Council of the
European Union

Brussels, 11 September 2017
(OR. en)

8178/1/17
REV 1 DCL 1

GENVAL 40
CYBER 55

DECLASSIFICATION

of document:	ST8178/1/17 REV 1 RESTREINT UE/EU RESTRICTED
dated:	4 September 2017
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Finland

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, 4 September 2017
(OR. en)

8178/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 40
CYBER 55

REPORT

Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Finland

Table of Contents

1. EXECUTIVE SUMMARY

The on-site visit was well organised by the Finnish authorities and included meetings with the relevant actors with responsibilities in the field of preventing and combating cybercrime as well as in the implementation and operation of European policies e.g. the National Cyber Security Centre Finland, the Ministry of the Interior, the Ministry of Justice, the Office of Prosecutor General, the National Bureau of Investigation, the National Police Board, the Ministry of Transport and Communication.

The Finnish authorities provided the evaluation team with complete information and clarifications on legal and operational aspects of preventing and combating cybercrime, cross-border cooperation and cooperation with EU agencies, and cyber strategy.

Finland's Cyber Security Strategy was adopted in 2013 and defines the key goals and guidelines which are used in responding to the threats against the cyber domain and which ensure its functioning. The strategy mostly focuses on the role of the police as opposed to the role of the judiciary. Since its adoption the strategy has not been reviewed and there appear to be no plans to do this in the foreseeable future.

Finland has one centralised police reporting database which utilises its own classification. Yet many officers entering reports in the system do not use the system properly and enter the classification wrongly. Thus, the evaluators felt that on the basis of the police statistics solely it is difficult to gather an overall picture of the extent of cybercrime in Finland. No CERT-FI statistics, number of referrals by FICORA or reliable statistics within the police or judiciary were available. This conclusion directly corresponds with general statements expressed by the National Cyber Security Centre. Therefore, in the evaluators' view cybercrime is under-reported, which makes the assessment of the resilience of the system difficult.

Finland has implemented the European instruments on cybercrime and the resulting measures.

There are general provisions regarding proceedings of investigations, coercive measures and police work in place. No special provisions for cybercrime exist. Due to the specificity of cybercrime the evaluators noticed the need to align legislation in order to give police powers that are compatible with cybercrime investigations.

The police is the competent authority for preventing and carrying out investigations related to cybercrime and in taking cases to prosecutors. The police cooperate with the other law enforcement authorities. The National Police Board operates as the police's central administrative authority under the Ministry of the Interior. The National Police Board plans, manages, develops and oversees police work and the associated functions. The availability of a dedicated budget for cybercrime training and equipment for police departments, managed by the National Police Board, is worth mentioning. It is felt that this acknowledges the importance the National Police Board is placing on the fight against cybercrime at both national and regional level.

The National Bureau of Investigation in Finland seems to be well prepared to tackle cybercrime in Finland, but there is a need to increase knowledge and competence at the regional and local level. It was noted that the National Bureau of Investigation has adopted a system of assisting in, rather than completely taking over, the less serious types of cybercrime investigation. However, it was recommended that general non-technical police personnel across all districts should have access to education in order to ensure a uniform and consistent understanding of cybercrime issues throughout the entire country.

There is a lack of specialisation within the judiciary. In the evaluators' view the current number of prosecutors specialised in cybercrime is not sufficient to deal with the current caseload. Moreover, there is no dedicated structure to fight cybercrime in the Prosecution Service. Due to the increase in cybercrime acts observed, there are grounds for appointing a dedicated group of prosecutors who conduct such cases.

The Finnish Communications Regulatory Authority (FICORA) maintains an overview of the functionality of electronic communications networks and information security, and of reports of potential information security threats. Contact between FICORA and the police appears to be regular yet informal. The conclusion and signing of a Memorandum of Understanding between the two parties should be considered as the first step in strengthening and formalising further collaboration between these two stakeholders. Taking into account the fact that cybercrimes are under-reported, the evaluators recommend that the introduction of a more mandatory reporting system, particularly for serious crimes, be actively considered (e.g. in case of attacks against critical infrastructures or banks).

The establishment of single points of contact by the Police to communicate with international service providers deserves special mention. This makes it easier to maintain relations between authorities and private industry which are based on trust and mutual respect.

Europol/EC3 and Eurojust are known to the practitioners and are asked for assistance. Finland has made use of Joint Investigation Teams quite often. It was noted that the Finnish authorities regard their experience as very positive and continue to promote the use of JITs in cross-border investigations due to the possibilities that exist within this framework.

The existing regional cooperation amongst Nordic countries is regarded as an effective best practice. Examples of this type of cooperation include the Nordic Arrest Warrant, sharing of liaison officers and the Nordic Training Platform. Also, the excellent cooperation with the Baltic States merits attention.

Knowledge about cybercrime issues amongst the judiciary is limited. Whereas there are plans to increase training offered to prosecutors on some basic aspects, systematic training for judges is currently not available. In the opinion of prosecutors there is a clear need for more education regarding cybercrime issues amongst prosecutors and judges. Specialist knowledge and access to tools within the regional and local police forces depend mainly on the individual police districts. The provision of systematic training for specialised police officers by exploiting already existing training opportunities available through external sources, such as the European Cybercrime Training and Education Group (ECTEG) and CEPOL, could also be considered.

There seem to be very limited and sporadic prevention campaigns and efforts directed towards the general population on the subjects of child abuse and, more generally, internet safety. In the evaluators' view there is an opportunity for the Cybercrime Centre, Cyber Security Centre, cyber security companies and NGOs to address this gap by pooling resources in order to implement visible and sustainable campaigns directed towards increasing awareness of this phenomenon amongst the general population.

Taking into account the ambitious approach in terms of countering cybercrime and the resources allocated to the fight against it, the opinion of the evaluators on the situation in Finland is positive and promising.

2. INTRODUCTION

Following the adoption of 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 European policies 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 should provide a comprehensive examination of the legal and operational aspects of tackling cybercrime, cross-border cooperation and cooperation with relevant EU agencies. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography[2] (transposition date 18 December 2013), and Directive 2013/40/EU[3] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

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

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

Experience from past evaluations show 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 for 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 cybercrime only but rather on the operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, it 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.

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

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

6 CETS no. 189; opened for signature on 28 January 2003, entered into force on 1 March 2006.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Finland was the twenty seventh 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 members 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 conducting the evaluation of Finland were Mr Timothy Zammit (Malta), Ms Aneta Trojanowska (Poland), and Mr Henrik Olin (Sweden). Two observers were also present: Mr Michael Schmid (Eurojust) together with Mr Sławomir Buczma from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Finland between 6 and 9 September 2016, and on Finland's detailed replies to the evaluation questionnaire together with its detailed answers to ensuing follow-up questions.

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

Finland's Cyber Security Strategy was adopted on 24 January 2013 as a Government Resolution. The Strategy defines the key goals and guidelines which are used in responding to the threats against the cyber domain and which ensure its functioning. One of the ten strategic guidelines of the Cyber Security Strategy is to make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime. Furthermore, it is expected that the police are provided with sufficient powers, resources and motivated personnel for cybercrime prevention, tactical police investigations as well as for processing and analysing the digital evidence.

The Cyber Security Strategy stresses the importance of international operational cooperation and continued and intensified exchange of information with the EU and with other countries' corresponding law enforcement officials, such as Europol.

The national implementation programme of the Cyber Security Strategy was published on 11 March 2014. A total of 74 measures suggested by administrative branches and the security of supply organisation were put together in the implementation programme to improve cyber security.

The Information Security Strategy for Finland was adopted by the Minister for Transport and Communications in March 2016. The strategy sets out how economic prosperity can be supported by building a more trusted and resilient digital environment.

3.2. National priorities with regard to cybercrime

When Finland's Cyber Security Strategy was created in 2013 police capabilities were recognised as one area of development. One of the strategic guidelines is: 'make certain that the police have sufficient capabilities to prevent, expose and solve cybercrime'. Based on this strategy an implementation plan was created. The plan has a total of 74 action points for different sectors of government. There are several action points in the plan which aims to improve police capabilities in the fight against cybercrime.

18	The Police University College will develop its training offer in cybercrime-related topics
45	A study will be made to assess the legal powers of police to efficiently prevent, expose and solve cybercrime
46	Ensuring that the national 24/7 contact point in the NBI has cybercrime-related capabilities to meet national and international needs
47	Ensuring that situational awareness of the cybercrime situation in Finland will be established and internet-related intelligence gathering and management will be improved
48	Organising and resourcing the fight against cybercrime

Several actions are already been taken regarding the above-mentioned action points.

18	The Police University College recruited a person in May 2015 to develop its cybercrime-related training offer. More about the achievements later in this questionnaire.
45	The study has been made and a report published about the legal powers of police to efficiently prevent, expose and solve cybercrime
46	The national 24/7 contact point in the NBI has been resourced with cyber duty officers.
47	A study was made about the police's approach to situational awareness of the cybercrime situation in Finland. It contains suggestions on how to build a comprehensive situational picture in cooperation with the government and private partners. The internet-related intelligence gathering and management have been strengthened.
48	A guideline for the fight against cybercrime was set by the National Police Board. A Cybercrime Centre was established in the NBI on 15.4.2015.

The new strategic police plan was launched in 2015. One goal of the plan is targeting resources at computerised crime prevention and developing cybersecurity know-how. Actions for achieving the goals are:

- Increasing know-how about cybercrime prevention;
- Allocating more resources to preventing cybercrime but also ensuring the cybersecurity of the police's own systems;
- Investigating how the police's powers to access data through different information networks should be increased.

In order to prevent cybercrime, the operating conditions of serious crime should be restricted, paying special attention to international priorities. The following actions are needed to achieve this goal:

• Keeping up to date with the development of criminal phenomena and priorities set for international cybercrime prevention as part of the EU Policy Cycle and making use of such knowledge expediently and in a proactive manner in national operations

• Preventing international cybercrime targeted at Finland, with the aim of uncovering and preventing cybercrimes before they occur and bringing criminals to justice in their countries of origin.

Deriving from the Finland's Cyber Security Strategy but also from law enforcement operational needs, 'cyber issues' have been acknowledged in all levels of policing. The plan stipulates that prevention is of the utmost importance regarding serious crime.

The new Cyber Crime Prevention Centre in the National Bureau of Investigations began operations on 1 April 2015. The Centre is geared towards improvement of police capacity to prevent and investigate serious crimes. In addition to prevention of cyber crimes, the new Centre is involved in internet intelligence as well as conducting threat assessments.

In order to fulfil the goals laid down by Finland's Cyber Security Strategy, the National Police Board set up a working group to draft a comprehensive cyber plan for the police on 25 March 2015 and its mandate has been set until the end of 2016. The working group gathers experts on cybercrime and cyber security matters from different units of the police force.

In addition, the National Police Board has issued written orders and guidelines on the use and maintenance of police data systems, on information security, on management of information security failure and the handling of confidential information. These instructions have not been translated into English.

The comprehensive cybercrime prevention plan is implemented by the National Police Board in close cooperation with local police units, the National Bureau of Investigations and the Ministry of the Interior. In the plan there are numerous actions to be taken in order to achieve its goals.

Furthermore, the Police is a member of Nordic Computer Forensic Investigators which offer courses in the forensic area. The police have launched a special quality programme which aims to improve analyses of digital evidence in a legally certain manner. In addition, the competence of authorities, prosecutors and judges involved in the investigation of cybercrime is improved by developing relevant training.

Finland is currently reviewing legislation relating to information gathering and data processing to ensure sufficient resources and powers to prevent, expose and solve cybercrime.

Finnish national priorities are the same as the EU cybercrime priority. Finland is taking part as an actor in all three sub-priority areas of EMPACT Cybercrime (cyber attacks, payment card fraud and child sexual exploitation).

Finland takes an active part in discussions concerning cybercrime within both the Council of Europe and the EU. The Ministry of Justice has also established a horizontal working group which deals with practical questions relating to international cooperation in criminal matters. In addition to representatives of the Ministries of Justice and the Interior, prosecutors and law enforcement authorities, as well as judges and the Criminal Sanctions Agency, are represented in that Working Group. For years it has turned out to be a useful forum for exchanging views and practices as well as informing legislators and practitioners of new legislation and developments in this field.

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

The Finnish authorities reported that the amount of online bank fraud (e-banking malware fraud) has declined and there have been only a few isolated cases in the last two years. However, a significant increase in the amount of online payment card fraud since last year has been observed (1Q 2016 174.6 % increase compared to 1Q 2015).

Phishing campaigns have become constant and, in addition, more carefully planned and executed than in the past. Social engineering in its various forms is more common nowadays than it was a few years ago. As a rather new phenomenon there have been quite a few cases of CEO fraud recently.

Malware, especially ransomware, has become more serious than before in terms of its capability to cause damage.

3.3.2. Number of registered cases of cyber criminality

The statistics for 2013 and 2014 were provided by Statistics Finland. Provisions concerning damage to data offences (Chapter 35, Sections 3(a) to 3(c) of the Criminal Code) and identity theft (Chapter 38, Section 9(a) of the Criminal Code) came into force on 4 September 2015 and because of that offences included in those provisions are not covered. Many offences relevant in this context are not only cybercrimes, but may be committed also in another way (for example forgery and fraud offences). Statistics information concerning those offences does not make any difference in this respect. The following numbers cover convictions at district courts:

	2013	2014
Endangerment of data processing (34:9 (a))	2	3
Message interception (38:3)	6	9
Aggravated message interception (38:4)	1	2
Interference with communications (38:5)	6	10
Aggravated interference with communications (38:6)	1	4
Petty interference with communications (38:7)	-	-
Interference in an information system (38:7 (a))	1	1
Aggravated interference in an information system (38:7 (b))	-	-
Computer break-in (38:8)	2	4
Aggravated computer break-in (38: 8 (a))	1	-
Offence involving a system for accessing protected services (38:8 (b))	-	-

3.4. Domestic budget allocated to preventing and fighting cybercrime and support from EU funding

There is no special budget allocation for any of the crime areas. However, there is a dedicated budget (EUR 420 000 in 2016) in the National Police Board for supporting police units in IT forensics training and equipment sourcing. Police units are mainly responsible for their own operations, training and sourcing of equipment.

There is no specific operational budget allocation in the National Bureau of Investigation for the Cybercrime Centre due to the organisational model of the centre. An operational budget is given to the three divisions of the National Bureau of Investigation in which the Centre's personnel are employed.

The Cybercrime Centre is organised in a matrix model. Although there is no specific budget allocation for the fight against cybercrime, divisions of the National Bureau of Investigation are actively using their resources in this area.

Combatting cybercrime and ensuring the know-how of the police in cybercrime investigations and in cyber forensics have been included in the National Internal Security Fund programme and its enforcement plan. The National Bureau of Investigation's Cybercrime Centre has applied for (via the National Police Board) and been granted funds from the EU Internal Security Fund for setting up the centre and developing technical capabilities (EUR 1 288 913 for 2015-2016).

3.5. Conclusions

- Finland's Cyber Security Strategy has been in place since 2013. It presents the vision, approach and strategic guidelines of cyber security in Finland. It indicates certain entities of public administration and describes their roles. It also emphasises the important role of preventive actions, which are aimed at increasing social awareness regarding virtual world threats.

- Finland's Cyber Security Strategy is supposed to cover all aspects of the topic. However, the strategy mostly focuses on the role of the police as opposed to the role of the judiciary. Partly, this has the effect that the main emphasis is on the prevention of cybercrime and its criminal liability is hardly mentioned at all. This choice should, in the opinion of the evaluators, be reassessed.

- The strategy is accompanied by an implementation plan. This implementation plan is subject to constant evaluation, but not the strategy itself. In the evaluators' view the necessary review of the Cyber Security Strategy should be conducted in order to reflect today's needs – such as including those of the judiciary in the strategy.

- Finland has one centralised police reporting database. The crime reporting database has its own classification. Yet, many officers entering reports in the system do not use the system properly and enter the classification wrongly. In the evaluators' view quality control in terms of collecting statistics calls for improvement.

- Furthermore, there are no CERT statistics, number of referrals by FICORA or reliable statistics within the Police or judiciary. The complete picture presented in statistical terms determines the scale of the problem of cybercrime in Finland. Without the complete data/statistics it is hard to define that problem. That conclusion directly corresponds with general statements in Finland's Cyber Security Strategy. Therefore, in the evaluators' view cybercrime is under-reported, which makes gathering of an overall picture of the extent of the phenomenon difficult.

- According to the information collected during the on-site visit no additional budget was provided to the Police following the publication of the cybersecurity strategy which set out tasks but not resources. The overall impression is that the judiciary and the Police lack resources they feel are needed to effectively combat cybercrime. A needs analysis has to be carried out in order to ensure that resources are in place. At practitioner level (police), there appears to be a very good understanding of the limitations and the possible solutions when dealing with cybercrime. However, the evaluators got the impression that practitioners feel that there is not the same level of 'appreciation' of the subject at the strategic level.

