measures counterfeiting websites containing or disseminating child pornography

Estonia does not have specialised units dealing exclusively with child pornography. Prefectures include child protection services that investigate serious offences connected with the sexual abuse of children on the internet and child pornography.

Orders to close websites and remove any information contained therein can be issued by the Technical Surveillance Authority, the Tax and Customs Board, the Police and Border Guard Board and the Data Protection Inspectorate. The service provider is responsible for the ICT service provided.

6.3 Online card fraud

6.3.l Online reporting

As a rule, smaller incidents are left unreported, but more important and repeated incidents are reported. The reasons why incidents are not reported probably depend on the specific person and situation. It can be assumed that incidents are left unreported because participation in the proceedings is considered troublesome.

6.3.2 Role of private sector

The cooperation between the banking sector and authorities is effective and magnetic stripe cards are no longer used. As a rule, banks report any suspicious transactions in their systems. There is also well-functioning cooperation between banks, the Financial Intelligence Unit and law enforcement authorities. Advanced security measures are used for the authorisation of internet transactions and a hardware-based security measure (ID card) is used in addition to passwords.

6.4 Conclusions

Estonia has developed clear mechanisms to report and respond to cyber attacks through legislation and the creation of specialised agencies to deal with any reported threat or attack. The team noted that CERT-EE and GovCERT were well integrated into the Information System Authority.

Estonia enters images of victims into the ICSE at Interpol, but no national database presently exists. The team was advised that plans are underway to establish a national database, but it is at an early stage of development.

Estonia has actively engaged with Europol's Raven/Haven operation and enters information on potential sex tourists on the EIS database although the team noted that there is no national database of known sex tourists.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

The contribution of the agencies has been positive and it has been substantial notably from the point of view of information exchange. Both Eurojust and Europol have provided help in conducting proceedings relating to different cybercrime acts. Support for the work of the JITs and the SIENA information exchange channel are important for Estonia. It also provides adequate training.

Cooperation to create joint investigation teams (JITs) is regulated by the Code of Criminal Procedure. Estonia has also transposed the Framework Decision on Joint Investigation Teams (JITs) 2002.

Estonia is also considering seconding an officer to the J-CAT at Europol.

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

Cooperation has taken place in the framework of concrete criminal proceedings. Information is exchanged with Europol through the corresponding channels (SIENA). Joint coordination meetings as well as the work of JITs have been organised in cooperation with Eurojust.

In Estonia's view it would be useful if the EU agencies built analytical capacities and paid more attention to regional difficulties. The creation of country-based desk officer positions in the corresponding agencies could also be considered, in order to ensure smooth communication and better analytical awareness of the specificities of each Member State.

In addition, Estonia would welcome efforts by the cybercrime centre EC3 of Europol to establish uniform operational standards for first-line officers, surveillance officers and investigators of cyberspace activities. In that respect, the European Committee for Standardisation (CEN) could provide help.

7.1.3. Operational performance of JITs and cyber patrols

Estonia has participated in JITs and the experience thus far has been positive. It considers JITs a useful instrument for conducting cross-border investigations. Another positive aspect is that it enables cross-usage of evidence in both proceedings without having to submit separate requests for legal assistance. Information is exchanged directly between investigators, thus ensuring operational effectiveness.

Estonia participates in a few JITs per year, whenever cross-border cases occur. For example, in 2010, Estonia formed a joint investigation team with the UK to process criminal offences in connection with dissemination of spyware, acquisition of bank account details and making fraudulent transfers. The experience was positive as it made it possible to perform the necessary actions effectively and to hand over evidence. The criminal matter was taken to court in the UK.

7.2 Cooperation between the Estonian authorities and Interpol

Estonia joined the International Child Sexual Exploitation (ICSE) database at Interpol in 2011 and it plans to develop a similar national database in the coming years.

Cooperation takes place mostly through the use of the Interpol cooperation channel for exchanging information. For Estonia, this is one of the most important cooperation channels. Other cooperation in the framework of Interpol takes place, in particular, in the form of training sessions, meetings and conferences. There is not much direct contact with the cyber centre of Interpol as it is located in Singapore.

