Council of the European Union

Brussels, 12 August 2016
(OR. en)

9892/1/16
REV 1 DCL 1

GENVAL 67
CYBER 63

DECLASSIFICATION

of document:	9892/1/16 REV 1
dated:	15 July 2016
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating Cybercrime" - Report on Cyprus

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, 15 July 2016
(OR. en)

9892/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 67
CYBER 63

DECLASSIFIED

REPORT

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

Table of Contents

1. EXECUTIVE SUMMARY 5

2. INTRODUCTION 10

3. GENERAL MATTERS AND STRUCTURES 13

3.1. National cyber security strategy 13

3.2. National priorities with regard to cybercrime 14

3.3. Statistics on cybercrime 19

3.3.1. Main trends leading to cybercrime 19

3.3.2. Number of registered cases of cyber criminality 20

3.4. Domestic budget allocated for the prevention of and fight against cybercrime and support from EU funding 21

3.5. Conclusions 22

4. NATIONAL STRUCTURES 24

4.1. Judiciary (prosecutions and courts) 24

4.1.1. Internal structure 24

4.1.2. Capacity and obstacles to successful investigation 24

4.2. Law enforcement authorities 25

4.3. Other authorities/institutions/public-private partnership 27

4.4. Cooperation and coordination at national level 27

4.4.1. Legal or policy obligations 27

4.4.2. Resources allocated to improving cooperation 29

4.5. Conclusions 29

5. LEGAL ASPECTS 32

5.1. Substantive criminal law pertaining to cybercrime 32

5.1.1. Council of Europe Convention on Cybercrime 32

5.1.2. Description of national legislation 32

DECLASSIFIED

A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems 32

B/ Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography 34

C/ Online Card fraud 37

5.2. Procedural issues 38

5.2.1. Investigative Techniques 38

5.2.2. Forensics and Encryption 39

5.2.3. E-Evidence 39

5.3. Protection of Human Rights/Fundamental Freedoms 40

5.4. Jurisdiction 41

5.4.1. Principles applied to the investigation of cybercrime 41

5.4.2. Rules in the case of conflicts of jurisdiction and referral to Eurojust 41

5.4.3. Jurisdiction for acts of cybercrime committed in the "cloud" 41

5.4.4. Perception of Cyprus with regard to legal framework to combat cybercrime 41

5.5. Conclusions 42

6. OPERATIONAL ASPECTS 44

6.1. Cyber attacks 44

6.1.1. Nature of cyber attacks 44

6.1.2. Mechanism for responding to cyber attacks 44

6.2. Actions against child pornography and sexual abuse online 46

6.2.1. Software databases identifying victims and measures to avoid re-victimisation 46

6.2.2. Measures to address sexual exploitation/abuse online, sexting, cyber bullying 46

6.2.3. Preventive actions against sex tourism, child pornographic performance and others 47

6.2.4. Actors and measures countering websites containing or disseminating child pornography 48

6.3. Online card fraud 50

6.3.1. Online reporting 50

6.3.2. Role of the private sector 50

6.4. Conclusions 51

DECLASSIFIED

7. INTERNATIONAL COOPERATION 54
7.1. Cooperation with EU agencies 54
7.1.1. Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA 54
7.1.2. Assessment of the cooperation with Europol/EC3, Eurojust, ENISA 54
7.1.3. Operational performance of JITs and cyber patrols 56
7.2. Cooperation between the Cyprus authorities and Interpol 56
7.3. Cooperation with third states 56
7.4. Cooperation with the private sector 57
7.5. Tools of international cooperation 57
7.5.1. Mutual Legal Assistance 57
7.5.2. Mutual recognition instruments 59
7.5.3. Surrender/Extradition 60
7.6. Conclusions 61

8. TRAINING, AWARENESS-RAISING AND PREVENTION 63
8.1. Specific training 63
8.2. Awareness-raising 64
8.3. Prevention 68
8.3.1. National legislation/policy and other measures 68
8.3.2. Public Private Partnership (PPP) 71
8.4. Conclusions 72

9. FINAL REMARKS AND RECOMMENDATIONS 75
9.1. Suggestions from Cyprus 75
9.2. Recommendations 76
9.2.1. Recommendations to Cyprus 76
9.2.2. Recommendations to the European Union, to its institutions, and to other Member States 78
Annex A: Programme for the on-site visit and persons interviewed/met 79
Annex B: Persons interviewed/met 82
Annex C: List of abbreviations/glossary of terms 84

DECLASSIFIED

1. EXECUTIVE SUMMARY

The evaluation visit to Cyprus took place between 18 and 20 November 2015. The Cypriot authorities invested much effort in the organisation of the visit, which overall was instructive and interesting.