- The availability of a dedicated budget for cybercrime training and equipment for police departments managed by the National Police Board is welcomed. It acknowledges the importance of the fight against this crime phenomenon at both national and regional level for the National Police Board.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

There are no prosecutors or courts dealing exclusively with cybercrime. A group of prosecutors in local prosecution units pursue most cases of cybercrime but they also have other tasks. No special powers have been granted to them.

The Prosecutor General has nominated four prosecutors to specialise in problems related to cybercrime. These tasks, however, are not their only ones. In the future they are expected to give assistance and training to other prosecutors. The Prosecutor General's Office has also organised a few seminars *inter alia* on cyber currency, child abuse material (CAM), etc. Prosecutors have also been given the opportunity to take part in courses organised by the police.

In Finland the police are in charge of the pre-trial investigation of crimes. Investigations occur in close cooperation with the prosecutor designated to deal with the case from the very beginning of the investigation, as all the decisions will have an impact on the prosecutor's subsequent opportunity to present evidence and try the case successfully.

4.1.2. Capacity and obstacles for successful prosecution

Difficulties mentioned by the Finnish authorities result from the lack of public prosecutors designated to handle solely cybercrime. At the Office of General Prosecutor, there is no state prosecutor who would be responsible for cybercrime. Since cybercrime is expected to increase and complex cybercrime cases generally involve international cooperation and ambiguous legal issues, the workload of public prosecutors is massive. Therefore, the current prosecution resources will most probably not be sufficient to handle cybercrime cases in the future. The resources invested at the police level can also not be fully exploited if there are not sufficient resources to prosecute the cases.

The Finnish authorities mentioned the difficulty of defining cybercrime. This may lead to problems as cases with cybercrime elements are not investigated and prosecuted by the police or prosecutors who are specialised in cybercrime. For example, drug trafficking via the Tor network would normally be handled by a prosecutor who is specialised in drug offences; distribution of child pornography via the Tor network by a prosecutor who is specialised in offences targeted at children; illegal sharing or usage of online copyright material/ business secrets by a prosecutor who is specialised in financial crimes; and identity theft or petty computer-related fraud by a junior prosecutor. The problems may occur as all the above-mentioned cases call for special knowledge on cybercrime. Thus, an obstacle in successful prosecution is that the cases may not always be dealt with by the people who have sufficient knowledge of cybercrime.

Insufficient general knowledge of cybercrime on the part of judges at district court level was also mentioned as an obstacle. This has led to judgments in which the content of evidence appears not to have been fully understood. Some judges also seem to be reluctant to handle cybercrime cases as they are not familiar with technical aspects. Specialisation by both prosecutors and judges would be desirable. Some difficulties also arise from the fact that there is a lack of court practice for many cybercrimes.

Furthermore, as from January 2015, plea bargaining has been put in place in the Finnish criminal procedure but it seems not to apply very well to cybercrime. This may be put down to the fact that in the case of thousands of victims, very often residing abroad, it is impossible to obtain the consent of all victims.

Lengthy proceedings are the main obstacle to successful cybercrime investigation, especially if evidence has to be obtained via MLA.

4.2. Law enforcement authorities

Finland has a single police organisation which is subordinate to the Ministry of the Interior. The Finnish Security Intelligence Service is a national police but is operating directly under the Ministry of the Interior. The police activities are planned, managed and supervised by the National Police Board. Each of Finland's 11 police departments is responsible for maintaining public order and security and preventing crime in the regions. The National Bureau of Investigation and the Police University College are Finnish police two national units and are managed and supervised by the National Police Board.

The Government steers police operations through goals entered in the Government Programme and through Government Resolutions.

The police force is a performance-managed organisation. Steering and monitoring it is the responsibility of the Ministry of the Interior. The police organisation is two-tiered: under the Ministry of the Interior, police operations are directed and guided by the National Police Board except the Finnish Security Intelligence Service which is under the Ministry of the Interior.

The key functions, operating principles and powers of the police are provided for by law. In addition to Acts and Government Decrees, the police is governed by Ministry of the Interior Decrees, instructions and guidelines. The role of the Finnish Police is to secure judicial and social order, maintain public order and security and prevent and investigate crime. The police lead pre-trial investigations and cooperate closely with the Border Guard and Customs, which are pre-trial authorities in their respective spheres of activity.

The Cybercrime Centre was established in 2015 as a specialised body to investigate cybercrime, but all police districts are also responsible for investigating cybercrime. The centre is responsible for international, organised, technically challenging and larger cybercrime cases. Police districts are responsible for all cases that have happened in their region. The Cybercrime Centre (the National Bureau of Investigation) and police districts normally easily agree which unit handles different cases. If they cannot find an agreement the National Police Board will intervene and make a decision.

All police districts have their own IT forensic groups. The ways districts have organised pre-trial investigation of cybercrime vary a lot. In many districts there are no specialised investigators. The Cybercrime Centre also supports all police units with investigation of cybercrime, IT forensic examinations, intelligence on internet and international cooperation.

The Security and Intelligence Service is responsible for cybercrime in its own domain but cybercrimes are investigated by the police.

With regard to the commitments of the Budapest Convention, the Communication Centre of the National Bureau of Investigation is the 24/7 contact point for international requests. Most of the international 24/7 tools in Finland have been integrated into one entity. The Communication Centre is located in the same place as Interpol Helsinki, SIRENE Finland and the Europol National Unit. Representatives of the Criminal Intelligence awareness function and Internet Intelligence function are also present in the Communication Centre almost around the clock. In addition, a senior police officer is always available as a duty officer and has access to all the Centre's resources if needed. The duty officer has legal competency to decide, for instance, on preservation of data, search and seizure as well as arrest.

Obtaining evidence by using the slow MLA procedure was mentioned by the Police as the main obstacle in cybercrime investigation. Quick seizure of data is a very critical issue in criminal investigation in general, but especially in cybercrime investigation. It is very common that the execution of MLAs takes at least 2-3 months. It is not rare for it to take one year or sometimes even longer. The problem becomes very serious if the results obtained by MLA generate the need for another request for mutual legal assistance. Another obstacle is that nowhere near all countries (not even those party to the Budapest Convention) have the legal possibility to execute a data preservation order.

4.3. Other authorities/institutions/public-private partnership

The Finnish Communications Regulatory Authority (FICORA) functions under the Ministry of Transport and Communications. FICORA maintains an overview of the functionality of electronic communications networks and information security, and reports of possible information security threats. The objective is also to increase awareness of information security in homes and companies e.g. by means of guidelines. FICORA also ensures the compatibility of communications networks and services.

The National Cyber Security Centre is an external division of FICORA. The Centre is responsible for:

- the readiness of telecoms operators, and viability of communications networks and services in the event of faults and disturbances, and in exceptional circumstances
- the protection of privacy in electronic communications
- electronic identification and electronic signatures
- official requirements in emergency traffic, interception and supervision of telecommunications
- the duties of the National Communications Security Authority (NCSA-FI)
- FI-domain name management.

FICORA's CERT-FI and NCSA-FI duties have been merged into the National Cyber Security Centre.

The NCSC-FI is a national information security authority. It develops and monitors the operational reliability and security of communications networks and services. Its CERT duties consist of preventing, detecting and resolving security breaches, as well as reporting information security threats. The Centre's NCSA duties include responsibility for security matters related to electronic transfer and processing of classified information.

NCSA-FI's duties concerning international information security obligations:

- preparation of guidance and agreements concerning national security activities;
- preparation of guidance on the handling of international classified information;
- management and accounting of the crypto material distribution network and guidance on the secure handling of the material (CDA);
- approval of cryptographic products for protecting international classified information in Finland (CAA);
- accreditation of information systems used for processing international classified information (SAA) (The accreditation process concerns government systems deployed to meet international information security obligations and the systems of companies that participate in international competitive bidding and need accreditation from a National Communications Security Authority.);
- coordination of and guidance on national TEMPEST activities (NTA).

The Centre's operations aim at ensuring that public communications networks and communications services are safe and interference-free, as well as securing critical societal functions. In accordance with the agreement concluded with the National Emergency Supply Agency, the NCSC-FI is, for its part, responsible for ensuring the functionality of technical systems critical to the security of supply. The NCSC-FI intends to develop and diversify its information security services by means of e.g. development work and extensive partnership networks.

FICORA also has several duties concerning national information security obligations:

- steering and supervision of telecoms operators' information security management: for example, monitoring compliance with the information security regulation (M47);
- steering and supervision of strong electronic identification and the provision of qualified certificates: for example, monitoring compliance with regulations M7 and M8 issued by FICORA and carrying out annual audits of certification authorities providing qualified certificates;
- assessment of authorities' information systems and telecommunications arrangements;
- accreditation of information security inspection bodies;
- cooperation with national and international security stakeholders.

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

The new Cyber Crime Centre in the National Bureau of Investigations (NBI) is geared towards improvement of police capacity to prevent and investigate serious crimes. In addition to prevention of cybercrime, investigation and digital forensics, the new centre is involved in internet intelligence as well as conducting threat assessments. The Cyber Crime Centre generates and maintains an analysed cybercrime situation picture and disseminates it as part of the Finnish combined situation picture. The Finnish Security Intelligence Service maintains a situation picture of its field of activities.

One of the actions in the police's strategic plan is to deepen cooperation with other safety and security authorities and make use of intelligence-led management and improve the analysis know-how and tools of the police. Cyber security arrangements follow the division of duties between authorities, businesses and organisations, in accordance with statutes and agreed cooperation.

The investigation of any crime and thus cybercrime takes place in close cooperation between the investigation authorities and the prosecutor designated to deal with the case. Investigation authorities have to inform the prosecutor's office of any crime where there is an international connection or other grounds for cooperation. The prosecutor is entitled to order investigation measures to be carried out. Any request to another State for mutual legal assistance needs to be reported to the prosecutor.

The main cooperation partner for the police in preventing and fighting cybercrime is the National Cyber Security Centre (NCSC-FI). Their CERT duties consist of preventing, detecting and resolving security breaches, as well as reporting information security threats. The NCSC-FI also maintains nationwide situational awareness of cyber security.

There are many overlapping areas in the NCSC-FI's tasks with the police, but the roles of both parties are clear. A short description of roles: the police's main tasks are the interception of criminals and pre-trial investigation of cybercrimes and the NCSC-FI's main tasks are situational awareness, prevention and supporting corporations and government agencies, especially critical infrastructure entities, to resolve security breaches (not only crimes). Also, a Memorandum of Understanding (MoU) is being negotiated between the NCSC-FI and the police regarding cooperation of parties. Cooperation is considered to be open and easy-going, especially on an operational level. With the forthcoming MoU, cooperation in other areas (communications, R&D, competence development etc.) will deepen.

4.4.2. Resources allocated to improving cooperation

In the NBI there is shared responsibility among all officers in their respective areas. It is considered very important and especially management-level personnel have put a lot of effort and time into building good working relationships with private sector entities.

According to the Finnish authorities, there is a need for more tools to test different modi operandi in order to be able to investigate them when needed and to enhance knowledge in that area. Criminals develop their methods quickly and law enforcement agencies (LEAs) are always lagging behind them due to the reactive nature of police organisations. For example, according to the Finnish authorities, weaknesses in NFC payments will probably be the target of criminals in future.

4.5. Conclusions

- Currently there are no prosecutors or courts dealing exclusively with cybercrime.

- The Office of the Prosecutor General will be re-organised as from the beginning of 2018. Specialised prosecutors will be divided into three areas: persons (including CSE and THB), economy (including tax fraud) and security (including terrorism and offences against IT systems). The number of prosecutors has been on the decline for years. Resources at the Office of the Prosecutor General need to match any increases in police resources in order to avoid a bottleneck.

- The evaluation team noted the plan to improve the service offered by the Prosecutor's Offices through organisational restructuring and increasing the number of specialised prosecutors dealing with cybercrime cases. Keeping in mind the fact that the police also expressed their intention to dedicate more resources towards this phenomenon and the already existing caseload, the evaluation team is concerned that the planned increase may still not be sufficient to avoid any bottleneck that may occur at the prosecutor's level.

- However, increasing the number of specialised prosecutors alone will not solve the difficulties mentioned by Finland as regards the definition of cybercrime. In the opinion of the evaluators, this can be addressed through a twofold approach: (1) increasing the general level of knowledge across the board to include prosecutors dealing with traditional cases that involve cybercrime elements; and (2) implementing a mechanism whereby prosecutors dealing with these cases may call for the help of specialised cybercrime prosecutors.

- The National Bureau of Investigation in Finland seems to be well prepared to tackle cybercrime, but the need to increase knowledge and competence at the regional and local level is evident. It seems that only four out of eleven police districts have 'adequate' knowledge of cybercrime amongst their investigators. Other departments may have a good understanding of technical issues amongst IT forensics personnel but not among the investigators. Therefore, in the evaluators' view, nationwide training on general cybercrime issues should be provided to investigators.

- The structure dedicated to fighting cybercrime has developed. Every district has a unit specialised in IT forensics. Nevertheless, it is necessary to provide proper equipment and to introduce dedicated forensic training, especially in the field of child pornography and card fraud.

- Worth mentioning is the method of the Finnish Cybercrime Centre at the NBI of not taking over whole cases but rather assisting the local police authorities in solving a problem. This leads to a learning effect for the competent regional investigators.

- This measure is further supported by a specifically allocated budget at the National Police Board for specific cybercrime training and equipment, which is also welcomed by the evaluators.

- Fighting against cybercrime and providing cybersecurity is implemented by both law enforcement agencies and the IT sector. Despite the frequent lack of formal documents indicating the range and character of cooperation, it seems that actions are conducted professionally.

- However, it would be advisable to prepare some standards regarding the gathering and sharing of information about the scale and character of threats. The data would, for instance, allow for the setting up of preventive programmes or social campaigns to enhance internet users' awareness of basic safety rules regarding cyber and other kinds of threats.

- Contact between FICORA and the Police appears to be regular yet informal. The conclusion and signing of an MoU between the two parties should be considered as the first step in strengthening further the collaboration between these two very important stakeholders.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1. Council of Europe Convention on Cybercrime

Finland has been a party to the Budapest Convention on Cybercrime since 2007.

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

Council Framework Decision 2005/222/JHA on attacks against information systems was transposed into Finnish law. Finland has also transposed Directive 2013/40/EU on attacks against information systems. In that context the Criminal Code (CC), especially Chapter 38 concerning data and communications offences, was amended (Law 368/2015). These amendments came into force on 4 September 2015.

Hence, there is an extensive body of law in place in Finland regarding cybercrime[7]. The following acts are criminalised therein: Computer break-in (Chapter 38, Sections 8 to 8(a)) and aggravated computer break-in (Chapter 38, Section 8); Aggravated interference with communications, petty interference with communications, interference in an information system and aggravated interference in an information system (Chapter 38, Sections 5 to 7(b)); Damage to data, aggravated damage to data and petty damage to data (Chapter 35, Sections 3(a) to 3(c)); Message interception and aggravated message interception (Chapter 38, Sections 3 and 4); Endangerment of data processing and an offence involving a system for accessing protected services (Chapter 34, Section 9(a) and Chapter 38, Section 8 (b)).

[7] Due to the large number of pages, a detailed description has not been included in the report. For further information, see Annex D.

Mitigating and aggravating circumstances are specified in the CC. Principals and accessories may be held criminally liable under Finnish law. Legal entities may be held criminally liable for offences perpetrated in the performance of their activity or in their interest or on their behalf. Chapter 9 of the Criminal Code includes provisions concerning corporate criminal liability. According to Section 1(1) a corporation, foundation or other legal entity in the operations of which an offence has been committed shall on the request of the public prosecutor be sentenced to a corporate fine if such a sanction has been provided in the Criminal Code for the offence. According to Chapter 9, Section 5 of the Criminal Code a corporate fine is imposed as a lump sum. The corporate fine is at least 850 euros and at most 850 000 euros.

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

The Finnish authorities stated that implementation of Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography did not require legislative measures because the relevant legislation was in line with the Directive. The Criminal Code (Law 540/2011) and some other laws were already amended on 1 June 2011 in relation to the obligations arising from the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Finland has been a party of that Convention since 2011.

Computer-related child pornography offences

The offences in question are *distribution of a sexually offensive picture, aggravated distribution of a sexually offensive picture depicting a child* and *possession of a sexually offensive picture depicting a child* (Chapter 17, Sections 18, 18(a) and 19, of the Criminal Code). These provisions are general, covering all kinds of ways of committing these offences.

Computer-related solicitation of children

The offence in question is *Solicitation of a child for sexual purposes* (Chapter 20, Section 8(b), of the Criminal Code). Provisions are general, covering all kinds of ways of committing these offences.

C/ Online card fraud

Finnish law counters any fraudulent financial operations made online. The conduct described as 'computer-related fraud' and 'computer-related forgery' are penalised by the Criminal Code.