7.3 Cooperation with third states

Estonia enjoys relatively good cooperation with third countries to ensure MLA works well. For example, cooperation with the USA is with the help of the FBI liaison officer based in Estonia and communication with other third countries is facilitated by Interpol.

Thus far, the help of Eurojust has not been used in communication with third countries. The help of Europol has been used once in operation Blackshades to communicate with the FBI in the USA. In that particular case the information exchange brought no added value, since representatives of the FBI are present in Estonia and cooperate closely with the Police and Border Guard Board in any event. At the same time, such information exchange could be useful in communicating with Russia and some other third countries.

7.4 Cooperation with private sector

The liability of internet service providers is provided for in the Electronic Communications Act. In situations where files with forbidden contents are found on an Estonian server, their removal has thus far taken place in close cooperation with the owner of the server. This means that the owner is contacted, the situation is explained to them and they are asked to block access. Until now, there have been no refusals and cooperation has always been successful.

Should a situation arise where the owner of the server does not cooperate, § 178 of the Penal Code allows such a situation to be interpreted as making child pornography available in any other manner, and, taking account of prior notification, this also comprises intent within the meaning of § 16 of the Penal Code.

An internet service provider is obliged to log and preserve the logs of IP addresses for one year.

Besides the Electronic Communications Act, several obligations are also provided for by Regulation No 140 of the Government of the Republic of 22 June 2006 ('Requirements for the provision of communications services and technical requirements for the communications networks'), established on the basis of § 87 (2) of the Electronic Communications Act. Pursuant to the Electronic Communications Act, an internet service provider is required to take appropriate technical and organisational measures to manage the risks related to security and integrity of the communication services and network. An internet service provider is also required to notify the Information System Authority immediately of all incidents endangering the ensuring of security and integrity of the communications network and services.

In the event of a fault in the data communication network, an internet service provider has to eliminate it within a reasonable period of time after becoming aware of the fault. According to the Regulation, an internet service provider must plan, design, build, maintain and use a communications network intended for the provision of communications services in such a way that: 1) the possibilities of unauthorised persons for accessing a communications network and the information transferred and preserved therein are limited; 2) the communications service is minimally disturbed in the occurrence of power cuts, communications network faults, software viruses and other factors disturbing the communications network and communications service; 3) a communications undertaking has to choose such methods and scope for maintenance works and to ensure the fulfilment of quality requirements set for communications services as mentioned in the communications service agreement.

The Electronic Communications Act also provides for liability for violation of requirements established for quality of communications services and for violation of requirements established for security and integrity of communications networks and services. In addition, liability is foreseen for unlawful restriction by the service provider of the internet service for the end-user, etc.

Microsoft has a local base in Estonia and active cooperation takes place with the authorities. The procedure for forwarding enquiries to the parent company of Microsoft by the Estonian bodies conducting proceedings has been agreed. To date, replies to the enquiries have been very effective and no failures have occurred.

7.5 Tools of international cooperation

7.5.1 Mutual Legal Assistance

According to the Ratification Act on the Convention on Cybercrime, the Ministry of Justice is the central authority within the meaning of Article 27 of the Convention; the Central Criminal Police is the point of contact within the meaning of Article 35(1) of the Convention. Pursuant to other conventions, the Ministry of Justice is the central authority; only the MLA 2000 convention allows requests for legal assistance to be forwarded directly to the executing authority. In the case of bilateral or multilateral agreements, the appointment of the central authority depends on the countries involved.

The admissibility and feasibility of all the legal assistance requests received are verified by the Office of the Prosecutor General. Requests to foreign countries are submitted through the Office of the Prosecutor General.

Thus the Prosecutor's Office and courts are authorised to submit requests for legal assistance within the limits of their competences, while judicial authorities or law enforcement authorities designated by them are authorised to execute the requests (in the latter case, the Prosecutor's Office delegates the execution of a request for legal assistance to the Police or the Tax and Customs Board). Requests for legal assistance are sent to or from Estonia through the central authority – the Ministry of Justice.