The evaluation team had the opportunity to talk to representatives of the different authorities involved in the prevention of and the fight against cybercrime, including officials from the Ministry of Justice and Public Order, the Office of the Commissioner for Electronic Communication and Postal Regulation, the Cyprus Pedagogical Institute, the Cyprus Police, etc. All the authorities spoken to were happy to exchange views in an informal way with the evaluation team. They all showed a high degree of commitment to preventing and fighting cybercrime. The Cypriot representatives met were well prepared and the mission was well organised, including logistics.

However, as the disadvantage of the evaluation visit was that there was no possibility to meet with the expert of the Attorney-General's Office.

The Cypriot approach towards cybercrime is designed to allow it to function properly. The size of the country (in terms of both territory and population) also determines the amount of financial and human resources allocated to deal with cybercrime and cybersecurity in more general terms. The key actors seem to have established a proper working ethic and atmosphere. They know each other personally (allowing easy communication), and they cooperate informally, while following all the necessary formal procedures at the same time. This approach appears to be quite result-oriented. Specific bureaucratic burdens were neither reported nor seen during the evaluation visit.

DECLASSIFIED

The National Cybersecurity Strategy was adopted by the Ministerial Council. The Office of the Commissioner of Electronic Communications and Postal Regulations is responsible for its monitoring and implementation. The National Cybersecurity Strategy is the instrument for steering the efforts made by Cyprus to prevent and combat cybercrime. It has provided the structures for the cooperation between all competent authorities, including public, private and non- governmental agencies especially in the field of awareness-raising, to which Cyprus devotes much effort in order to combat this form of crime. However, there is some room for improvement in terms of the actual implementation of the Strategy, mostly regarding human resources and funding.

Cyprus implemented most of the European instruments on cybercrime and the resulting measures. The main actor in countering cybercrime is the Office for Combating Cybercrime (O.C.C.), Cyprus Police, which is responsible for the investigation of cybercrime, specifically hacking and child pornography as defined in the Law on the Convention against Cybercrime, L.22(III)/2004. Its work is supported by the Digital Evidence Forensic Laboratory (DEFL), Cyprus Police, which is responsible for the effective examination of electronic evidence. DEFL is staffed with specialised officers for the collection and forensic analysis of electronic devices.

The proper usage of available EU funds for up-to-date forensic software and hardware equipment, technical appliances that are used for investigation, modern equipment for the purposes of DEFL, has to be reported on. In the evaluators' view, being properly equipped with IT tools is crucial for conducting successful cybercrime investigations. Therefore, in the opinion of the evaluators the use of EU funds is of significant importance in enabling the relevant authorities to work in the most efficient manner and to utilise their full potential. At the same time, the Cypriot authorities should also contribute to providing sufficient funding in the area of fighting cybercrime**.**

Close cooperation and swift dialogue between the police and the Public Prosecution Service was reported, though – as a disadvantage of the visit – the team did not have the opportunity to meet with an expert of the Attorney General's Office.

DECLASSIFIED

Cyprus' approach towards cybercrime is multidisciplinary. However, a consistent mechanism for responding to cyber attacks has not been yet established. The Department of Information Technology Services (DITS) was designated by the Government and established under the supervision of OCECPR as the Government CIRT of Cyprus (Cyprus GOVCIRT) (P.I. 358/2010). The development of a national CERT is still ongoing within the framework of the implementation of the National Cybersecurity Strategy. According to the Cypriot authorities, it is expected to be completed by 2017.

The police cooperates with private companies reporting a cyber attack to help them resolve this problem and investigate the offence. Critical infrastructure operators in the field of electronic communications have specific legal and regulatory obligations as regards network and information security which cover availability, cyber attacks, prevention and mitigation measures. Operators also have reporting obligations relating to incidents affecting availability of networks and services and data breaches. Multifaceted cooperation between public authorities and the financial sector could work to benefit both of them and significantly increase the level of cybersecurity in Cyprus. At the moment, the public authorities do not cooperate directly with banks and other financial institutions but a cooperation framework is under consideration.