Computer-related fraud

The offences in question are *fraud, aggravated fraud, petty fraud, means of payment fraud, aggravated means of payment fraud* and *petty means of payment fraud* (Chapter 36, Sections 1 to 3, of the Criminal Code and Chapter 37, Sections 8 to 10, of the Criminal Code).

Computer-related forgery

The offences in question are *forgery, aggravated forgery* and *petty forgery* (Chapter 33, Sections 1 to 3, of the Criminal Code). These provisions are general, covering all kinds of ways of committing these offences [8].

[8] Please refer to Annex D to find a description of these offences.

D/ Other cybercrime phenomena

Identity theft is criminalised in the Criminal Code (Chapter 38, Section 9(a)).

Chapter 38, Section 9(a) – Identity theft
A person who in order to deceive a third party unlawfully uses the personal information, access codes or other corresponding identifying information of another and in this manner causes economic loss or more than petty impediment to the person to whom the information belongs, shall be sentenced to a fine for *identity theft*.

Although the Finnish authorities stressed that it was not clear what was meant by 'spam', junk emails or unsolicited bulk emails were regarded as falling under this term. Acts related to spam are similar to an offence referred to as 'harassing communications' (Chapter 24, Section 1(a), of the Criminal Code).

Chapter 24, Section 1(a) – Harassing communications
A person who, with intent to disturb, repeatedly sends messages or calls another so that the act is conducive to causing said other person considerable disturbance or harm, shall be sentenced for *harassing communications* to a fine or to imprisonment for at most six months.

5.2. Procedural issues

5.2.1. Investigative techniques

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

Provisions concerning search of data contained in a device are set out in Chapter 8, Sections 20 to 29, of the Coercive Measures Act. The definitions and the prerequisites of such search are included in Sections 20 and 21:

Chapter 8, Section 20 – Definition of a search of data contained in a device

(1) A *search of data contained in a device* refers to a search that is directed at the data contained at the time of the search in a computer, a terminal end device or in another corresponding technical device or information system.

(2) A search of data contained in a device may not be directed at a confidential message, in respect of which Chapter 10 contains provisions on telecommunications interception, traffic data monitoring and technical surveillance.

Chapter 8, Section 21 – Prerequisites for a search of data contained in a device

(1) A search of data contained in a device may be conducted if:

(1) there is reason to suspect that an offence has been committed and the most severe punishment provided for the offence is imprisonment for at least six months, or if the matter being investigated involves circumstances connected to the imposition of a corporate fine; and

(2) it may be presumed that the search may lead to the discovery of a document or data to be seized as referred to in Chapter 7, Section 1, subsections 1 or 2, or to a document to be copied on the basis of Chapter 7, section 2, and that is connected with the offence under investigation.

(2) A search of data contained in a device may also be conducted in order to return the device to a person entitled to it, if there are grounds to suspect that it has been illegally taken from someone.
(3) The decision on conducting a search of the premises may be extended to cover also a technical device or information system on said premises, if the search in question is not one intended to find a person.

The search of data contained in a device is not a covert (secret) coercive measure. However, obtaining evidence in secret from the subject is possible according to Chapter 10, Section 23, of the Coercive Measures Act:

Chapter 10, Section 23 – Technical surveillance of a device and its prerequisites
(1) The *technical surveillance of a device* refers to other than solely sensory surveillance, recording or other processing of the operation of a computer or other corresponding technical device or of the data or identification data contained therein, for the purpose of the investigation of a factor that is of significance for the clarification of an offence.
(2) Technical surveillance of a device may not be used to obtain information about the content of a message or the identifying data referred to in Section 6, subsection 1.
(3) The criminal investigation authority may direct technical surveillance of a device to a computer or another corresponding technical device or its program referred to in subsection 1 that is probably used by a person suspected of committing an offence, when there are grounds to suspect this person of an offence referred to in Section 16, subsection 3.

Section 16(3) covers offences for which the most severe punishment provided is imprisonment for at least four years and some other more minor offences.

Provisions concerning seizure are laid down in Chapter 7 of the Coercive Measures Act. When the object is a document (it may also take the form of data) the primary offence is copying.

Chapter 7, Section 1 – Prerequisites for seizure

(1) An object, item of property or document may be seized if there are grounds to suspect that:

(1) it may be used as evidence in a criminal case;

(2) it has been taken from someone in an offence; or

(3) it may be ordered to be forfeited.

(2) is the provisions of subsection 1, paragraphs 1 and 2, also apply to information that is contained in a technical device or in another corresponding information system or in its recording platform (*data*). The provisions in this Chapter regarding a document also apply to a document that takes the form of data.

Chapter 7, Section 2 – Copying of a document

(1) Seizure of a document to be used as evidence in accordance with Section 1, subsection 1, paragraph 1, shall be replaced by copying said document if a copy is sufficient from the point of view of the credibility of testimony.

(2) A document shall be copied without undue delay after possession has been taken of it. After being copied it shall be returned without delay to the person from whom it was taken.

(3) If a document cannot be copied without delay due to the nature or extent of the document or documentation, the document shall be seized.

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

The definitions and the prerequisites of telecommunications interception and traffic data are included in Chapter 10, Section 3 and Section 6, of the Coercive Measures Act:

Chapter 10, Section 3 – Telecommunications interception and its prerequisites

(1) *Telecommunications interception* refers to the monitoring, recording and other processing of a message sent to or transmitted from a network address or terminal end device through a public communications network referred to in the Telecommunications Services Act or a communications network connected thereto, in order to determine the contents of the message and the identifying data connected to it referred to in Section 6. Telecommunications interception may be directed only at a message that originates from or is intended for a a person suspected of an offence.

(2) A criminal investigation authority may receive permission for telecommunications interception directed at a network address or terminal end device in the possession of or otherwise presumably used by a person suspected of an offence, when there are grounds to suspect him or her of:

(1) genocide, preparation of genocide, a crime against humanity, an aggravated crime against humanity, a war crime, an aggravated war crime, torture, violation of a prohibition against chemical weapons, violation of a prohibition against biological weapons, violation of a prohibition against anti-infantry mines;

(2) endangerment of the sovereignty of Finland, incitement to war, treason, aggravated treason, espionage, aggravated espionage, disclosure of a national secret, unlawful gathering of intelligence;

(3) high treason, aggravated high treason, preparation of high treason;

(4) aggravated distribution of a sexually offensive picture depicting a child;

(5) sexual abuse of a child, aggravated sexual abuse of a child;

(6) manslaughter, murder, homicide, preparation of an aggravated offence directed against life or health as referred to in Chapter 21, Section 6a, of the Criminal Code and in accordance with Sections 1, 2 and 3 of said Chapter;

(7) arrangement of aggravated illegal entry into the country, aggravated deprivation of liberty, trafficking in persons, aggravated trafficking in persons, kidnapping, preparation of kidnapping;

(8) aggravated robbery, preparation of aggravated robbery, aggravated extortion;

(9) aggravated concealment of illegally obtained goods, professional concealment of illegally obtained goods, aggravated money laundering;

(10) criminal mischief, criminal traffic mischief, aggravated sabotage, aggravated endangerment of health, a nuclear device offence, hijacking;

(11) an offence committed with terrorist intent, preparation of an offence committed with terrorist intent, directing of a terrorist group, promotion of the activity of a terrorist group, provision of training for the commission of a terrorist offence, recruitment for the commission of a terrorist offence, financing of terrorism, as referred to in Chapter 34(a), section 1, subsection 1, paragraphs 2-7 or subsection 2 of the Criminal Code;

(12) aggravated damage to property or aggravated damage to data;

(13) aggravated fraud, aggravated usury;

(14) aggravated counterfeiting;

(15) aggravated impairment of the environment; or

(16) an aggravated narcotics offence.

(3) A warrant for telecommunications interception may also be issued when there are grounds to suspect a person of the following in connection with commercial or professional activity:

(1) aggravated giving of a bribe;

(2) aggravated embezzlement;

(3) aggravated tax fraud, aggravated assistance fraud;

(4) aggravated forgery;

(5) aggravated dishonesty by a debtor;

(6) aggravated taking of a bribe, aggravated abuse of public office;

(7) aggravated regulation offence;

(8) aggravated abuse of insider information, aggravated market distortion; or

(9) an aggravated customs offence.

(4) An additional prerequisite to the issuing of the warrant referred to above in subsection 3 is that the offence was committed in order to obtain especially large benefit and the offence has been committed in an especially methodical manner.

(5) A warrant for telecommunications interception may also be issued if there are grounds to suspect someone of aggravated pandering in which especially large benefit is sought and the offence has been committed in an especially methodical manner or the offence is one referred to in Chapter 20, Section 9(a), subsection 1, paragraph 3, of the Criminal Code. (1180/2014)

Chapter 10, Section 6 – Traffic data monitoring and its prerequisites

(1) *Traffic data monitoring* refers to the obtaining of identifying data regarding a message that has been sent from or received by a network address or terminal end device connected to a telecommunications network referred to in Section 3, the obtaining of location data regarding the network address or the terminal end device, or the temporary prevention of the use of the network address or terminal end device. *Identifying data* refers to data referred to in Section 2, paragraph 8, of the Act on the Protection of Privacy in Electronic Communications that can be connected to the subscriber or user and that is processed in telecommunications networks in order to transmit or distribute messages or keep messages available.

(2) A criminal investigation authority may be issued with a warrant for traffic data monitoring of a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect said person of:

(1) an offence for which the most severe punishment is imprisonment for at least four years;

(2) an offence committed with the use of the network address or terminal end device, for which the most severe punishment is imprisonment for at least two years;

(3) unauthorised use of an automatic data processing system, committed with the use of a network address or terminal end device;

(4) exploitation of a person subjected to the sex trade, solicitation of a child for sexual purposes or pandering;

(5) a narcotics offence;

(6) preparation of an offence committed with terrorist intent, training for the preparation of a terrorist offence or financing of a terrorist group;

(7) an aggravated customs offence;

(8) aggravated concealment of illegally obtained goods;

(9) preparation of the taking of a hostage; or

(10) preparation of aggravated robbery. (369/2015)

(3) Section 17 of the Act on the Exercise of Freedom of Speech in Mass Communications (460/2003) contains provisions on the transfer of identifying data concerning an electronic message.

- **preservation of computer data;**

  Provisions concerning the data retention order and period of validity of such order are set out in Chapter 8, Sections 24 and 25, of the Coercive Measures Act

Chapter 8, Section 24 – Data retention order

(1) If, before the search of data contained in a device, there is reason to assume that data which may be of significance for the clarification of the offence is deleted or is changed, an official with the power of arrest may issue a data retention order. Such an order requires a person holding or administering data, but not the suspect in an offence, to maintain the data unchanged. The order may also apply to data that can be assumed to be transmitted to a device or information system within the month following the issuing of the order. On request a written certificate of the order shall be given, detailing the data that is the object of the order.

(2) The provisions of subsection 1 also apply to data in a message transmitted by an information system that relates to the origin, destination, routing and size of the message as well as to the time, duration, nature and other corresponding factors of the transmission (*transmission information*). (1146/2013)

(3) A criminal investigation authority does not, on the basis of the retention order referred to in subsection 1, have the right to obtain information on the contents of the message, transmission information or other recorded information. If several service providers have participated in the transmission of the message referred to in subsection 2, a criminal investigation authority has the right to obtain the transmission information necessary to identify the service providers. (1146/2013).

Chapter 8, Section 25 – Period of validity of a data retention order

A data retention order is issued for three months at a time. The order may be renewed when required by the investigation of the offence. The order must be rescinded as soon as it is no longer necessary.

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

It is possible to obtain an order for stored traffic data also to cover a time period prior to the issuing of the warrant (Chapter 10, Section 9(3), of the Coercive Measures Act) - *The warrant for traffic data monitoring and for obtaining location data*

(3) The warrant may be issued and the decision may be made for at most one month at a time and the warrant or decision may be issued to extend also to the period prior to the issuing of the warrant or the taking of the decision, which may be longer than one month.

Provisions concerning stored content data are set out in Chapter 10, Section 4, of the Coercive Measures Act – *The obtaining of information other than through telecommunications interception*

(1) If it is probable that the message referred to in Section 3 and the identifying data connected with it is no longer available through telecommunications interception, the criminal investigation authority may be granted permission, notwithstanding the prohibition in Chapter 7, Section 4, and subject to the prerequisites set out in Section 3, to confiscate or copy them from a telecommunications operator or a corporate or association subscriber.

(2) If the obtaining of information for the determination of the content of a message is directed at a personal technical device that is suitable for sending and receiving a message and that is directly connected to a terminal end device, or it is directed at the connection between such personal technical device and a terminal end device, and the prerequisites set out in Section 3 are fulfilled, the criminal investigation authority may be issued with a warrant to obtain the information other than through telecommunications interception.

Under Section 25 of the Act on the Prosecution Service:

(1) A prosecutor has, regardless of secrecy provisions, the right to obtain without charge the information and documents necessary to carry out official duties from an authority and a corporation established for the performance of a public function unless the provision of such information or document to a prosecutor for use as evidence is prohibited or restricted by law.

(2) A prosecutor has, regardless of business, banking or insurance secrecy obligating a corporation member, an auditor, a board member or an employee, the right to obtain the information necessary to carry out official duties.

- **order for user information**

Relevant provisions are set out in Chapter 4, Section 3, of the Police Act (872/2011) - *Obtaining information from a private organisation or person*

(1) At the request of a commanding police officer, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members and employees of an organisation. The police have the same right to obtain information needed in a police investigation referred to in Chapter 6 if an important public or private interest so requires.

(2) In individual cases, the police have the right to obtain from a telecommunications operator and a corporate or association subscriber on request contact information about a network address that is not listed in a public directory or data identifying a network address or terminal end device if the information is needed to carry out police duties. Similarly, the police have the right to obtain postal address information from organisations engaged in postal services.

Especially in the area of ICT forensics, these points are important:

- Take over devices (such as mobile phones) with the security code open
- Obtain additional information about the target from the internet to find out the possible use of social media, cloud services, passwords etc. (Open Source Intelligence)
- Legal interception of data before an arrest, if possible
- In addition to the legal interception of data, it could be useful to use other means which are mentioned in the section 'Technical surveillance of a device' of the Coercive Measures Act
- Effective cooperation between the authorities (Police, Customs, Border Guard, FICORA's Cyber Security Centre, Defence Forces)
- Effective cooperation between the Police and the private sector (for example, the financial sector)
- International cooperation (for example, joint investigation teams).

5.2.2. Forensics and encryption

The acquisition of digital evidence is performed and the replicated data is analysed in the context of preliminary investigation of criminal offences. Digital evidence is used in the investigation of all kinds of crimes, including cybercrime. Remote searches, e.g. copying data from cloud drive, are possible in Finland. Cross-border remote searches have not yet been performed and legislative alignment is being sought.

The following problems related to encryption were mentioned:

- Increasing use of encryption; e.g. encryption of mobile phone memory;
- Strong encryption and strong passwords;
- Malware-related encryption;
- Network traffic encryption.

They are addressed in cybercrime investigation and ICT forensics by:

- Taking over devices (such as mobile phones) with the security code open
- Acquiring more computing power and better password libraries
- Investigating vulnerabilities of encryption methods
- In addition to data traffic interception, methods to monitor the use of live computers or mobile devices should be investigated.

In the field of decryption, the National Bureau of Investigation's Cybercrime Centre has started cooperation with the Finnish Defence Research Agency which is a specialist centre. The Cybercrime Centre has also carried out encryption-related information exchange with the Finnish Communications Regulatory Authority's National Cyber Security Centre.

Decryption of malware-related configuration files was carried out in cooperation with private companies only on a few occasions.

5.2.3. e-Evidence

E-evidence as such is not defined under Finnish legislation. The Code of Judicial Procedure regulates in a general manner the principle of free assessment of evidence by the Court. In accordance with *Chapter 17, Section 1* (732/2015) the court has to consider the weight of shown evidence. In this regard when law enforcement authorities or private sector companies are collecting, storing and transferring data, it has to be documented properly. Evidence gathering is the most crucial stage. In most cases software and tools commonly used by law enforcement authorities create time stamps, logs and protocols ensuring the integrity of the data. When private sector entities collect data, authentication of data might require the hearing of witnesses from another country and also there is a risk of non-compliance with police standards, or even with the law, during evidence gathering.

Currently e-evidence is transferred to prosecutors on different media: thumb drives, DVDs etc. A new case management system under development (AIPA) will enable electronic data transfer. It is a fact that e.g. a basic photo or screen capture on paper or pdf file entails a significant loss of data. In some cases the police downloaded websites with content and links and handed it over to the prosecutor on DVD. According to the Finnish authorities, this practice could be used more often. The current case management system (SAKARI) does not allow e-evidence to be transferred from police to prosecutor or from prosecutor to the court. The prosecutor or police takes care of sharing e-evidence with other parties involved in the trial, by taking necessary copies of the e-material. In many cases this vast material is not well organised. The manpower deployed to analyse e-evidence is not sufficient and protocols transferred from the police to prosecutor often contain ambiguous documents without a proper evidential theme. The lack of analyst resources is a major shortcoming.