For the communication channel, Estonia allows the use of any means of transfer enabling written recording – post, fax, e-mail. Estonia accepts the same channels for incoming requests. Additional information is usually requested by e-mail, sometimes by fax. If needed, the party submitting the request is contacted by telephone.

Number of requests received from abroad	
2010	685
2011	707
2012	679
2013	719
Number of requests sent by Estonia to foreign countries	
2010	260
2011	305
2012	332
2013	275

The Council of Europe conventions on cooperation in the field of criminal law and European Union instruments on mutual recognition are applicable to the provision of legal assistance. Chapter 19 of the Code of Criminal Procedure (international cooperation) allows requests for legal assistance to be executed or sent virtually without restrictions (with the exception of general grounds for refusing international cooperation). Estonia has no separate provisions that regulate international cooperation specifically on cybercrime.

In cases involving third countries, Estonia uses legal assistance agreements and other international agreements where available. The Information System Authority identifies, monitors and solves security incidents in Estonian computer networks and provides information about threats.

A criminal offence must correspond to the necessary elements of a criminal offence as set out in the Penal Code. Urgent requests are accepted by e-mail or fax; whenever possible, requests are treated without delay. There are no separate statistics for cybercrime; also, average response times for legal assistance requests on cybercrime are not calculated. In 2013, the average time for executing a request for legal assistance was 42 days in Estonia (32 days when executing requests from the Republic of Finland). Estonia makes good use of the EJN to find the necessary contacts in other States.

7.5.2 Mutual recognition instruments

Two decisions to freeze property or evidence in connection with computer-related fraud were received from Croatia. In both cases, it was not possible to implement the seizure, as the accounts were empty and were later closed by the bank.
No other measures have been implemented or requested from other countries by Estonia.

The protection order, the framework decision on the exchange of prisoners and the mutual recognition of confiscation orders only entered into force on 1 January 2015. So Estonia has no experience in using these measures to date.

7.5.3 Surrender/Extradition

Surrender is regulated by § 491 of the Code of Criminal Procedure;

Code of Criminal Procedure § 491. General conditions for surrender

(1) A person may be surrendered for continuation of criminal proceedings with regard to him or her in a requesting state if the person is suspected or accused of a criminal offence which is punishable by at least one year of imprisonment in the requesting state.

(2) A person shall be surrendered regardless of the punishment for the act pursuant to the Estonian Penal Code if imprisonment of at least three years is prescribed as maximum punishment in the requesting state for commission of the following criminal offences:

1) participation in a criminal organisation;

2) terrorism;

3) trafficking in human beings;

4) sexual exploitation of children and child pornography;

5) illicit trafficking in narcotic drugs and psychotropic substances;

6) illicit trafficking in weapons, ammunition and explosives;

7) corruption;

8) fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests;

9) money laundering;

10) counterfeiting money

11) computer-related crime,

12) environmental crime, including illicit trafficking in endangered animal species and endangered plant species and varieties;

13) facilitation of unauthorised entry and residence;

14) manslaughter, causing serious damage to health;

15) illicit trade in human organs and tissue;

16) kidnapping, unlawful deprivation of liberty and hostage taking;

17) racism and xenophobia;

18) organised or armed robbery;

19) illicit trafficking in cultural goods, including antiques and works of art;

20) swindling;

21) extortion;

22) piracy and counterfeiting of products and trafficking therein;

23) forgery of administrative documents and trafficking therein;

24) counterfeiting and forgery of means of payment;

25) illicit trafficking in hormonal substances and other growth promoters;

26) illicit trafficking in nuclear or radioactive materials;

27) trafficking in stolen vehicles;

28) rape;

29) arson;

30) criminal offences which fall within the jurisdiction of the International Criminal Court;

31) unlawful seizure of aircraft or ships;

32) sabotage.

(3) Surrender of a person for the purposes of execution of a judgment of conviction made with regard to him or her is permitted under the conditions provided for in subsections (1) and (2) of this section if at least four months of the sentence of imprisonment have not yet been served.