According to the statistics on number of cybercrimes reported to the police or by the police, the majority of cases are related to online child abuse. Far fewer cases of cyber attacks and payment card fraud reported. Taking that into account, the number and nature of cybercrime reports, in the opinion of the evaluators, Cyprus does not fully reflect current cybercrime threats. Moreover, statistics available on cybercrime are, in the evaluators' opinion, not sufficient to build up an overall perception of this phenomenon in Cyprus.

DECLA-

Specific emphasis is placed on prevention and awareness-raising. Cyprus has invested a great deal of effort and enthusiasm in teaching and prevention programmes, which may be considered as examples of best practice. This effort is based on the close collaboration of the public sector (Ministry of Education and Culture through the Cyprus Pedagogical Institute) and the private sector, through the Industry (e.g. ISPs), non profit organisations (e.g. Hope for Children, CNTI), organised groups (School for Parents) which are contributing with enthusiasm in awareness and prevention programmes.

In 2006, *CyberEthics* co-founded project which includes partners from the private and public sector was initiated as an Awareness Node, responsible for informing children, parents, teachers and other stakeholders about Internet safety issues and educating them in how to be safe on the Web. A separate project, the Hotline for reporting illegal content found on the Internet, was established. The Hotline aimed at making it possible to report illegal content found on the Internet involving child sexual abuse images and racism and xenophobia. Its goal was to allow the public and especially teenagers and young adults to facilitate the process for a safer Internet environment through the reporting of illegal content.

In 2008 the Awareness Node and Hotline were merged, and in 2009 *CyberEthics* became a Safer Internet Centre with the inclusion of a Helpline. The latter aimed at providing people with the means to receive support on harmful conduct, harmful contact, harmful content and uncomfortable or scary experiences on the Web. It promoted the helpline to the public, to encourage people to use this tool.

The Cyprus Pedagogical Institute introduced programmes for supporting schools, teachers, pupils and parents to implement annual action plans for the safe use of internet.
In the context of the "Safe School for the Internet Programme" learning designs are introduced in the classrooms, educational content is being developed, professional development is offered to teachers and school based workshops are implemented for pupils, teachers and parents on internet safety and protection issues.

DECLASSIFIED

One of the most interesting and valuable programmes introduced in schools is the "Young Coaches for the Internet" programme. The main idea is that children are taught about Internet security by other children, not by adults and in this way they take responsibility for their own learning, they prepare their own action plans for their schools, they get involved in peer learning activities and train others, including their teachers and parents. Other programmes and activities offered by the Cyprus Pedagogical Institute include an annual competition for the production of short videos by students on safe internet issues, participation in the esafetylabel programme and the administration of a central safe internet filter in all schools. At the same time other projects are offered in schools and innovative use of the internet as part of learning and development of transversal skills needed in the digital society.

Although Cyprus stresses the importance of prevention and the education of children, the training of professionals in the field of cybercrime seems to be insufficient. No regular or specialized training courses on cybercrime are aimed at judges and prosecutors. In the opinion of the evaluators, training and the achievement of excellence is a crucial issue for the effectiveness of the fight against cybercrime. Specifically, joint training courses provide mutual understanding of the specific knowledge, legal requirements and different experiences of the main actors involved in countering cybercrime. Cybercrime is a highly complex and constantly evolving field of criminality, which, without proper specialist training, is not easy to understand. Therefore, joint training courses for judges, prosecutors and police officers could be of added value.

This situation may change in the future since Cyprus has started a project called 3CE aimed at establishing a centre of expertise on cybercrime at the national level, encompassing police officers, prosecutors and judges.

Europol/EC3 and Eurojust are known to the practitioners and are sometimes asked for assistance. However, Europol is more frequently used.

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

DECLASSIFIED

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 preventing and combating cybercrime.

Member States welcomed the choice of cybercrime as the subject for the seventh mutual evaluation round. However, due to the broad range of offences 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 the 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.

DECLASSIFIED

1 Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997, p. 7.
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 ratifying 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'. That Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems.[6]

Experience from past evaluations shows that Member States will be at different stages in the implementation of relevant legal instruments, and the current process of evaluation could also provide useful input 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 only on the implementation of various instruments relating to fighting cybercrime but rather on the related operational aspects in the Member States.