Furthermore, prosecutors can be challenged by defence if evidence gathering is not documented properly. Network investigation tools (e.g. police malware) are often kept secret as long as possible and sometimes these techniques are not clearly explained to the judge deciding on coercive measures.

In the Finnish authorities' opinion, it is very difficult to exchange cyber intelligence in cross-border judicial cooperation due to lack of trust. Sometimes these investigative techniques have great commercial value (like zero date vulnerability). If evidence is collected by private companies, information on their investigative techniques is very limited. In the case of decisive evidence, poor documentation could significantly impair the value of evidence and lead to acquittal.

There are no specific admissibility rules for e-evidence.

5.3. Protection of Human Rights/Fundamental Freedoms

Legislative measures concerning cybercrime offences, including the implementation of international criminalisation obligations, have been carried out in a way that respects human rights and fundamental freedoms and the rule of law. The principle of proportionality and necessity in a democratic society have been taken into account. In line with the principle of legality the provisions are precise, exact and foreseeable.

Concerning the investigative measures, a balance between the protection of human rights and fundamental rights and the effectiveness of criminal investigation has to be found. Measures used in investigations and regulated in the Coercive Measures Act (806/2011) interfere with the use of human rights and fundamental freedoms. Deeply interfering measures are usually allowed only in investigations of serious offences.

There are legal remedies for the defendant. A district court decides on the use of some coercive measures (for example many covert (secret) coercive means). If the measure is ordered by a police official or in some rare cases by the prosecutor, the court must, at the request of the person concerned, decide whether the measure is to remain in force (for example, travel ban and seizure). Moreover, at the request of the person concerned, the court must reconsider whether the measure is to remain in force (for example, remand and seizure). All court decisions on coercive measures are covered by the possibility of making either an ordinary appeal or an extraordinary appeal (no time limit and an urgent hearing).

Coercive measures used in criminal investigations interfere with human rights and fundamental freedoms in ways depending on the nature of the measure in question. The Coercive Measures Act includes provisions on, for example, apprehension, arrest and remand (Chapters 2 and 3), restriction of contacts (Chapter 4; covers apprehended, arrested and remanded persons), travel ban (Chapter 5), seizure for security for the payment of a fine, of compensation or restitution or of an amount to be declared to be forfeited to the State (Chapter 6), seizure and copying of a document (Chapter 7), search (Chapter 8) and covert (secret) coercive means (telecommunications interception, traffic data monitoring, on-site interception, technical observation etc.).

Measures deeply interfering with human rights and fundamental freedoms are usually allowed only in investigations of serious offences and the district court decides on the use of these measures. The provisions on covert coercive means include some measure-tied extra conditions such as 'particularly important significance in the clarification of an offence' or 'necessary for the clarification of an offence'. Certain principles have to be taken into account in the decision-making concerning the use of all coercive measures. According to the principle of proportionality set out in Chapter 1, Section 2, of the Coercive Measures Act, coercive measures may be used only when they may be deemed justifiable with regard to the seriousness of the offence under investigation, the importance of clarifying the offence, the degree to which the use of coercive measures infringes on the rights of the suspect in the offence or others, and the other circumstances of the case. In accordance with Chapter 1, Section 3(1), of the Coercive Measures Act (principle of minimum intervention), the use of a coercive measure may not infringe on the rights of anyone beyond what is necessary in order to achieve the purpose for which it is used.

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

There are no specific jurisdiction rules for cybercrime offences. Chapter 1 of the Criminal Code is applicable to all offences. The starting point is that Finnish law applies to an offence committed in Finland (Section 1(1)). An offence is deemed to have been committed both where the criminal act was committed and where the consequence contained in the statutory definition of the offence became apparent (Section 10(1)). The Criminal Code of Finland is also applicable to some offences committed outside the territory. This covers for example offences connected with a Finnish vessel, offences directed at Finland, offences directed at Finns and offences committed by Finns (Section 2, 3, 5 and 6). When an offence has been committed outside Finland, in many cases the requirement of dual criminality has to be fulfilled.

5.4.2. Rules in the event of conflicts of jurisdiction and referral to Eurojust

Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of jurisdiction in criminal proceedings has been transposed into national law. However, no experience in terms of conflicts of jurisdiction has been reported.

If a crime has been committed outside Finland, arrangements for investigations are negotiated with the respective country. So far conflicts of jurisdiction have been solved by investigating cases in the country of residence of the perpetrator. Discussions through Eurojust also take place with regard to direct negotiations between judicial authorities in the States involved.

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

The Finnish Penal Code's provisions (Chapter 1) on jurisdiction date from 1996. Jurisdiction issues on cybercrime may be difficult to resolve in comparison to ordinary criminal cases.

Finland established jurisdiction in situations where the perpetrator or the victim of the crime is Finnish, but in such cases the prosecutor needs to find out whether the other State(s) is (are) handling the case and, secondly, receive from the authority of the State where the offence was committed a document containing the relevant provisions of that State. It may be difficult to establish the geographical location where the criminal act was committed. These situations should be envisaged and consideration should be given as to how to improve practice with a view to ensuring effective prosecution while also avoiding positive conflicts of jurisdiction.

The following problems arise while gathering evidence: If evidence rapidly changes place, the authorities investigating must very speedily be able to send requests to many different countries. The borderless nature of cyberspace gives rise to special challenges for law enforcement and judicial authorities. Electronic evidence, which nowadays is crucial to investigations and for judicial authorities, can be stored, changed and deleted in seconds from anywhere in the world. Consequently electronic evidence may also be moved, deleted and controlled or fragmented in several jurisdictions globally within seconds.

Moreover, the current procedures for mutual legal assistance (MLA) need to be faster and more effective. If data is moved to locations that are inaccessible to law enforcement or judicial authorities, this hinders the MLA mechanisms for cooperation since this mechanism is based on the principle of territoriality, i.e. the location of data. It has been noted that MLA procedures were in some cases too slow and cumbersome to be effective in cybercrime investigations. Sometimes it is not known from which country to request assistance (e. g. MLA is impossible in situations where the location of the data is completely unknown).

Thus it is important to find solutions to the questions regarding under which circumstances a State can investigate a cybercrime and exercise investigative measures and what kind of a connection is needed between the matter and the State investigating an offence. In particular, connecting factors other than the location of data (e.g. nationality or the habitual residence of the suspect or the location of the person affected by the crime) should be taken into account in this regard.

At present the physical location of data has become less relevant. It is not only a question of trans-border access to data, but also a question related to purely national measures. To reach effective solutions it is essential to develop common views. This work is beginning at EU level.

As regards 'clouds', it is being debated in Finland whether the police have the legal right to access an account or profile directly without the intervention of a foreign State and the consent of the holder in a situation where the investigator has the username and password, and the national legal requirements for *search of data contained in a device as a remote search* and *copying of data* (seizure) are met.

5.4.4. Perception of Finland with regard to the legal framework to combat cybercrime

The location of data has traditionally been a decisive factor regarding jurisdiction in cybercrimes. The importance of location has gradually diminished, especially e.g. through the fact that internet service providers (ISPs) are able to control where data is governed and where it is available. Another issue that has had an effect on this has been the fact that the location of data may be hard if not impossible to determine. All of this has resulted in a situation in which MLA is often requested from a country where data is governed instead of where the actual data is located. In addition to ISPs, a similar approach to tackling this issue should be broadened to cover natural persons and legal persons as well. Therefore, the location of data cannot be the only factor establishing a country's jurisdiction over data that can be randomly stored in different locations or be mirrored or moving all over the world in cyberspace.

The key characteristic of cloud computing is independence of location. According to the Council of Europe T-CY Committee's definition of cloud computing, the specific feature is that data tends not to be held on a specific device or in closed networks but is distributed over different services, providers, locations and often jurisdictions. Developing a common understanding of a borderless internet where the relevant factor is who is controlling the data and where it is controlled from (location/nationality of a data subject (suspect/accused)), instead of where the actual data may be located, is necessary in order to secure access to evidence located in cyberspace. A common framework needs to be developed, particularly in two situations: 1) when data is governed by the ISP from somewhere other than where the actual data is located and MLA is needed in order to obtain data from foreign jurisdictions and 2) when MLA is not applicable (location of data is unknown or unclear as is commonly the case in cloud systems) or is not a reasonable way to proceed in the matter (data can be obtained in another way).

The key question regarding this issue is that if a State has undisputed jurisdiction to investigate a certain crime, could its jurisdiction to access digital evidence be altered or even cease to exist depending on where data is at any given time located or how it is stored. Often the answer is negative because the question of the location of data cannot be rationally answered or the answer may be irrelevant due to the fact that the MLA cannot be successfully addressed to the country in which the data is located.

In order to achieve the best possible results countries have to ascertain that the instruments of mutual legal assistance as well as instruments based on mutual recognition are used to the full extent and effectively, and especially as swiftly as possible. There are many ways to improve cooperation e.g. strengthening cooperation between the 24/7 networks, including between judicial authorities, developing notification procedures or other subsequent control mechanisms for urgent situations as well as developing standardised electronically transmitted requests.

The question concerning direct trans-border cooperation with service providers is a delicate one. The element of control of the authorities in both States is important because of fundamental rights, data protection and sovereignty issues. Direct contacts may be accepted by both the requesting and requested States and common rules could be developed on that basis. These kinds of procedures may be appropriate as regards specific situations or data, e.g. subscriber data. Moreover, it is reasonable to develop lighter regimes for subscriber data, which is the most requested type of data for criminal proceedings and is not related to confidential communication like content data and traffic data.

The question of trans-border access to data is relevant only in cases where the criminal investigation authority has reason to believe that data acquisition involves it crossing a border. This starting point should be taken into account. When dealing with trans-border cases, a common legal framework is needed for situations where mutual legal assistance is not possible. It should be clarified when this kind of situation is at hand. At least situations of 'loss of location', where the electronic evidence is stored or even constantly moving somewhere in the 'cloud', should be covered. In situations like this trans-border access to data could be allowed if it is technically possible. The authority in question should follow the same procedures as in national cases.

It is essential to develop common views to reach effective solutions. Since the work has been conducted at EU level it is reasonable to avoid duplicated work. In many cases taking advantage of the work already done by the Council of Europe has been useful when discussing possible future EU actions. Currently an ad hoc Council of Europe group (Cloud Evidence Group) related to the Budapest Convention explores solutions for getting better access to electronic evidence, e.g. by drafting guidance notes or even by drafting an additional protocol.

5.5. Conclusions

- Finland ratified the Council of Europe Convention on Cybercrime in 2007. Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems were transposed into Finnish law.

- Finland has been a party to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse since 2011. Therefore, according to the Finnish authorities, Directive 2011/93/EU on combating the sexual abuse and the sexual exploitation of children and child pornography did not require legislative measures since the relevant legislation was in line with the Directive.

- Computer-related fraud and computer-related forgery are penalised by the Criminal Code.

- Encryption is considered to be a challenge. Network traffic encryption and whole hard drive encryption were mentioned as the areas where it has not yet been possible to deal effectively with the problem of encryption.

- E-evidence is not defined by national legislation and there are no special admissibility rules related to e-evidence. E-evidence is subject to the same rules of evidence as paper documents and is admissible under the Code of Judicial Procedure.

- General provisions regarding proceedings of investigations, coercive measures and police work are in place. However, there are no special provisions for investigation of cybercrime. The insufficiency of the current investigative measures to prosecute cybercrime seems to be the most striking problem in this field in Finland. Certain coercive measures, e.g. the interception of telecommunication, are limited to a group of specifically listed criminal offences. This list does not include any offences that fall under the scope of cybercrime, except for aggravated online fraud. Keeping in mind the special nature of cybercrime offences and their requirements for investigations, in the evaluators' view it would be useful to examine whether this list could be extended specifically to cybercrime offences or other ways could be found to enable these coercive measures to be used in such investigations. Furthermore, the introduction of specific investigative measures that are so far not covered by the existing catalogue might be examined.

- There are no specific jurisdiction rules for cybercrime offences and Chapter 1 of the Criminal Code is applicable to all offences. As regards jurisdiction in the clouds it is being debated in Finland whether the police have the legal right to access an account or profile directly without the intervention of a foreign State and the consent of the holder in a situation where the investigator has the username and password, and the national legal requirements for *search of data contained in a device as a remote search* and *copying of data* (seizure) are met. Cross-border remote searches have not yet been performed and legislative alignment is being sought.

- In the opinion of the evaluators the difficulties mentioned by the Finnish authorities with regard to jurisdiction and collection of e-evidence from the cloud are similar to those faced by most other Member States. Thus there is the need for a common solution at EU level. Therefore, the EU institutions should be encouraged to find solutions to legal problems regarding jurisdiction and collection of e-evidence from the cloud.

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1. Nature of cyber attacks

The following cyber attacks were investigated in Finland:

- DDos attacks against governmental institutions and banks;
- Malware such as Jsocket and Dridex targeting private companies and individuals. In most cases mobile devices or individuals were attacked;
- Ransomware: Cryptolocker, Cryptowall, Locky and malware against mobile devices;
- Computer intrusions also combined with extortion, targeting private companies;
- Card not present frauds: using stolen credit card data of individuals and private companies;
- Computer related frauds, like tampering data in order to distort the outcome of data processing or utilization of vulnerabilities in websites in order to gain financial benefit;
- Phishing campaigns: targeting individuals in order to gather personal information, online bank credentials or credit card information;
- CEO frauds, targeting private companies, sometimes by using compromised email accounts.

They were conducted by both foreign and domestic individuals or organised crime groups (OCGs). In most cases investigations involved cooperation with Europol and/or the FBI .

6.1.2. Mechanism to respond to cyber attacks

There is no multidisciplinary documented mechanism involving several governmental agencies and/or private entities. However, all relevant parties have taken part in many cyber exercises and there are several working groups in which these issues are discussed. There are two main actors responsible for tackling serious cyber attacks (crimes): the police and the Cyber Security Centre. According to the Finnish authorities, cooperation between those entities works very well.

Under the Information Society Code (Section 275), a telecoms operator must notify FICORA of significant information security violations or threats to information security in the services. The operator must also notify FICORA of the estimated duration and consequences of information security violations and threats, corrective measures taken as well as measures undertaken to prevent the reoccurrence of such violations.

The measures applicable to the notification of personal data breaches are regulated in European Commission Regulation 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications. The Regulation harmonises procedures on how to notify FICORA and users of personal data breaches and the content of these notifications. The Regulation is directly applicable legislation, hence it applies to all telecoms operators as it stands. Notification of other information security violations is regulated in FICORA's Regulation 66 on disturbances in telecommunications services.

In practice, all notifications of security incidents are done by using the form provided for reporting in Annex 2 to Regulation 66 (Telecoms operator's notification of information security incident). The notification can also be made by email. The text can be free-form as long as it provides the same information that is included in the notification form. If there is reason to suspect that the information security of the message delivery system used for submitting the notification has been violated, or the situation calls for immediate measures from FICORA, the first notification should be made immediately by telephone based on the existing information. In long-term cases, the telecoms operator must keep FICORA up-to-date on how the situation develops. An electronically submitted notification that can be produced in a written and readable form is considered a written notification.

Regulation 7 on the obligation of identification service providers and certification authorities providing qualified certificates to the public to submit notifications to FICORA requires such entities to submit notifications. According to the law, the actors must, before starting operations, submit a notification to FICORA as well as the information on the basis of which FICORA assesses the reliability and the information security of the operations.

The actors must also notify FICORA of significant changes in the operations and if the operations are discontinued. In addition, the actors must provide FICORA with an annual report detailing the extent of the operations as well as threats to the information security of the service.

Identification service providers and certification authorities providing qualified certificates must notify FICORA of any significant threats or disturbances concerning the information security of their services and of the measures taken in response. If necessary, FICORA may request a service provider to give further details of the changes and disturbances. FICORA can also order a service provider to fix the detected defects.

FICORA has issued further provisions on the contents and submission of notifications of operational changes, annual reports and disturbance notifications by a regulation and the related explanatory notes. FICORA produces information on the current information security situation for players critical to the security of supply and provides a common information exchange channel for these players.

FICORA maintains bidirectional mailing lists for the providers of services critical to the security of supply. The mailing lists provide the players with a forum for confidential discussions on issues related to information security. Also, FICORA's NCSC-FI contributes to the lists by sending information security notices on topical issues. The notices are of interest to all the companies critical to the security of supply, in particular to the group of companies for which the mailing list in question is intended.

Mobile access to internet is widely used in Finland and data retention information is stored only for a few months. Without the port number used to access mobile internet it is not possible to target the suspect because there could be hundreds of users with the same IP address.

6.2. Actions against child pornography and sexual abuse online

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

Finland started in 2015 a project to establish a national database for child abuse material (CAM). This database will also be used for victim identification.

The Finnish authorities stated that no specific measures have been introduced to avoid re-victimisation in the event of images/videos not being deleted.