7.6 Conclusions

- Estonia makes good use of JITs given its size and has had effective results from this type of cooperation.

- Estonia also engages with Europol/EC3 although the team considers that it could make better use of Europol/EC3 particularly if it joined the J-CAT. The team could see benefits for Estonia in this regard.

- Estonian authorities enjoy good cooperation with the private sector at police level but not clear if judicial authorities including prosecutors enjoy the same level of engagement during the criminal investigation. It was considered that it would be useful if judges and prosecutors were included in meetings with the private sector to ensure that any future evidence to be provided was handled correctly and deemed admissible in Court.

Estonia enjoys good cooperation with the US as a FBI liaison officer has been posted there although formal requests for mutual legal assistance can still be limited due to conditions and restrictions imposed by the US. Estonia advised that cooperation with Russia could be improved and whilst noting that engagement must be mutual the team encourages Estonia to continue its efforts to enhance this cooperation. Cooperation with Russia could also be improved at EU level.

8. TRAINING, AWARENESS RAISING AND PREVENTION

8.1. Specific training

Different training sessions are provided by CEPOL, the Tallinn University of Technology, OLAF, and CERT. In addition, the Estonian Forensic Science Institute (EFSI) has organised some training sessions.

- In autumn 2014, a digital forensics and cyber security centre at the Tallinn University of Technology (TUT) was established on the initiative of the Ministry of Justice and the EFSI with the support of a 2CENTRE financing programme. Cooperation in the centre is based on the public-private partnership principle.

- In autumn 2014, a Master's programme on IT Law was launched in the Faculty of Law in the University of Tartu.

- In 2010, a cyber security and digital forensics study programme was launched in the Tallinn University of Technology (TUT). The aim of the study programme is to provide broad-based knowledge on the security of information systems and professional skills in the field of cyber security incidents and e-evidence. The studies provide a good basis for working in the field of cyber security, where success depends on cooperation between different specialists. As a rule, cyber security teaching staff have professional experience in the private or public sector, thus keeping the study programme up to date and responsive to actual needs.

Training sessions of the TUT between 2010 and 2014

Name of training	*Start date*	*End date*
Advanced Cyber Investigations Training	*20.5.2014*	*23.5.2014*
Child Abuse in Cyberspace	*30.9.2013*	*4.10.2013*
Combating Cybercrime in Europe	*8.2.2012*	*10.2.2012*
Cyber Conflict 2011	*7.6.2011*	*10.6.2011*
Cybercrime Forensics	*29.10.2012*	*31.10.2012*
Cybercrime Investigation Training	*9.9.2012*	*14.9.2012*
Cybercrime Network Conference	*8.12.2013*	*11.12.2013*
Cybercrime vs Cybersecurity	*26.10.2014*	*31.10.2014*
Cybercrime/ Child Abuse in Cyberspace	*4.11.2012*	*9.11.2012*
Elimination of Children Cybercrime	*11.10.2012*	*12.10.2012*
European Cooperation in Cybercrime Prevention	*17.3.2011*	*17.3.2011*
HighTech and Cybercrime	*17.10.2011*	*21.10.2011*
Investigating Cybercrime	*17.9.2012*	*21.9.2012*
Cyber Security	*2.9.2011*	*2.9.2011*
Seminar on ICT and Cybercrime	*12.12.2013*	*12.12.2013*
MS Capacities to Detect Cybercrime	*22.4.2013*	*26.4.2013*
Solution of electr. violence and cybercrime	*8.10.2014*	*14.10.2014*
Union capacities to investigate Cybercrime	*6.10.2014*	*10.10.2014*
New Trends in Cybercrime Investigation	*27.3.2014*	*27.3.2014*
Cybercrime and Digital Evidence	*27.5.2014*	*27.5.2014*

- Training for the Police and Border Guard Board in relation to cybercrime has been offered mostly by CEPOL and Europol; there have also been some internal training sessions. ECTEG has so far offered no training.