Therefore, apart from cooperation with prosecution services, this will also encompass how police authorities cooperate with Eurojust, ENISA and Europol/EC3, and how feedback from those actors is channelled to the appropriate police and social services. The evaluation focuses on the implementation of national policies with regard to the 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 victims of cybercrime.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Cyprus was the sixteenth 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 was drawn up by the Presidency. Member States nominated experts with substantial practical knowledge in the field pursuant to a written request made to delegations on 28 January 2014 by the Chairman of GENVAL.

DECLASSIFIED

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

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

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

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

The experts charged with undertaking the evaluation of Cyprus were Ms Veronika Podlahová (Czech Republic), Mr Renato Grgurić (Croatia) and Mr Rafał Kierzynka (Poland). Two observers were also present: Mr Dimitar Hadzhiyski (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 from the evaluation visit that took place in Cyprus between 18 and 20 November 2015, and on Cyprus' detailed replies to the evaluation questionnaire, together with their detailed answers to the ensuing follow-up questions.

DECLASSIFIED

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

The Cybersecurity Strategy of the Republic of Cyprus has been in place since March 2013. The Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR) is responsible for the monitoring and implementation of this strategy.

The National Cybersecurity Strategy is modelled on the EU Strategy. The Strategy refers to horizontal actions related to the four pillars which are Network and Information Security, cyber defence, cyber diplomacy and cybercrime. It identifies 17 Actions (fields of work) to be carried out by all relevant stakeholders, including protection of critical infrastructure, threat assessment, awareness, international cooperation, cooperation with the industry and academia. The Strategy describes the role of each key player in the field of cyber security.

The Ministry of Transport and Communications and Works has the lead with regard to network and information security, the Ministry of Defence has the lead with regard to cyber defence issues, the Ministry of Foreign Affairs is responsible for issues relating to cyber diplomacy. The Ministry of Justice and Public Order, together with the Cyprus Police, are the authorities responsible for the prevention and combating of cybercrime.

The OCECPR, which has the responsibility for overall coordination of the Strategy's implementation, has created a Steering Group under Action 17 of the National Cybersecurity Strategy in accordance with a decision of the Council of Ministers with participants from all the above ministries, so that dependencies and synergies are identified and taken on board during the implementation of the National Cybersecurity Strategy.

DECLASSIFIED

The Cyprus Police also contributes to the work carried out, inter alia, under Action 14 Awareness of the National Cybersecurity Strategy. The Cyprus Police has created a specialised Office for Combating Cybercrime (O.C.C.), thus achieving the necessary expertise in dealing with the particularities of these offences. The Cyprus Police is also involved in other Actions under the National Strategy.

3.2. National priorities with regard to cybercrime

The Ministry of Justice and Public Order and the Cyprus Police take action in areas, such as: the reporting of crime and information gathering; technical resources; cooperation with other competent authorities (including private organizations); awareness; training; legislation; effective international cooperation; and network safety.

National priorities have been drawn up in the following fields:

Prevention

The O.C.C. is responsible for raising awareness in the field of cybercrime. Furthermore, a member of the O.C.C. participates on the Advisory Board of the Safer Internet Centre "*Cyberethics*" co funded project, which is coordinated by the Cyprus Neuroscience and Technology Institute (CNTI), a non -governmental organisation. "*Cyberethics*" runs under the Insafe and Inhope programmes in Cyprus for the prevention of cybercrime. Moreover, staffed by highly trained and educated personnel, the O.C.C. delivers 100 awareness lectures on an annual basis for school children, teachers, parents and other organized groups. At the same time, the O.C.C organises public events at central points and distributes leaflets both in Greek and in English with cybercrime raising-awareness material.

DECLASSIFIED

The O.C.C. has developed a handbook, which describes the work undertaken in this field.
Moreover, the O.C.C. implemented in January 2014 the Cybercrime Reporting Platform[7] and the Cyprus Police Mobile Application[8] that allows the public to report cybercrime online.
Other governmental and non -governmental agencies are also involved in the prevention of cybercrime (more information under section 8.2).