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

The Cybercrime Centre maintains and updates frequently the access blocking list of websites including CAM. The blocking list is provided so that ISPs can stop their customers for using those websites. It was reported that not a single ISP was using the list.

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

The Association of Finnish Travel Agents (SMAL) has been active since the 1990s. It has produced a leaflet called 'The dark side of tourism' (title freely translated) and has updated that leaflet. The biggest travel agencies belonging to SMAL have committed themselves to the Code regulation developed by ECPAT, international travel agencies and UNICEF. With the help of this Code regulation travel agencies train their personnel and give instructions to travellers for the purpose of preventing this kind of tourism. The travel agencies committed to the Code regulation are responsible for almost 85 per cent of foreign flight package tours.

The Police has the 'Net tip' system.

Finland has been involved in international Safer Internet programmes (co-funded by the European Commission) for over a decade. From 2012 the Department for Media Education and Audiovisual Media in the National Audiovisual Institute has coordinated the Finnish Safer Internet Centre (FISIC) in close cooperation with its consortium members from the Mannerheim League of Child Welfare and Save the Children Finland. The Finnish Safer Internet Centre is a member of the international Insafe network.

FISIC exists to promote safer and better use of internet and mobile technologies among children and young people. FISIC consists of an awareness centre, helpline services and hotline work. The objective of the awareness centre is to raise citizens' awareness and increase competences in creating better and safer internet and other digital environments. The centre organises awareness-raising campaigns and develops materials and toolkits for dissemination. The main dissemination portal for professionals working with children and young people is the Media Literacy School (www.mediataitokoulu.fi) which offers information, exercises and a research database related to media and information literacy (MIL) as well as internet safety. Media Literacy Week (MLW) is held annually as a part of FISIC's awareness work in order to promote the national goals of MIL and media education.

The main objective of the helpline is to answer online questions and telephone calls from children and parents related to children's use of online technologies. Parents and children can obtain advice on how to deal with harmful contact (grooming), harmful conduct (cyberbullying), and harmful content, and uncomfortable or scary experiences of using online technologies.

Save the Children Finland maintains a hotline, Nettivihje, which offers the public a way to report potential illegal online content in Finland, especially in relation to child sexual abuse material (CSAM). Nettivihje is a member of the INHOPE (International Association of Internet Hotlines) network.

Save the Children Finland is also working to help sex offenders. Its campaign calls for responsibility to be taken by sex offenders.

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

The Cybercrime Centre's CSE team works nationally and internationally. The team consists of three police officers. Their role is to act as a point of contact nationally and internationally. They cooperate with international partners and analyse cases and proposed international projects. They take initial investigative actions in order to find more information about possible Finnish offenders and to see which police district would be the most suitable to take on the case.

All police districts investigate child sexual exploitation cases all the time in their violent and sexual crimes units. Special training is provided for those investigators that work with children.

According to the Finnish Act on preventing measures of child pornography (*Laki lapsipornografian levittämisen estotoimista),* internet service providers can block access to websites containing child pornography. The Police maintain a list of websites with this kind of content. The list is given to the internet operators so they can use it to block access to these pages from their users. The private sector can choose the methods used in possible filtering/blocking of access. The internet service providers are required to remove any child pornography material that is found in web pages hosted by them (Act on provision of information society services (458/2002), Section 15).

According to the Information Society Code (917/2014)

Section 185

Order to disable access to information

Upon request from a public prosecutor or a person in charge of inquiries or on application by a party whose right the matter concerns, a court may order the information society service provider referred to in section 184 to disable access to the information stored by it if the information is clearly such that keeping its content available to the public or its transmission is prescribed punishable or as a basis for civil liability. The court shall urgently process the application. The application cannot be approved without an opportunity for the service provider and the content provider to be consulted except if the consultation cannot be arranged as quickly as the urgency of the matter necessarily requires. A court order must also be imposed on the content provider. If the content provider is not known, the court may order the information society service provider to take care of notification. An order ceases to be in effect unless charges are raised for an offence based on the content or transmission of information referred to in the order or, when concerning a liability, action is brought within three months of issuing the order. On request by a public prosecutor, by an injured party or by an interested party within the time limit referred to above, the court may extend this time limit by a maximum of three months.

The information society service provider and the content provider have the right to apply for reversal of the order in the court where the order was issued. When dealing with a matter concerning reversal of the order, the provisions of Chapter 8 of the Code of Judicial Procedure shall be observed. However, the court takes care of the necessary procedures to hear a public prosecutor. The reversal must be applied for within 14 days of the date when the applicant was notified of the order. The information must not be made available again when the hearing of the case concerning the reversal is pending unless otherwise ordered by the court dealing with the case. A public prosecutor also has the right to appeal the decision that reversed the order.

When the server is located outside Finland this information is passed to the competent authority through international channels, usually with a SIENA message.

6.3. Online card fraud

6.3.1. Online reporting

If a citizen notices a fraudulent transaction on their credit card invoice, the bank that issued the card is contacted in the first place. Depending on the case, the bank may require the cardholder to report the case to the police. If the bank recognised that the transaction was clearly such that the cardholder had no connection to it, it pays the money back to the cardholder and covers the losses. If the case is unclear, most banks usually require the customer to report the case to the police for two reasons: firstly, so that the police can investigate it; secondly, many banks do not know whether their customer is truthful and they want the police to be involved in the case to make sure of that.

The Finnish police claimed to have good cooperation with Finnish banks. In regular meetings it is discussed what kinds of cases banks should report to the police. The general understanding is that Card Not Present cases and online fraudulent transactions are so usual and frequent that if they were all reported to the police for investigation, it would suffocate the police investigation unit resources. This kind of case does not usually have any links to Finland other than the cardholder, and fraudulent sums are so small that most countries would not answer an MLA request if one was sent, so the tactic is to gather larger cases and prevent fraud phenomena by exchanging information so that large-scale criminal attempts stop at the early stages. This is why not all cases are reported to the police. However, if requested, the banks would gladly report all cases of fraud to the police, but in the spirit of mutual cooperation and limited resources, this matter is under constant discussion.

Citizens themselves, however, report cases to the police frequently. This can easily be done with a web form. Regrettably most reports lack information, making cases impossible to investigate.

6.3.2. Role of the private sector

Finnish police and all card-issuing Finnish banks form a group called Card Risk Management (CRM) which meets six times a year and shares this kind of information. In urgent cases this trusted network will start an email discussion or call each other.

Recommendations to use sophisticated geo-blocking or warning systems are normal. The police and the banking sector exchange information on modi operandi of crimes in order to adjust the payment infrastructure to make it more secure.

Authorisation of online transactions also requires the cooperation of the retail sector. Some merchants require three-factor authentication (using bank credentials) when making purchases with a credit card. This is however always the decision of the retail company. Banks recommend their own Verified By Visa and MasterCard Secure Code products, but it is up to the retail company to decide whether to use them. The police do not advertise these services in particular.

In the NBI there are no specific personnel dedicated to this area of responsibility. It has been considered a shared responsibility among all officers in their respective areas. It is considered very important and especially management-level personnel have put a lot of effort and time into building good working relationships with private sector entities.

6.4. Conclusions

- There is no multidisciplinary mechanism to respond to cybercrime involving governmental agencies and private entities. However, it was reported that all relevant parties have taken part in many cyber exercises and there are several working groups in which these issues are discussed. The main actors responsible for tackling serious cyber attacks (crimes) are the police and the Cyber Security Centre/ FICORA.

- In the evaluators' view the reporting mechanism related to cybercrime is limited and not mandatory. As a consequence the police are not informed about cyber attacks unless they detects them themselves. When the Cyber Security Centre comes across issues that may be a criminal offence it will advise the citizen to lodge a police report. Therefore, it is recommended that the introduction of a more mandatory reporting system, particularly for serious crimes, be actively considered (e.g. critical infrastructures, attacks on banks).

- The Cyber Security Centre/ FICORA sends out alerts to respective stakeholders. At the time of the on-site visit an MoU was being finalised with the police. After the on-site visit the evaluation team was informed that the MoU on cooperation between FICORA and the Police was singed in October 2016.[9]

- The Finnish authorities reported that Finland had been rated successfully in Microsoft's cyber trust rating, which was attributed to two factors: (1) the success of FICORA's use of automated notification tools and (2) the size of the country, allowing for ease of communication between key players. In the opinion of the evaluators, formalising this rapport will ensure the sustainability of existing relationships.

[9] The evaluation team did not study the content of the MoU.

- In the field of fighting child pornography the police reported that they could not keep up with CSE investigations that were being received from abroad and, therefore, rarely generated their own cases. The CAM database is still being set up. The Finnish NBI is liaising with Denmark in order to set up a database.

- The evaluation team recognised that the Cybercrime Centre maintains and updates a list of websites containing CAM. This list is provided to ISPs with the intention of preventing their customers from accessing such websites. According to the Finnish Act on preventing measures of child pornography (*Laki lapsipornografian levittämisen estotoimista)*, internet service providers can block access to websites containing child pornography. However, it was reported that not a single ISP is using the list. Therefore, in the opinion of the evaluators Finland should engage in discussions with ISPs in order to encourage them to refer to this list.

- The evaluation team welcomes the ongoing plans to establishing a hash-database for CAM. It is recommended that the resources required to ensure the long-term sustainability of this initiative be identified and put in place. This applies especially as the photographs concerned need to be looked through often by police investigators who have not received special training. Regarding cooperation with the private sector, the size of the country and existing relationship between key stakeholders have allowed for the creation of a good working platform also at local level. The establishment of the eCIP network is just one of the examples that was noted by the evaluating team during the on-site visit.

- The evaluation team noted that fighting against online fraud appears to be divided into small individual cases. There is no clear view of the bigger picture of these types of case. In the case of some crimes, the opening investigation procedure depends on the victim's decision to submitting a complaint. Such actions may seem to be quite ineffective.

- Apart from cybercrime, a possible increase in specialisation could also lead to the establishment of a fraud unit within the prosecution authorities, as this wish was expressed by participants from the judiciary.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

There are no specific formal requirements for cooperation between national authorities and Eurojust.

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

Finland considers the work of Europol/EC3 and Eurojust very valuable in the fight against cybercrime due to its borderless nature. European agencies play a key role in bringing Member States and also third countries together by facilitating strategic and operational meetings and offering their other valuable services in the fight against cybercrime.

Europol has analysed massive amounts of IP addresses, chats, log files, etc. EC3 has found links between perpetrators and identified criminal groups and networks. Eurojust has coordinated the work of JITs, coordinated and supported action days and granted funding in order to secure the admissibility of e-evidence throughout the criminal procedure. Europol and Eurojust meetings increase cross-border trust between investigating authorities and prosecutors. Mutual trust is a crucial element for intelligence exchange and paramount for efficient judicial cooperation. Eurojust-supported face-to-face coordination meetings have proved to be important in achieving trust.

Parallel investigations are often at different phases, e.g. in JIT Mozart Finland and the Netherlands had to wait to press charges and avoid giving press releases in order not to compromise investigations in other Member States. As the crime was continuing and new victims came out every day, postponing actions was a difficult decision, but it was achieved during Eurojust coordination meetings.

The Cybercrime Centre works in close cooperation with Europol/EC3 and Eurojust. With ENISA there is very little cooperation. Also police districts have some cooperation with EC3. Finland believes that it could improve cooperation by sending more information about all cybercrime cases automatically to EC3. This would increase the knowledge base of EC3 and in return Finland would obtain information about domestic cases connected to other European cases.

The Nordic Forum for cybercrime cooperation has been established and heads of cybercrime centres meet twice a year and discuss common goals, EMPACT activities, form common opinions, share best practices and exchange expertise.

According to the Finnish authorities, EC3 should increase its investment in analytical resources or at least maintain the current level. Both the Finnish LEA and Finnish prosecution would benefit from Finnish police having their own liaison officer in the Joint Cybercrime Action Taskforce (J-CAT). The US and UK authorities are feeding EC3 with their own investigations. The J-CAT board, on which EU Member States are not well represented, is giving US and UK investigations high priority. There is a risk of uneven support for cases investigated by smaller Member States. A Finnish J-CAT liaison officer would improve information exchange to/from EC3 and between EC3 and Eurojust's national desk.

The Finnish judiciary would benefit from a Cyber Secretariat hosting a dedicated network in the field of cybercrime. The Secretariat would penetrate horizontally a wide field of different crime types supporting prosecutors with up-to-date information and expertise. A Cyber Secretariat/Unit would mean there would be permanent in-house cyber expertise at Eurojust. Currently, expertise relies too much on people working at national desks with a certain interest in cyber issues and there are too few of them.

Further simplified procedures for applying JIT funding and more resources allocated for a Eurojust coordination role are paramount for cyber investigations/prosecutions as they are by nature in many cases multilateral and even cross-continental investigations/prosecutions involving actors from the public and private sector.

Finland has been involved in three JITs in relation to cybercrime. Eurojust has facilitated coordination meetings for JIT Mozart (Austrian lead with regard to banking malware) and JIT Eurymus (Finnish lead with regard to hacking, swatting, etc.). One JIT did not request Eurojust support. In these two multilateral cases one of the best practices found was to organise two-day meetings in The Hague starting with an operational information exchange and analysis at Europol followed by judicial-level coordination at Eurojust.

Operation Blackshades was a multinational Eurojust coordinated operation in which more than ten countries including non-EU countries participated. In this operation, law enforcement agencies targeted purchasers of Blackshades software. During the joint action days hundreds of house searches and dozens of arrests were made on the premises of purchasers of the malware in question.

In the area of payment card fraud, Finland had many successful cases involving Europol/Eurojust coordination. As an example: in 2011 a skimming group was arrested in Finland, and due to the information gathered in Finland and sent to Europol, Germany and Romania initiated OP Pandora-Storm to dismantle the whole OCG. The process took two years and involved the cooperation of many EU Member States, but the result was that the higher leaders of the organisation were also arrested.

7.1.3. Operational performance of JITs and cyber patrols

In the opinion of the Finnish authorities, JITs are very powerful and useful tools for cooperation when participating countries have common interests and the objective of cooperation is clear enough. However, the fact that the US authorities cannot participate in JITs as a member is very unfortunate as the US authorities is a very important counterpart in almost every significant investigation.

Some examples of good cooperation based on JITs was given. Finland was a member of JIT Mozart comprising six countries. JIT Mozart was established in 2013 to investigate online bank fraud. During three years of active investigation the JIT resulted in a number of arrests of fraudsters, mule handlers and money mules in several countries - both EU and non-EU countries. In this particular investigation EC3 proved to be an excellent organisation in terms of analysis and coordination. With the help of EC3 the national investigation team was able to concentrate on national investigation while EC3 collected information in order to build up the big picture, identified targets and revealed intelligence gaps. Establishing a joint investigation team allowed tasks to be shared and resources to be used in a more efficient way. The Finnish authorities were able to use existing contacts very efficiently for the benefit of the whole JIT. The amount of information and evidence collected was massive, but because of the JIT sharing them was easy. JIT Mozart expired in March 2016 after the main targets were taken down and the JIT was no longer necessary.

JIT Eurymus, targeting a Europe-based hacker team, though pending at the time of the on-site visit, expired in September 2016. EC3 has also been involved with this JIT, providing assistance with analysis and coordination.

Special JIT funding was allocated by Eurojust to JIT MOZART cooperation. For JIT Eurymus special funding has not been necessary.

Many police districts have a visual presence in cyberspace**.** Helsinki police district is especially good at this. It has a full-time team of officers dedicated to this role. Having an online presence is part of the police's preventive work. Virtual police officers also contribute to solving crime and disseminating information about important current issues. Virtual police officers can discuss important issues in a more light-hearted manner. One of the objectives of this is to make the police appear less intimidating to the public and to encourage people to contact the police. However, virtual police officers cannot discuss confidential or private information.

7.2. Cooperation between the Finnish authorities and Interpol

Interpol channels were used in order to find a POC from non-EU countries with which Finland has not established any contacts. Subsequently Interpol's help was requested to organise an operational meeting with non-EU countries.

7.3. Cooperation with third States

Finland has no specific policy with respect to third countries. Finland has been actively seeking cooperation especially with neighbouring countries and also with China and USA. Liaison Bureaus of third countries in Europol have been useful in establishing contacts with certain third countries with which Finland does not have existing contacts, such as Colombia and Australia. In certain cases, as in Operation Blackshades two years ago, Eurojust played a significant role in judicial coordination between third countries such as the US and Canada. From the Finnish point of view the most important added value from Europol/Eurojust is their ability to find POCs and establish contacts.

In multilateral cases it has been possible for one Member State to issue an MLA request to a third country and then share the information obtained with other JIT members.

7.4. Cooperation with the private sector

Key tactics to overcome obstacles to cross-border cooperation, specifically regarding online card fraud, are the following:

1. Participating actively in Europol EMPACT projects and meetings;
2. Initiating cross-border investigations when feasible;
3. Sending information on ongoing cases to Europol to enable an effective analysis of European OCGs.