- Training for Prosecutors, organised by Police and Border Guard Board, Security Police Board, Supreme Court and Tallinn University of Technology, focuses on the detection and securing of digital evidence and is attended by numerous judges, prosecutors and law enforcement officials.

- In addition, Academy of European Law (ERA) cybercrime training courses were attended in total by 10 prosecutors.

- Prosecutors also attended Eurojust´s strategic meeting in 2014: Cybercrime – rising to the challenges of the 21st century and the International Cyber Security Congress (ICSS) in 2014 and 2015.

- Estonian practitioners attended the kick-off brainstorming session (under the initiative of the Dutch prosecution service) aimed at establishing a functioning EU Cybercrime Prosecutors / Practictioners Network at Eurojust.

The costs of cybercrime-related training have grown year by year. Between 2011 and 2014, approximately EUR 7,000 was spent annually for training in the field of cybercrime. In total, 86 persons have participated in training. The operational programme of the Cyber Security Strategy 2014-2017 provides for an increase in training costs.

Training is also provided to those dealing with internal cooperation which mostly takes place in the form of CEPOL and Europol training sessions. *Ad hoc* refresher training is also provided. The length of a training session is usually a few days. Training is attended when needed and possible.

Training is organised by the Information System Authority and the CERT. The aim of training is to support the understanding and skilled management of technology-related risks. The objective is to ensure the mitigation of unacceptable risks in information and communications systems, taking into account security requirements in designing the systems and throughout their entire life cycle.

8.2. Awareness raising and Prevention

Estonia has good experience in broad-based network activities for ensuring a safe internet, contributing to early reduction and prevention of child abuse including a project on wiser internet use ('Targalt Internetis').

The Police and Border Guard Board cooperates directly with non-profit organisations for awareness raising. For example, support is provided for the dissemination of campaign messages and conferences are organised ('Tunne oma netisõpru!' ('Know your web-friends!'), https://www.youtube.com/watch?v=6MFpx_E6BPQ 'Kaitske mind kõige eest!' ('Protect me against everything!'), etc.).

There is also cooperation in administering the online hotline vihjeliin.ee for reporting pages with illegal content, as well as in supporting the work of the child helpline 116111 and the missing children hotline 116000. Tips are exchanged and mutual counselling is provided on reacting to incidents.

The web constables of the Police and Border Guard Board have an important role in awareness-raising. They are the main spokespersons of the police in preventing threats on the internet. They provide counselling on identity theft, threatening and defamation, bullying, abuse and the activities of the police among others, and distribute information and forward alerts. It is possible to send information and tips to them.

Internet security is dealt with in the study programmes of universities. In addition, *ad hoc* lectures are given by representatives of various bodies responsible for cyber security.

RIA provides training using European Funds with the spend on awareness raising rising to more than €100k in total.

8.3 Public Private Partnership (PPP)

One of the examples of such a partnership is the digital forensics and cyber security centre at the Tallinn University of Technology, established in autumn 2014. Cooperation in the centre is based on the public-private partnership principle.

The private sector is involved mostly in cases where security flaws of widely used and/or important systems occur. In such instances, the aim of the cooperation is to block and prevent attacks to the resources bearing the security flaw. The Estonian authorities also forward information to internet service providers and hosting service providers on malware-infected customers and break-ins to websites and strongly recommends that victims to turn to the police if damage has been caused in connection with the activities of malware or a break-in to a website.

8.3. Conclusions

- It is clear that Estonia makes training available to practitioners and has a dedicated budget of €7k per annum devoted to cybercrime. The team noted, however, that this training does not appear to be systematic or regularly provided and could be considered somewhat *ad hoc* in nature.

- The team was pleased to note that Estonia avails of CEPOL and EC3 training but from speaking to practitioners it became apparent that many were not aware of training that is available and therefore this training is not used to its full potential.

- Estonia has invested in several notable awareness raising and preventative measures with a view to advising the public of the inherent risks of using the internet. This awareness raising, which targets particularly vulnerable groups, is well established and appears successful. The creation of web constables is a particularly innovative idea.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Estonia

Estonia considers that it has the general capacity to prevent and fight cybercrime. It recognises cyberspace-related risks at an early stage and has made substantial efforts to strategically minimise them. The main challenge lies in the processing of cybercrime acts that have already been committed and the scarcity of specialists who have followed the necessary training.