The Finnish authorities invoked the need to make cross-border cooperation more effective. MLA instruments, the EJN and Eurojust are tools which are at the prosecutors´ disposal. Also swift cooperation via informal channels, such as emails or telephone, have proved successful in overcoming some of the challenges identified and have helped in preparing formal requests.

The direct records disclosure services by private companies to the law enforcement community are conducted on a voluntary basis and due regard of sovereignty. Some of them provide their services directly from their headquarters, some via their regional representatives. This cooperation started in 2006 and Finland has not faced any notable obstacles. If a private company does not provide such services, the MLA procedure applies.

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

The Budapest Convention is used to provide mutual legal assistance for cybercrime.
Furthermore, there are provisions on legal assistance in the Act on International Legal Assistance in Criminal Matters, which is a general legal framework for Finland to execute and issue requests for mutual legal assistance without e.g. a reciprocity requirement. In addition to that, Finland has signed the most relevant MLA conventions, such as the European Convention on Mutual Assistance in Criminal Matters and its two protocols.

Double criminality is not required for executing MLA requests in Finland, except when coercive measures are to be applied. Also in cases when data retention is requested, the double criminality principle does not apply (Section 15 of the Act on International Legal Assistance in Criminal Matters). However, if double criminality is required, it is applied *in abstracto*.

Currently Finland is in the progress of implementing Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, which amends the system of mutual legal assistance between EU Member States. When the implementation legislation comes into force, it will no longer be possible for police authorities to issue an EIO without validation by a judicial authority. The intention is that prosecutors will be designated as validating authorities. For purposes of transmission, the intention is to apply a flexible system so that both the issuing and validating authorities may be contacted.

For a pre-trial stage MLA request to Finland from other EU Member States the National Bureau of Investigation is the central contact point (see EJN Atlas). The International Affairs unit of the agency decides on the execution of a request and directs the request to an investigative entity unless the International Affairs unit can process the matter itself.

MLA requests to Finland from countries outside the EU are sent to the Ministry of Justice as the central authority (Unit for International Judicial Administration). Urgent requests via Interpol channels are accepted in accordance with the European Convention on Mutual Assistance in Criminal Matters (Article 15, point 5).

The LEA and prosecutors have an obligation to act in close cooperation and the LEA has to comply with orders and instructions by the prosecutor as provided for in Chapter 5 of the Preliminary Investigation Act.

MLA requests from Finland to other EU Member States are sent directly. The National Bureau of Investigation is the national central contact point for the investigation authorities. The requests are checked by the NBI's International Affairs unit before they are translated and sent to the country concerned. Although the email address and fax number of an addressee are provided in the EJN Atlas, a problem is that the Finnish national data protection regulation is stricter than the available technical possibilities for fast communication (excluding Interpol I 24/7 and Europol Siena).

The prosecution authorities directly contact judicial authorities in other EU Member States. The EJN and Eurojust are contacted when assistance is needed. Technically speaking, the courts are also competent authorities, but they very rarely exercise the right to request assistance.

The requests frequently concern the services of Facebook, Microsoft, Google and Skype as well as Kik. Other companies occur only randomly. Therefore, the majority of MLA requests are addressed to the United States and Canada. Consequently, Finnish requests are sent via the central authority – the Ministry of Justice. In the reverse case, there are only a few companies in Finland of international significance in this particular context which generate MLA requests from other States. The number of requests is still moderate.

There are no statistics on cybercrime-related MLA requests. Requests in both directions, transmitted through the Ministry of Justice, are not catalogued by the type of offence, so this information cannot be provided.

There are no particular legal conditions to be fulfilled to send MLA requests. However, as cybercrime is quite technical, the rentity has to be clearly identifiable and traceable. In some circumstances this may require technical details of the context as a whole. As an issuing State Finland may in principle request the same investigation measures as in domestic situations.

In those situations where Finland is a requesting State, it complies with EU/international instruments on legal assistance and conditions set by the executing State, e.g. following the practice and recommendations of the US Department of Justice so that it is possible to contact directly the service provider located there if only subscriber data is required. When Finland is an executing State, requests should be sent via the competent authorities (where other than publicly available electronic data is requested). Where coercive measures are requested (such as traffic or content data), in principle the same procedure applies as in domestic cases, which means that a court order has to be obtained, if required in a similar domestic case. In general Finland supports exploring possibilities to apply more simple procedures where only subscriber information is requested.

As the United States is the most frequently occurring country concerning Finnish requests, the FBI Legal Attaché Office is very important for consultation purposes. Sometimes the US Department of Justice case handler is consulted directly, for instance, when determining if the available information is sufficient enough to obtain the required information.

Prosecutors use pre-MLA consultations. Some countries like the USA have asked to receive a draft of the MLA request in order to advise whether changes/additions need to be made to the request before issuing it officially. The most frequently used channel by prosecutors is the Eurojust national desk. The EJN contact point network is also available.

Finland has bilateral crime prevention agreements with a number of countries. The most frequently applied is the Agreement on Cooperation in Crime Prevention between the Government of the Republic of Finland and the Government of Estonia. There are no statistics available as to how often the agreement has been applied in cybercrime cases. Cooperation with Lithuania, Latvia and Sweden also works quite smoothly.

MLA is the one and only instrument to be used in evidence gathering in cases involving countries outside the EU. If there is no connection to the country in question, Finland tries to speed up the process by sending the MLA or an early warning in advance.

7.5.2. Mutual recognition instruments

There are no statistics available as to what extent mutual recognition instruments have been used in relation to cybercrime.

The National Bureau of Investigation has used European Arrest Warrant EAW's in two separate cases within past seven years. Total of three individuals have been arrested and extradited to Finland for investigation, prosecution and trial.

Mutual legal assistance request are used frequently in the cybercrime investigations and NBI has joined several Joint Investigation Teams in cybercrime investigations.

7.5.3. Surrender/Extradition

Every offence for which the maximum penalty is at least one year of imprisonment is subject to extradition and surrender in Finland.

The Ministry of Justice is the competent authority for sending and receiving extradition requests from third countries. An extradition request is only sent at the initiative of the prosecutor of the case. Extradition is always requested and decided by the Ministry of Justice. No method of transmission is excluded; requests may be sent directly, via diplomatic channels or through Interpol.

The competent authority to issue an EAW is the prosecutor of the case. EAW requests should be sent to prosecutors of the Helsinki prosecution office. The EAW and Nordic Arrest Warrant procedure as regards cybercrime is exactly the same as for any other crime where surrender is possible. The same applies to extradition. Provisional arrest is possible.

Extradition or surrender procedures in Finland differ depending on the requesting country. The legal framework that applies to the extradition/surrender depends whether the requesting country is one of the EU Member or associate States that has implemented the framework decision on the European arrest warrant or another Nordic State. The competent authority in these cases is the district court of Helsinki whereas the Ministry of Justice is the competent authority in all other extradition cases. With this division, cases are subject to different processes, which has an effect on the legislation applied and may also affect the length and outcome of the extradition/surrender process.

The urgency of the extradition or surrender request has no effect on the extradition procedure itself, since there is no special 'urgent extradition/surrender procedure' in Finnish legislation. However, search and apprehension of the person sought for extradition/surrender are dealt with on a case-by-case basis and may be resourced and executed in a manner that facilitates as urgent a procedure as possible.

There are no statistics available regarding the average response time in extraditions.
Surrender based on a European or Nordic arrest warrant is relatively fast. The procedure takes approx. 20 days on average when the person to be surrendered agrees to be surrendered and approx. 30 when he/she does not.

With regard to 'response time', as soon as a request is provided in the form of an alert in the Schengen Information System or a Red Notice in INTERPOL's database, the police may take action immediately. Should the extradition request be delivered to the Ministry of Justice, or to a prosecutor where applicable, they will request the police to take appropriate measures without any significant delay.
The same rules apply as to any other extradition, consequently the average response time would be the same, that is two months at the most.

Only three cases exist which were based on cybercrime offences, all of them extradited to the US on the basis of the bilateral extradition treaty. Two of the cases dealt with trafficking in contraband cigarettes through the internet and one was a conspiracy to commit violations of the computer fraud and abuse act (identity theft).

Regarding the Nordic countries there is a Nordic Arrest Warrant arrangement which is also used for surrender.

7.6. Conclusions

- Due to the size of the Finnish Prosecution Service, the operational role of the Office of Prosecutor General and the informal method of internal cooperation, it seems that the use of and cooperation with Eurojust is available for prosecutors in need of Eurojust assistance in a satisfactory manner.

- The Cybercrime Centre closely cooperates with Europol/EC3 whereas with ENISA very little cooperation was reported.

- Finland considers the work of Europol/EC3 and Eurojust very valuable in the fight against cybercrime due to its borderless nature. European agencies play a key role in bringing Member States and also third countries together by facilitating strategic and operational meetings and offering their other valuable services in the fight against cybercrime.

- The Finnish authorities frequently make use of JITs. It seems that Finnish experience of JIT cooperation is very positive and has given good operational results in many investigations. This trust in the tool is based on positive experiences with JITs in the past as well as on low administrative hurdles for its establishment. In the evaluators' view this practice can set a good example for other Member States.

- The ongoing work on improving and maintaining good relations with third States by the National Bureau of Investigation seems impressive. The quite informal way of cooperating is most likely a very effective basis for successful international cooperation.

- Furthermore, the evaluators appreciated the Finnish approach towards foreign ISPs specifically from the US. A single point of contact was established in order to communicate with the representatives of the providers. The competent post-holder also maintains good relationships with the relevant personnel of the providers, which leads to a spirit of mutual trust and thus results in providing voluntary cooperation.

- The retention of data requested from service providers pending MLA is currently capped at 90 days though, according to the Finnish authorities, it should be increased to 180 days. Moreover, a mechanism whereby the availability of data is established prior to formulating MLA requests could be set up. This would avoid the situation of drawing up MLAs in relation to non-existent data. Standard templates for requests would also be helpful.

- The evaluation team noted a very good example of international cooperation in criminal matters among the Nordic States. Particular examples are the Nordic Arrest Warrant, sharing of liaison officers and the Nordic Training Platform.

- Also, cooperation with countries from the Baltic region such as Estonia, Latvia, Lithuania, and Sweden is exemplary. The first meeting of representatives of this group took place in September 2016. Cooperation with the neighbouring countries is, in the opinion of the evaluators, an example of best practice.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

Judges

The Ministry of Justice offers training on cybercrime to judges. During the past few years approximately 150 judges have been trained on the subject. There are plans to make the training of judges and judiciary personnel more systematic. A new independent body, the Board for Training of Judges, will be set up to plan the training. The training will be organised in phases. A one-year basic training programme will be followed by a learning-while-working training programme. Participants in this programme will be selected nationwide. Lawyers with at least three years of applicable work experience can in the future apply for a three-year assistant judgeship. An assistant judge is appointed for a fixed term entailing a considerable amount of training.

Prosecutors

Training of prosecutors in Finland is divided into starter courses organised for new prosecutors. It lasts six months, mostly provided online with two training days in the Prosecutor Academy. It aims at providing a basic knowledge of prosecutors' work.

For a prosecutor with 1-3 years of experience courses are organised partly online with altogether 15 training days (3 days x 5 times) at the Prosecutor Academy. They aim to strengthen and deepen the skills of prosecutors generally, and do not offer training in specific offences.

The International Association of Prosecutors (IAP) provides for its members cybercrime-related digital (web) training. The Office of the Prosecutor General, the Finnish Association of Prosecutors and some individual prosecutors are members of the IAP. Under the IAP's umbrella there is the e-crime network GPEN, which – among other activities – arranges e-crime training courses, presentations and webinars. Some Finnish prosecutors have participated in these webinars.

In 2010-2016 the following cyber-related training took place:

- ABC course in ICT – basic information, three 2-day courses organised (2010, 2011, 2012)
    - Trainers from NBI, PGO
    - Forensics, obtaining evidence, basic problems in CAM, defamation, online fraud, credit card fraud
- Freedom of speech related crimes online, 2-day course (2011)
    - Trainers from NBI, PGO, district prosecution
    - Defamation, right to protect source of information, threats online, virtual police, coercive measures
- Crimes against copyright, one-day course (2013)
    - Trainers from NBI, district prosecutor, district judge, Anti-Piracy Centre, defence lawyer
    - Forensics, victims' demands, pirate bay**,** peer networks
- Credit card fraud, half-day course (2014)
    - Trainers from NBI, experts from 'Nets Ltd'
- CAM, two 3-day courses (2014, 2015)
    - Trainers from KBI, local police, district prosecution, Police Academy
    - Offences, categories of images, MLA, networks' characteristics, pre-trial cooperation, cases of PG's sole competence, methods of spreading content, investigation thereof, hash numbers, quality of technical part of the protocol, punishments for various categories of images, using police as witness, forfeiture of instrument of crime

- Violations of the population registration law, one 2-day course (2015)
    - Trainers from prosecution, police, data protection ombudsman's office, city of Tampere
    - Content of the offences, registrar's activity and responsibility, data protection ombudsman's role
- Regional training in district offices (when they so wish), 3-hour basic training

In 2017 a basic cyber course for all prosecutors is to be organised followed by a case-based, more advanced course.

The police

The Police University College of Finland has been providing cybercrime-related courses in its curricula roughly since the beginning of the 2000s. Courses have covered a broad area of topics related to cybercrime prevention, such as digital forensics (i.e. computer, network and mobile forensics), utilising internet to support crime prevention and investigation of cybercrime and offences related to child sexual abuse (including material depicting such offences). The instructors have mainly been experts of the National Bureau of Investigation and other units. In addition to this, various training events have been organised especially in the field of advanced digital forensics by the experts of the cybercrime units. Such training events have mostly been commercial training courses offered by digital forensics companies. These courses have usually been either training in the specific tools manufactured by the training company or more general training that takes advantage of such tools. Training has, in the vast majority of cases, been ad hoc, without long-term systematic guidelines or objectives, and has comprised individual courses rather than a full training programme.

The Police University College is currently substantially reforming its cybercrime prevention education and training. Among other things, the curriculum is under construction, outsourced training services are being reconsidered, for example by taking varying needs of different LEAs more carefully into consideration, international cooperation in the field of cybercrime training has been increased and more human resources have been allocated to cybercrime education and research.

Specialisation studies for ICT crime investigators were offered once at the Police University College in 2009-2011. Corresponding studies are being developed to be put into practice with the reformed curricula in the future. Finland is also becoming a member of the Nordic Computer Forensic Investigators programme that consists of training modules of different levels.

The Police University College of Finland is responsible for organising diploma and advanced studies in police training, for further training given in the training institute and for research and development in the police field, including cybercrime-related training and research. Experts of the national police units support the Police University College by consulting the requirement specification and quality assurance of the courses as well as taking part in teaching.

In 2015 the training costs incurred by the Police University College were approximately EUR 270 000. The training costs covered by the units themselves have presumably topped EUR 50 000 nationwide.

Core cybercrime courses are mainly in the interest of LEAs and therefore such courses are primarily offered by their own training organisations, although increasing demand for this kind of training has recently arisen also outside of the LEA sector.

The Police University College has recently put more effort into collaboration in education between higher education institutions in the field of cybercrime training and education. The objective is to take advantage of each party's strengths and core know-how and to combine them in order to build new courses that would benefit everyone in the alliance.

Academia

The Finnish Police University College collaborates with universities and universities of applied sciences in both education and in research. There are a lot of cybersecurity-related courses available in higher education but their main focus is rarely on cybercrime though the topics may often touch on it. Cyber security is also a topic of research in some universities.

EU agencies

CEPOL and EC3 allocate seats for Finnish students at their courses according to their conventions. The number of Finnish students is relatively low annually . The Finnish police has a representative in ECTEG. Courses developed by ECTEG have not yet been implemented in Finland but they play a key role in the curriculum plan of the Police University College.

Finnish perception

Access to ENISA and CEPOL training and training material should be simplified for the judiciary. All cyber training and EU-funded academic projects should be better coordinated. Europol, ENISA, Eurojust or the Commission could take the lead in this work. It is obvious that cyber training is scattered and lacking in efficiency.

There is neither overall training nor responsibility therefor. The Ministry of Justice is responsible for judges, the Office of the Prosecutor General for prosecutors and LEAs for their staff. Joint training would be desirable in addition to separate training.

8.2. Awareness-raising

FICORA maintains nationwide situational awareness of cyber security. One of FICORA's objectives is also to increase awareness of information security in homes and companies, for example by means of guidelines. The National Cyber Security Centre Finland (NCSC-FI) at FICORA also issues alerts, 'Information security now!' articles and vulnerability reports.

Furthermore, cyber security and cybercrime-related threats have been taken into account in Finnish basic education. In the basic education curriculum cyber security and information security have been noted in improving students' skills in information technology. The aim is to achieve a broad awareness of cybercrime-related threats. Education in information technologies starts from the first grade. Pupils are taught to act responsibly and safely. They are advised to understand the principles of information and communication technologies and the crucial concepts in this area. Pupils are guided to use information technologies in a responsible, safe and ergonomic manner. During basic education the pupils acquire experience in using information technology also in global interactions. They learn to be aware of its significance, possibilities and risks in global actions. Schools give education on how to protect oneself from cybercrime risks.