As for future developments, the ability to ensure the cooperation capacities of different bodies both horizontally and vertically is of key importance. The current structure and arrangements for cooperation are insufficient. For example, the role and responsibility of national authorities in the management of cyber defence is currently not unambiguously clear to all important stakeholders.

There is evidently an ever increasing need for closer international cooperation due to the fact that national borders become blurred in cyberspace. Since it is very easy for criminals to act by ignoring national borders, it increases the need for closer cooperation between national agencies of different countries. Estonia's reputation for cyber-awareness is also important. Estonia has continued to be among the pioneers in the field of cyber security and the voice of Estonian specialists is heard. At the same time, choosing clear focuses and harmonising messages is needed to maintain and improve Estonia's reputation, as Estonia does not have enough resources to participate in myriad forms of cooperation.

Estonia is a small and communal country. In the community, people are supposedly more aware of threats and inappropriate behaviour is recognised faster. This is also facilitated by several projects and programmes implemented through cooperation between the private and public sectors. Information and counselling channels are available, including a child helpline, an online hotline and web constables. The themes are systematically examined in public (for instance, cases of internet child pornography are discussed in the media). In parallel with technological development, continuous effort needs to be made to raise people's awareness of threats on the internet.

In a safe community, people protect themselves from the potential risk of falling victim to cybercrime. In particular, families, acquaintances, kindergartens, schools and local governments must have more say in shaping the teaching about the risks in relation to the use of the internet and digital means and about appropriate behaviour in cyberspace. On the whole, prevention work that begins from kindergartens and schools should, rather than individual interventions, be implemented more on the level of universal prevention in a consistent manner, through efficient prevention programmes available for all Estonian kindergartens and schools.

Improving cooperation between the public and private sector (communications undertakings) would make it possible to prevent the spreading of websites with inappropriate content on the internet and to react to the offences committed by using synergies of different measures.

Improving international cooperation would promote prevention and prosecution, as cybercrime often involves cross-border cases.

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 Estonia was able to satisfactorily review the system in Estonia.

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

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

9.2.1 Recommendations to Estonia

1. Prosecutors and judges are not directly included/refereneed in the Strategy and their role, therefore, is somewhat unclear. It is recommended that their role be better defined in future strategies/action plan or in a separate addendum to the current strategy.

2. It is recommended that Estonia considers establishing a centralised cybercrime unit within the Police and Border Guard Board. The creation of a dedicated unit would alleviate the current high reliance on individuals and ensure continuity of the work and development of greater specialisation in this area. This would also serve to improve communication between the Police and prosecutors.

3. It is recommended that the training programme on cybercrime for practitioners be extended. In particular, training should be provided to judges in order to equip them with the necessary skills to adjudicate complex cybercrime cases. The services and products provided by Europol/EC3 and ECTEG should also be promoted in this regard.

4. Estonia should improve its cooperation with EC3 Focal Points and consider joining the J-CAT. This would be beneficial particularly in light of the importance Estonia gives to cybersecurity at national level.

5. The team noted that plans are underway to develop a national child recognition data base, however, it is still at an early stage of development. Estonia is encouraged to advance its plans in this regard.

6. The team recommends that Estonia keeps its data retention legislation under review in light of the ECJ ruling.

7. Estonia should consider amending its criminal procedure code to capture e-evidence and create specific procedures on how to gather e-evidence.

8. The team supports the use of Web constables on the internet in Estonia. It encourages Estonia to further develop this service and consider increasing the number of constables available to provide the best coverage possible.

9. Estonia should continue to build on its bilateral relations with third countries. Efforts should continue to improve mutual legal assistance with third countries, particularly with Russia, using all available channels including the Eurojust contact points in third countries.