8.3. Prevention

8.3.1 National legislation/policy and other measures

According to the Police Act the duty of the police is to prevent, detect and investigate crimes. The strategy for preventive policing was launched in 2014. The strategy highlights the importance of cooperation between the authorities and other stakeholders. Prevention of crime focuses information-led policing. Improved situation awareness and setting priorities are two of the key elements of the strategy.

The growth of social media has had an impact on Finnish police work. Police officers use social media. By communicating, they strive to serve people every day, even after office hours, to increase the visibility of the police, offering possibilities for interaction and thus preventing crime, and of course to provide general information, give advice and attempt to promote the social participation of citizens.

The new updated National Action Plan for the Prevention of Violent Radicalisation and Extremism was adopted in April 2016.

The NBI has communicated to the general public via news media and via Twitter accounts of the Cybercrime Centre and the Head of the Cybercrime Centre in order to educate them and warn them about acute phenomena. Also a lot of presentations have been given to several interest groups (private sector companies, the financial sector and university students).

So far preventive work has been on ad hoc basis and has not been planned in advance. This has been recognised as an area for improvement and in future preventive work will be given higher priority and will be done in a planned way in cooperation with the National Cyber Security Centre.

The National Cyber Security Centre has been issuing alerts and 'Information security now!' articles and vulnerability reports. It also works with several interest groups in order to prevent and resolve cyber security breaches.

8.3.2 Public Private Partnership (PPP)

The Ministry of the Interior has a working group with the private sector which aims to prevent criminality such as cybercrime against businesses.

Finland considers cooperation with the private sector to be an important tool to prevent cybercrime. However, there are no fixed structures, MoUs or other agreements in place with the private sector unless use is made of services and/or products from them. Operational cooperation is based on mutual trust and takes place in a case-by-case manner.

8.4. Conclusions

- Training for judges is organised by the Ministry of Justice. Even though Finnish authorities have reported that 150 judges have been trained on the subject, such initiatives appear to be sporadic and very basic. There is no structured and prospective training programme aimed at increasing the skills and knowledge of judges with regard to cybercrime. In the evaluators' view a higher degree of specialisation seems to be needed to ensure a certain level of knowledge of cybercrime among all judges.

- With regard to prosecutors the evaluation team noted limited specialisation. Furthermore, there are plans to train prosecutors on some of the more basic aspects. In the opinion of the prosecutors met there is a clear need for more education regarding cybercrime issues amongst all prosecutors and judges.

- Regarding the police, the level of knowledge of the specialised investigators is very high. However, the importance of the ability of the regional police to tackle cybercrime should also not be underestimated. The main challenge has been that training provided so far has only addressed specialists and, in the evaluators' view, the training possibilities should also cover the regional police.

- Police training has been organised on an ad hoc basis. The Police University College so far does not have a systematic approach to the training of police investigators. Lecturers for courses organised at the Police University College are mainly provided by the NBI. An ISF-funded project included a survey on training needs and implementation of training. Specialist knowledge and access to tools depend mainly on the initiatives of individual districts. Therefore, the Police University College could consider the provision of systematic training for specialised police officers by exploiting already existing training opportunities available through external sources, such as ECTEG and CEPOL.

- A major issue observed in Finland is that there is no long-term plan that will ensure the sustainability of the cyber-related training being given to the police, prosecutors or judges. Apart from the specialisation of the NBI, there is a need to raise the general level of knowledge on cybercrime within the judiciary and police officers. Although the evaluators noticed attempts to implement courses on cybercrime in the training of prosecutors, a more systematic approach is recommended for all the above-mentioned professions.

- As regards prevention, FICORA does not have its own prevention campaigns targeting the general population. In fact, there appears to be no centralised approach or single entity coordinating prevention campaigns targeting the general population. There appear to be very limited and sporadic prevention campaigns and efforts directed towards the general population on the subjects of child abuse and, more generally, internet safety. In the opinion of the evaluators, there is an opportunity for the Cybercrime Centre, Cyber Security Centre, cyber security companies and NGOs to address this gap by pooling resources in order to implement visible and sustainable campaigns directed towards increasing awareness of this phenomenon amongst the general population.

- The lack of public awareness and knowledge about cyber threats, as well as legal regulations in that field are the main reasons to consider relocation of responsibility to IT entities that cooperate directly with the police. Furthermore, the organisation of prevention campaigns with particular reference to child pornography and addressed to young people should be taken into account in order to prevent them from falling victims of cybercrime.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Finland

Finland feels a need to put its capabilities in perspective with the risks and challenges faced. Although Finland is not a central target of cybercrime it faces the same challenges as higher-risk countries, but the frequency and number of attacks are lower.

The Cybercrime Centre's assessment is that, in terms of capabilities (prevention, situational awareness), there is more expertise and skilled resources dedicated to fighting cybercrime in all parts of Finland.

The National Cyber Security Strategy, as well as the European one, highlights only briefly the importance of training prosecutors and judges. The Finnish Action Plan has no action in relation to training of the judiciary or capacity building. Criminal liability should be one of the cornerstones of the Cyber Security Strategy. The current strategy is about intelligence gathering and crime prevention and public-private cooperation and police resources. This alone does not bring criminals before justice.

On the other hand, police presence in the social media is a new and evolving feature. It is an element of all police work, pre-emptive activities included. By communicating, they strive to serve people every day, even after office hours, to increase the visibility of the police, offering possibilities for interaction and thus preventing crime, and of course to provide general information, give advice and to attempt to promote the social participation of citizens.

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 Finland was able to satisfactorily review the system in Finland.

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

The evaluation team thought it fit to make a number of suggestions for the attention of the Finnish 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 Finland

1. Should conduct the necessary review of Finland's Cyber Security Strategy in order to reflect current needs e.g. by including the judiciary's needs in this strategy and addressing the perceived lack of appreciation at strategic level expressed by practitioners; (cf. 3.1, 3.2 and 3.5)

2. Should work on reliable and comprehensive statistics from various stakeholders involved in fighting cybercrime (such as CERT-FI, FICORA, the police and judiciary) to define the main trends in cybercrime and have a clearer view of its development in Finland; (cf. 3.3 and 3.5)

3. Should be encouraged to increase the number of prosecutors specialised in fighting cybercrime; (cf. 4.1.1 and 4.5)

4. Should be encouraged to increase knowledge and competence at regional and local level, specifically by making provision for general non-technical police personnel across all districts to be trained in order to ensure a uniform and consistent understanding of cybercrime issues; (cf. 4.2 and 4.5)

5. Is encouraged to review the existing set of coercive measures to be applied in cybercrime cases with a view to extending them, given the specific nature of cybercrime investigations; (cf. 5.2.1 and 5.5)

6. Should consider strengthening the reporting obligation to the police, for example by introducing a more mandatory reporting system, particularly for serious crimes in the case of attacks on critical infrastructures or banks; (cf. 6.1.2, 6.3.1 and 6.4)

7. Should be encouraged to finalise the establishment of a hash database for CAM and to ensure the long-term sustainability of this initiative; (cf. 6.2.1 and 6.4)

8. Should engage in discussions with ISPs in order to encourage them to refer to the list of websites containing CAM; (cf. 6.2.2 and 6.4)

9. Should raise the general knowledge of cybercrime within the judiciary by enhancing training opportunities for judges and prosecutors and organising more events or training modules on cybercrime; (cf. 8.1 and 8.4)

10. Should enhance prevention and awareness-raising campaigns and efforts directed towards society on the subjects of child abuse online and internet safety; (cf. 8.2, 8.3.1 and 8.4)

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

1. Member States should consider setting up a dedicated budget for cybercrime training and equipment for police departments, both at national and regional level, as managed by the National Police Board in Finland; (cf. 3.4 and 3.5)

2. Member States should consider adopting a system of assisting in, rather than completely taking over, the less serious types of cyber crime investigations from the local police districts to the central level, in order to facilitate knowledge sharing and capacity building at local level as practised by the National Bureau of Investigation in Finland; (cf. 4.2 and 4.5)

3. Member States are recommended to establish good platforms of cooperation with the private sector such as the eCIP network in Finland; (cf. 6.2.4 and 6.4)

4. Member States are recommended to make use of JITs in cross-border investigations relating to cybercrime due to the possibilities that exist within this framework, such as those encountered by Finland; (cf. 7.1.2 and 7.6)

5. Member States are recommended to establish single points of contact within the police with international service providers to facilitate a smooth communication flow between national authorities and the private industry, based on trust and mutual respect, as in the case of the police in Finland; (cf. 7.5.1 and 7.6)

6. Member States are recommended to enhance their cooperation with neighbouring countries to strengthen their policy to fight cybercrime, as carried out by Finland with the Nordic and Baltic countries; (cf. 7.5.3 and 7.6)

7. The EU institutions should be encouraged to pursue solutions to legal problems regarding jurisdiction and collection of e-evidence from the cloud; (cf. 5.5)

8. The EU institutions and agencies should consider how to involve third countries in JIT cooperation; (cf. 7.3)

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

6 - 9 September 2016

Monday, 5 September 2016

Arrival of GENVAL experts, Helsinki - Vantaa airport

Tuesday, 6 September 2016

National Bureau of Investigation, Jokiniemenkuja 4, Vantaa.

Participants:
Ministry of the Interior, National Police Board, National Bureau of Investigation Ministry of Justice and Office of the Prosecutor General.

9.30.	**Welcoming of the Evaluation Team**
9.45.	**National structures. General matters**
11.00.	**Coffee break**
11.15.	**Cyber attacks**
12.30.	**Lunch**
13.30.	**Online card fraud**
14.30.	**Prevention of cybercrime**
16.30.	**End of the meeting**

Transfer to hotel

Wednesday, 7 September 2016

Office of the Prosecutor General, Albertinkatu 25 A, Helsinki

Participants:
Office of the Prosecutor General, Ministry of Justice, Ministry of the Interior, National Bureau of Investigation.

Representative of the Save the Children takes part in session "Offences related to child sexual abuse online Child pornography".

9.00. **Finnish prosecution service**

9.30. **Mutual recognition**

10.15. **Coffee break**

10.30. **Offences related to child sexual abuse online and child pornography**

11.30. **Training and awareness raising activities**
Investigation and prosecution

12.30. **Lunch**

Ministry of Justice, Eteläesplanadi 10, Helsinki

Participants:

Ministry of Justice, Office of the Prosecutor General, Ministry of the Interior

13.30. **Criminalisation. Procedural issues**

14.30. **Coffee break**

14.45. **Jurisdiction**

Mutual legal assistance. Surrender / Extradition

16.30. **End of the meeting**

Thursday, 8 September 2016

Ministry of Transport and Communications, Eteläesplanadi 16, Helsinki

Participants:

Ministry of Transport and Communications, Finnish Communications Regulatory Authority (National Cyber Security Centre Finland (NCSC-FI)), Ministry of the Interior, Ministry of Justice, National Bureau of Investigation.

9.30. - 10.00. **Prevention of cybercrime in the field of the Ministry of Transport and Communications**

10.00. - 10.45. **National Cyber Security Centre Finland, tasks and role**

10.45. - 11.00. **Coffee break**

11.00. - 11.30. **Cooperation with private sector**

11.30. - 12.30. **Discussion**

12.30. - 14.00. **Lunch**

Ministry of the Interior, Erottajankatu 2, Helsinki
Room: 238

14.00. - 15.00. **Cyber Security in Finland**

End of the meeting

Friday, 9 September 2016

Ministry of the Interior, Erottajankatu 2, Helsinki
Room: 238

Participants:

Ministry of the Interior, National Police Board, National Bureau of Investigation Ministry of Justice and Office of the Prosecutor General.

9.00. **Wrap-up-session**

12.00. **Close of the meeting**

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 6 September 2016

Venue: National Bureau of Investigation,

Person interviewed/met	Organisation represented
Mika Junninen	Senior planning officer Ministry of Justice
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General
Hannele Taavila	Counsellor for Legislative Affairs Ministry of the Interior
Tiina Ferm	Counsellor for Legislative Affairs Ministry of the Interior
Jenni Juslen	Senior Adviser National Police Board
Timo Laine	Chief Superintendent National Police Board
Timo Piiroinen	Head of Cybercrime Center, National Bureau of Investigation
Tero Muurman	Detective Chief Inspector ,National Bureau of Investigation
Ville Elenius,	Senior Detective Constable, National Bureau of Investigation
Lars Henriksson	Detective Superintendent National Bureau of Investigation

Meetings on 7 September 2016

Venue: Office of the Prosecutor General

Person interviewed/met	Organisation represented
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General
Harri Tiesmaa	Legal Counsellor Office of the Prosecutor General
Pia Mäenpää	District prosecutor , Prosecutor's Office of Eastern Finland
Juho Lehtimäki	District prosecutor, Prosecutor's office of Itä-Uusimaa
Tero Toiviainen	Senior Specialist Police University College
Sari Sarani	Detective Chief Inspector, National Bureau of Investigation
Veera Uusoksa	Manager, Children and Digital Media Save the Children Finland

Venue: Ministry of Justice

Person interviewed/met	Organisation represented
Mika Junninen	Senior planning officer, Ministry of Justice
Merja Norros	Ministerial Counsellor, Ministry of Justice
Janne Kanerva	Counsellor of Legislation, Ministry of Justice
Anu Juho	Judge, Helsinki District Court
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General

Person interviewed/met	Organisation represented
Lars Henriksson	Detective Superintendent National Bureau of Investigation

Meetings on 8 September 2016

Venue: Ministry of Transport and Communication

Person interviewed/met	Organisation represented
Timo Kievari	Director of Safety and Security unit, Ministry of Transport and Communication
Jarna Hartikainen	Head of Cooperation and Situation Awareness, National Cyber Security Centre Finland
Jyrki Pennanen	Private Sector - Fingrid Plc
Tomi Pitkänen	Private Sector - Neste Plc
Tiina Ferm	Counsellor for Legislative Affairs Ministry of the Interior

Venue: Ministry of Interior

Person interviewed/met	Organisation represented
Yrjö Benson	Special Adviser, Ministry of Finance
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General
Hannele Taavila	Counsellor for Legislative Affairs Ministry of the Interior

Meetings on 9 September 2016

Venue: Ministry of Interior

Person interviewed/met	Organisation represented
Hannele Taavila	Counsellor for Legislative Affairs Ministry of the Interior
Juhani Korhonen	Ministerial Counsellor , Ministry of Justice
Mika Junninen	Senior planning officer Ministry of Justice
Timo Piiroinen	Head of Cybercrime Center, National Bureau of Investigation
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	FINNISH OR ACRONYM IN ORIGINAL LANGUAGE	FINNISH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
AFTA	*AFTA*		Association of Finnish Travel Agents
CAM	*CAM*		child abuse material
CRM	*CRM*		Card Risk Management
CC	*CC*		the Finnish Criminal Code
FICORA	*FICORA*		The Finnish Communications Regulatory Authority
FISIC	*FISIC*		the Finnish Safer Internet Centre
MoU	*MoU*		Memorandum of Understanding
NBI	*NBI*		The National Bureau of Investigations
NCSA-FI	*NCSA-FI*		The National Communications Security Authority
NCSC-FI	*NCSC-FI*		The National Cyber Security Centre Finland
OCG	*OCG*		organised crime groups
SAKARI	*SAKARI*		Case management system
SMAL	*SMAL*		The Association of Finnish Travel Agents

Annex D: Finnish Legislation

Illegal access to information system

Offences in question are *computer break-in* and *aggravated computer break-in* (Chapter 38, Section 8 and Section 8(a) of the Criminal Code). Regardless of the English language names of these offences it's not necessary that the offence is committed by using a computer or is directed to a computer (see definitions below).

Chapter 38, Section 8 - Computer break-in

(1) A person who by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully hacks into an information system where information or data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a *computer break-in* to a fine or to imprisonment for at most two years.

(2) Also a person who, without hacking into the information system or a part thereof,

(1) by using a special technical device or

(2) otherwise by by-passing the system of protection in a technical manner, by using a vulnerability in the information system or otherwise by evidently fraudulent means

unlawfully obtains information or data contained in an information system referred to in subsection 1, shall be sentenced for a computer break-in.

Chapter 38, Section 8(a) - Aggravated computer break-in

(1) If the computer break-in is committed

(1) as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2 or

(2) in a particularly methodical manner

and the computer break-in is aggravated also when assessed as a whole, the offender shall be sentenced for *an aggravated computer break-in* to a fine or to imprisonment for at most three years.

Chapter 6, Section 5 - Grounds increasing the punishment

(1) The following are grounds for increasing the punishment:

(1) the methodical nature of the criminal activity,

(2) commission of the offence as part of the activity of an organised criminal group,

(3) commission of the offence for remuneration,

(4) commission of the offence for a motive based on race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation or disability or another corresponding grounds, and

(5) the criminal history of the offender, if the relation between it and the new offence, due to the similarity between the offences or otherwise, shows that the offender is apparently heedless of the prohibitions and commands of the law.

(2) "Organized criminal group" refers to a structured association of three or more persons, existing for a period of time and acting in concert with the aim of committing offences that are punishable by a maximum sentence of imprisonment for at least four years, or offences referred to in Chapter 11, section 10 or Chapter 15, section 9.

Chapter 6, Section 6 – Grounds reducing the punishment

The following are grounds for reducing the punishment:

(1) significant pressure, threat or a similar influence that has affected the commission of the offence,

(2) strong empathy or an exceptional and sudden temptation that has led to the offence, the exceptionally great contribution of the injured party or a corresponding circumstance that has been conducive to decreasing the capability of the offender to conform to the law,

(3) reconciliation between the offender and the injured person, other attempts of the offender to prevent or remove the effects of the offence or his or her attempt to further the clearing up of the offence, and

(4) the grounds mentioned in section 8(1) and (3).

Chapter 6, Section 7 – Grounds mitigating the punishment

In addition to what is provided above in section 6, grounds mitigating the punishment that are also to be taken into consideration are

(1) another consequence to the offender of the offence or of the sentence**,**

(2) the advanced age, poor health or other personal circumstances of the offender, and

(3) a considerably long period that has passed since the commission of the offence, if the punishment that accords with established practice would for these reason lead to an unreasonable or exceptionally detrimental result.

Chapter 6, Section 8 – Mitigation of the penal latitude

(1) The sentence is determined in accordance with a mitigated penal latitude if

(1) the offender has committed the offence below the age of 18 years,

(2) the offence has remained an attempt,

(3) the offender is convicted as an abettor in an offence, through application of the provisions of Chapter 5, section 6, or his or her complicity in the offence is otherwise clearly less than that of other accomplices,

(4) the offence has been committed in circumstances that closely resemble those that lead to the application of grounds for exemption from liability, or

(5) there are special reasons for this pursuant to section 6 or 7 or on other exceptional grounds, mentioned in the sentence.

(2) In determining the punishment pursuant to subsection 1, at most three fourths of the maximum sentence of imprisonment or fine and at least the minimum sentence provided for the offence may be imposed on the offender. If the offence is punishable by life imprisonment, the maximum punishment is instead twelve years of imprisonment and the minimum punishment is two years of imprisonment.

(3) What is provided in subsection 2 also applies in determining the sentence for a person who committed an offence in a state of diminished responsibility. However, diminished responsibility does not affect the applicable maximum punishment.

(4) If the maximum punishment for the offence is imprisonment for a fixed period, the court may in cases referred to in this section impose a fine as the punishment instead of imprisonment, if there are especially weighty reasons for this.

Chapter 6, Section 8(a) – Mitigation of the penal latitude on the basis of confession

(1) The sentence is determined in accordance with a mitigated penal latitude if the offender has contributed to the clarification of his or her offence as provided in Chapter 1, sections 10 and 10(a) and Chapter 5(b) of the Criminal Procedure Act (689/1997) and in Chapter 3, section 10(a) of the Criminal Investigation Act (805/2011).

(2) In determining the punishment on the basis of subsection 1, at the most two thirds of the maximum length of imprisonment or of the maximum amount of the fine may be imposed, and at the least the minimum amount that is provided for the type of punishment. If the maximum punishment that is provided for the offence is imprisonment for a determinate period, the court may impose a fine instead of imprisonment, if there are special reasons for this.

(3) The judgment shall note not only the punishment imposed but also what punishment the court would have imposed without the benefit of what is provided above.

The penalty scale of computer break-in runs from a fine to imprisonment for at most two years and the penalty scale of aggravated computer break-in runs from a fine to imprisonment for at most three years. The minimum and maximum level of fine is defined in Chapter 2(a), Section 1(1) of the Criminal Code. A fine shall be passed as day fines, the minimum number of which is one and the maximum number is 120. The minimum level of imprisonment is defined in Chapter 2(c), Section 2(2) of the Criminal Code. A sentence of fixed-term imprisonment is imposed for at least fourteen days.

Chapter 6, Section 9 of the Criminal Code contains provisions on the choice between conditional and unconditional imprisonment:

Illegal system interference

Chapter 38, Section 5 – Interference with communications

(1) A person who by tampering with the operation of a device used in postal, telecommunications or radio traffic, by maliciously transmitting interfering messages over radio or telecommunications channels or in another comparable manner unlawfully prevents or interferes with postal, telecommunications or radio traffic, shall be sentenced for *interference with communications* to a fine or to imprisonment for at most two years.

Chapter 38, Section 6 - Aggravated interference with communications

(1) If in the interference with communications

(1) the offender commits the offence by making use of his or her position in the service of an institution referred to in the Telecommunications Act, a cable operator referred to in the Cable Transmission Act (307/1987) or a public broadcasting institution, or his or her other special position of trust,

(2) the offence prevents or interferes with the radio transmission of distress signals or such other telecommunications or radio transmissions that are made in order to protect human life,

(3) the offence is committed as part of activity that has to a significant degree affected information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b),

(4) the offence is committed as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2,

(5) the offence causes particularly serious impediment or economic loss, or

(6) the offence is directed at a device, information system or communications, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these,

and the interference with communications is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated interference with communications* to imprisonment for at least four months and at most five years.

Chapter 38, Section 7 - Petty interference with communications

(1) If the interference with communications, in view of its nature or extent or the other circumstances of the offence, is of minor significance when assessed as a whole, the offender shall be sentenced for *petty interference with communications* to a fine.

Chapter 38, Section 7(a) – Interference in an information system

(1) A person who in order to cause detriment or economic loss to another, by entering, transferring, damaging, altering or deleting data or in another comparable manner unlawfully prevents the operation of an information system or causes serious interference in it shall be sentenced for *interference in an information system* to a fine or to imprisonment for at most two years.

Chapter 38, Section 7(b) – Aggravated interference in an information system

(1) If in the interference in an information system

(1) particularly significant detriment or economic loss is caused,

(2) the offence is committed in a particularly methodical manner,

(3) the offence is committed as part of activity that has to a significant degree affected information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b),

(4) the offence is committed as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2,

(5) the offence is directed at an information system, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these,

and the interference in an information system is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated interference in an information system* to imprisonment for at least four months and at most five years.

Illegal data interference

Offences in question are *Damage to data, aggravated damage to data and petty damage to data* (Chapter 35, Sections 3(a) to 3(c) of the Criminal Code).

Chapter 35, Section 3(a) – Damage to data

(1) A person who, in order to cause damage to another, unlawfully destroys, demolishes, hides, damages, alters, renders unusable or conceals data recorded on an information device or another recording or data in an information system, shall be sentenced for *damage to data* to a fine or to imprisonment for at most two years.

Chapter 35, Section 3(b) – Aggravated damage to data

(1) If the damage to data

(1) causes particularly serious harm or economic loss,

(2) is committed as part of the activity of an organised criminal group referred to in Chapter 6, section 5, subsection 2,

(3) is committed as part of activity that has affected a significant amount of information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b), or

(4) is directed at an information system, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these,

and the damage to data is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated damage to data* to imprisonment for at least four months and at most five years.

Chapter 35, Section 3(c) - Petty damage to data

If the damage to data, when assessed as a whole, with due consideration to the minor significance of the damage or the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty damage to data* to a fine.

Illegal interception of computer data

Offences in question are *message interception* and *aggravated message interception* (Chapter 38, Sections 3 and 4 of the Criminal Code).

Relevant are also Chapter 38, Section 8(2) of the Criminal Code concerning computer break-in and Section 8(a) concerning aggravated computer break-in related to offences defined in Section 8(2). These offences are already covered by answers connected with illegal access to information system, see above.

Chapter 38, Section 3 - Message interception

(1) A person who unlawfully

(1) opens a letter or another closed communication addressed to another or by hacking obtains information on the contents of an electronic or other technically recorded message which is protected from outsiders, or

(2) obtains information on the contents of a telephone call, telegram, transmission of text, images or data, or another comparable telemessage transmitted by telecommunications or an information system or on the transmission or reception of such a message

shall be sentenced for *message interception* to a fine or to imprisonment for at most two years.

Chapter 38, Section 4 - Aggravated message interception

(1) If in the message interception

(1) the offender commits the offence by making use of his or her position in the service of a telecommunications company, as referred in the Act on the Protection of Electronic Messages (516/2004) or his or her other special position of trust,

(2) the offender commits the offence by making use of a computer program or special technical device designed or altered for such purpose, or otherwise especially methodically, or

(3) the message that is the object of the offence has an especially confidential content or the act constitutes a grave violation of the protection of privacy and the message interception is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated message interception* to imprisonment for at most three years.

Misuse of devices

The offences in question are *endangerment of data processing* and *an offence involving a system for accessing protected services* (Chapter 34, Section 9(a) and Chapter 38, Section 8 (b) of the Criminal Code.

Chapter 34, Section 9(a) – Endangerment of data processing

A person who, in order to impede or damage data processing or the functioning or security of an information system or telecommunications system,

(1) imports, obtains for use, manufactures, sells or otherwise disseminates or makes available

(a) a device or computer program or set of programming instructions designed or altered to endanger or damage data processing or the functioning of an information system or telecommunications system or to break or disable the technical security of electronic communications or the security of an information system, or

(b) an information system password, access code or other corresponding information belonging to another, or

(2) disseminates or makes available instructions for the production of a computer program or set of programming instructions referred to in paragraph (1), shall be sentenced, unless an equally severe or more severe penalty for the act is provided elsewhere in the law, for *endangerment of data processing* to a fine or to imprisonment for at most two years.

Chapter 38, Section 8(b) — Offence involving a system for accessing protected services

A person who, in violation of the prohibition laid down in section 269, subsection 2 of the Information Society Code (917/2014), for commercial purposes or so that the act is conducive to causing considerable detriment or loss to a provider of protected services, produces, imports, offers for sale, rents out or distributes a system for accessing protected services, or advertises, installs or maintains the same, shall, unless a more severe or equally severe penalty is provided elsewhere in law for the act, be sentenced for an *offence involving a system for accessing protected services* to a fine or to imprisonment for at most one year.

Computer-related child pornography offences

Offences in question are *distribution of a sexually offensive picture, aggravated distribution of a sexually offensive picture depicting a child* and *possession of a sexually offensive picture depicting a child* (Chapter 17, Sections 18, 18(a) and 19 of the Criminal Code). These provisions are general, covering all kind of ways to commit these offences.

Chapter 17, Section 18 - Distribution of a sexually offensive picture

(1) A person who manufactures, offers for sale or for rent or otherwise offers or makes available, keeps available, exports, imports to or transports through Finland to another country, or otherwise distributes pictures or visual recordings that factually or realistically depict

(1) a child,

(2) violence or

(3) bestiality

shall be sentenced for *distribution of a sexually offensive picture* to a fine or imprisonment for at most two years.

---

(4) A child is defined as a person below the age of eighteen years and a person whose age cannot be determined but whom there is justifiable reason to assume is below the age of eighteen years. The picture or visual recording is deemed factual in the manner referred to in subsection 1, paragraph 1, if it has been produced in a situation in which a child has actually been the object of sexually offensive conduct and realistic, if it resembles in a misleading manner a picture or a visual recording produced through photography or in another corresponding manner of a situation in which a child is the object of sexually offensive conduct.

The definitions of the terms factual and realistic apply correspondingly in the cases referred to in subsection 1, paragraphs 2 and 3.

Chapter 17, Section 18(a) - Aggravated distribution of a sexually offensive picture depicting a child

(1) If, in the distribution of a sexually offensive picture depicting a child

(1) the child is particularly young,

(2) the picture also depicts severe violence or particularly humiliating treatment of the child,

(3) the offence is committed in a particularly methodical manner or

(4) the offence has been committed within the framework of an organized criminal group referred to in Chapter 6, section 5, subsection 2 and the offence is aggravated also when assessed as whole, the offender shall be sentenced for *aggravated distribution of a sexually offensive picture depicting a child* to imprisonment for at least four months and at most six years.

Chapter 17, Section 19 - Possession of a sexually offensive picture depicting a child

(1) A person who unlawfully has in his or her possession a picture or visual recording which depicts a child in the sexually offensive manner referred to in section 18, shall be sentenced for *possession of a sexually offensive picture depicting a child* to a fine or to imprisonment for at most one year.

(2) A person who in return for payment or otherwise by agreement has obtained access to a picture or visual recording referred to in subsection 1 so that it is available to him or her on a computer or another technical device without being recorded on the device shall also be sentenced for possession of a sexually offensive picture depicting a child.

Computer-related solicitation of children

The offence in question is *Solicitation of a child for sexual purposes* (Chapter 20, Section 8(b) of the Criminal Code). Provisions are general, covering all kind of ways to commit these offences.

Chapter 20, Section 8(b) – Solicitation of a child for sexual purposes

(1) A person who suggests a meeting or other contact with a child so that it is apparent from the contents of the suggestion or otherwise from the circumstances that the intent of the person is to prepare sexually offensive pictures or visual recordings of the child in the manner referred to in Chapter 17, section 18, subsection 1, or to subject the child to the offence referred to in section 6 or 7 of this Chapter, shall be sentenced for *solicitation of a child for sexual purposes* to a fine or to imprisonment for at most one year.

(2) Unless a more severe sentence is provided in law for the act, also a person who solicits a person below the age of eighteen years to engage in sexual intercourse or in another sexual act in the manner referred to in section 8(a) or to perform in a sexually offensive organized performance shall be sentenced for solicitation of a child for sexual purposes.

Computer-related fraud

Offences in question are *fraud, aggravated fraud, petty fraud, means of payment fraud, aggravated means of payment fraud* and *petty means of payment fraud* (Chapter 36, Sections 1 to 3 of the Criminal Code and Chapter 37, Sections 8 to 10 of the Criminal Code).

Chapter 36, Section 1 - Fraud

(1) A person who, in order to obtain unlawful financial benefit for himself or herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for *fraud* to a fine or to imprisonment for at most two years.

(2) Also a person who, with the intention referred to in subsection 1, by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss, shall be sentenced for fraud.

Chapter 36, Section 2 - Aggravated fraud

(1) If the fraud

(1) involves the seeking of considerable benefit,

(2) causes considerable or particularly significant loss,

(3) is committed by taking advantage of special confidence based on a position of trust or

(4) is committed by taking advantage of a special weakness or other insecure position of another and the fraud is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated fraud* to imprisonment for at least four months and at most four years.

Chapter 36, Section 3 - Petty fraud

If the fraud, when assessed as a whole, with due consideration to the benefit sought or the amount of loss caused or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty fraud* to a fine.

Chapter 37, Section 8 - Means of payment fraud

(1) A person who, in order to obtain unlawful economic benefit for himself or herself or another

(1) uses a means of payment without the permission of the lawful holder, in excess of his or her right based on such permission, or otherwise without lawful right, or

(2) transfers a means of payment or means of payment form to another in order to have it used without lawful right shall be sentenced for *means of payment fraud* to a fine or to imprisonment for at most two years.

(2) Also a person who, by overdrawing his or her account or exceeding the agreed maximum credit limit, misuses a means of payment referred to in subsection 1 and in this way causes economic loss to another shall be sentenced for means of payment fraud, unless when using the means of payment he or she intended to compensate the loss without delay.

Chapter 37, Section 9 - Aggravated means of payment fraud

If in the means of payment fraud

(1) considerable or particularly significant loss is caused or

(2) the offender has, for the commission of the offence, made or had made means of payment forms from which the means of payment used in the offence was prepared, or if the offence is otherwise committed in a particularly methodical manner and the means of payment fraud is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated means of payment fraud* to imprisonment for at least four months and at most four years.

Chapter 37, Section 10 - Petty means of payment fraud

If the means of payment fraud, when assessed as a whole, with due consideration to the amount of benefit sought or the amount of loss caused or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty means of payment fraud* to a fine.

Computer-related forgery

Offences in question are *forgery, aggravated forgery* and *petty forgery* (Chapter 33, Sections 1 to 3 of the Criminal Code). These provisions are general, covering all kind of ways to commit these offences.

Chapter 33, Section 1 - Forgery

(1) A person who prepares a false document or other item or falsifies such a document or item in order for it to be used as misleading evidence or uses a false or falsified item as misleading evidence shall be sentenced for *forgery* to a fine or imprisonment for at most two years.

Chapter 33, Section 2 - Aggravated forgery

If in the forgery

(1) the item that is the object of the offence is an archival document stored by an authority or a general register kept by an authority and such a document or register is important from a general point of view, or the item otherwise has a particularly significant probative value, or

(2) the offender uses technical equipment procured for the commission of forgery offences or otherwise acts in a particularly methodical manner and the forgery is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated forgery* to imprisonment for at least four months and at most four years.

Chapter 33, Section 3 - Petty forgery

If the forgery, when assessed as a whole, with due consideration to the nature of the item or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty forgery* to a fine.