10. Estonia should continue to foster good relations with the private sector beyond the mandatory reporting requirements. To this end, prosecutors and judges should engage with the private sector to explain how data should be provided the authorities to ensure that the evidence is admissible in Court.

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

1. A concerted European effort needs to be made to tackle cybercrime. Issues such as how to collect e-evidence, jurisdictional issues and accessing data stored in the 'cloud' need to be considered at a European level.

2. The EU through the European External Action Service (EEAS) is recommended to continue working with third states to improve cooperation, the ability to investigate cybercrime committed overseas and the possibility of gathering digital evidence held outside the EU.

3. Member States are encouraged to follow the Estonian example of using the available resources from the European Union (such as the European Union Internal Security fund) to increase its capacity to respond to cybercrime.

4. Member States are also encouraged to realise the importance of working with the private sector to tackle cybercrime and make efforts to adopt a partnership approach to encourage the private sector to share information with the authorities.

5. The European Commission needs to consider the implications of the ECJ ruling on the Data Retention Directive and to bring forward any necessary proposals to the Council in this regard.

9.2.3 Recommendations to Eurojust/Europol/ENISA

1. The European Cybercrime Training and Education Group (ECTEG) should continue to offer and promote training for law enforcement authorities in the Member States on cybercrime.

ANNEX A: PROGRAMME OF THE VISIT

16. March evening

Arrival of experts

17. March

09: 40 – Ursula is picking up the experts from Radisson's Hotel

10:00 - 12:00 meeting at the Estonian Ministry of the Interior

12.30 – 13.30 lunch / briefing

14.00 – 15.00 meeting at the Central Criminal Police

15.30 – 16.30 meeting at the Information System Authority

19.00 - … Dinner offered by the Deputy State Secretary of the Ministry of Interior

18. March

9:15 – the driver of the Ministry of Interior will pick up the experts

9.30 - 11.30 meeting at the Estonian Ministry of Justice

12.00 – 13.00 lunch /briefing

13.30 – 14.45 meeting at the Estonian Prosecutor General´s Office

15.15 – 16.30 NATO Cooperative Cyber Defence Centre of Excellence

19. March

9.30 – 11:00 meeting at the Estonian Ministry of the Interior, discussion and conclusions

11:30 - … Departure

ANNEX B: LIST OF PARTICIPANTS

Ministry of Interior:

Raivo Küüt

Uku Särekanno

Veiko Kommusaar

Ursula Kimmel

Jenny Jakobson

Kaarel Kalm

Ministry of Justice:

Heili Sepp

Tuuli Ploom

Markko Künnapuu

Imbi Markus

Eneli Laurits

Üllar Lanno (Estonian Forensic Science Institute)

Office of the Prosecutor General:

Eve Olesk

Robert Laid

Piret Paukštys

Police and Border Guard Board:

Väino Kiuru

Kristi Mäe

Dmitri Rudakov

Maarja Punak

Information System Authority:

Sven Kivvistik

Jana Orlovski

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CCP	-	Code of Criminal Procedure
CEPOL	-	European Police College
CERT	-	Cyber Emergency Response Team
DNS	-	Domain Name System
EC3	-	European Cybercrime Center at Europol
ECTEG	-	European Cybercrime Training and Education Group
EEAS	-	European External Action Service
EFSI	-	Estonian Forensic Science Institute
EJTN	-	European Judicial Training Network
ENISA	-	European Network and Information Security Agency
ERA	-	Academy of European Law
EUROJUST	-	The European Union's Judicial Cooperation Unit
EUROPOL	-	The European Police Office
GENVAL	-	Working Party "General Questions including Evaluation"
ICSE	-	International Child Sexual Exploitation
ICSS	-	International Cyber Security Congress
J-CAT	-	Joint Cybercrime Action Taskforce at Europol
JIT	-	Joint Investigation Team

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
LEA	-	Law Enforcement Authorities
MLA	-	Mutual Legal Assistance
MoJ	-	Ministry of Justice
OLAF	-	European Anti-Fraud Office
RIK	-	Centre of Registers and Information Systems
SMIT	-	IT and development centre
TUT	-	Tallin University of Technology