Legislation

The main laws in the field of cybercrime in Cyprus are:

1. The Law ratifying the Convention on Cybercrime (Budapest Convention), L.22(III)/2004. This legislation covers hacking, child pornography and fraud committed via electronic communication and the Internet.
2. The Law that revises the legal framework on the prevention and combating the sexual abuse and sexual exploitation of children and child pornography, L 91(I)/2014. This legislation ratifies the EU Directive 2011/93/EE and covers child pornography, grooming and notice and takedown.
3. The Law ratifying the Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts, L.26(III)/2004. This legislation covers racism and xenophobia via computer systems and the Internet.
4. The Law on the Processing of Personal Data, L.138(I)/2001.
5. The Law on the Retention of Telecommunication data for the investigation of serious offences, L. 183(I)/2007. This legislation transposed Directive 2006/24/JHA. Although the Directive was invalidated by the Court of Justice of the EU, the national law is still valid. The national law is founded on a constitutional provision and it includes specific safeguards for the protection of privacy; for example, communication data are released only following a court order. A case was recently filed with the Supreme Court on the impact of the annulment of the EU Directive on Law 183(I)/2007 and the Supreme Court found that it complied with the European Convention of Human Rights.
6. Law 112(I)/2004 Regulating Electronic Communication and Postal Services.
7. Law implementing Directive 2013/40/EU on attacks against information system, 147(i)/2015.

DECLASSIFIED

[7] https://cybercrime.police.gov.cy/police/CyberCrime.nsf/subscribe_en/subscribe_en?OpenForm
[8] http://mobile.cypruspolicenews.com/landing/Desktop#.VbclTfmm2jw

Capacity Building

The O.C.C. and the Digital Evidence Forensic Laboratory (DEFL) are situated at the Cyprus Police Headquarters in Nicosia and consist of 5 and 10 specialized and trained officers respectively. The head and his assistants are responsible for both offices. Three members of the DEFL have a Masters degree in Computer Forensics and are trainers in the forensic examination of digital evidence. In the framework of funding programmes such as Hercule II and the Internal Security Fund 2014-2020, both the O.C.C. and DEFL were granted funding with the aim of renewing all necessary hardware and software that are used for forensic investigation. Moreover, by means of secondary funding, a specialized training room will be set up in 2016. Hercules II project was finalized on 30/6/2015 while the second project under the Internal Security Fund will be finalized in different phases by 2020. Overall, both offices are at a very good level with regard to capacity building for combating cybercrime.

Training

The personnel of the O.C.C. and DEFL participate in specific training programmes on an annual basis. The majority of these programmes are offered by CEPOL, OLAF, ECTEG, FBI and other organizations. At the same time, the members of the O.C.C. proceeded with the organisation of training for the field officers in Cyprus in cooperation with the Cyprus Police Academy.

In 2014, the O.C.C. provided training sessions to Palestinian Authority officers, as well as to other governmental departments of Cyprus.

Moreover, in the context of "Prevention of and Fight against Crime Programme" of the European Union (ISEC), Cyprus was granted funding for the establishment of the Cyprus Cybercrime Center of Excellence (3CE). This action is coordinated by the Cyprus Neuroscience & Technology Institute, a non-governmental organisation, along with the Office of the Commissioner of Electronic Communications and Postal Regulation, the European University Cyprus, Aditess LTD and the O.C.C., which act as partners.

DECLASSIFIED

The 3CE project will develop short-term, highly focused and specialised training seminars on cybercrime-related issues for public and for private sector participants. Courses will facilitate the exchange and diffusion of tacit knowledge and expertise, familiarise participants with new technologies and tools and improve their day-to-day activities relating to the prevention and combating of cybercrime. The courses will be available to prosecutors and judges, law enforcement officers, university students and civil servants.

Public Awareness

The O.C.C. cooperates closely with other governmental departments, NGOs and the private sector as regards the prevention of cybercrime. A member of the O.C.C. and a representative of the Ministry of Justice and Public Order sits on the Advisory Board of the "*CyberEthics*" project. Moreover, the members of O.C.C. deliver lectures on an annual basis to school students and teachers and other organized groups on the safe use of internet. For example, every year the O.C.C participates in the events organised for the Safe Internet Day. Additionally, in cooperation with the other *CyberEthics* project partners, the O.C.C organised events for the public in order to raise awareness regarding Internet safety. The O.C.C works closely with Internet Service Providers (ISPs), the Pedagogical Institute (Ministry of Education and Culture) and the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR).

As part of prevention policy, the O.C.C., issues and distributes leaflets on Internet safety in both Greek and English to all fifth elementary - grade students in Cyprus (5 000 leaflets). Other organisations involved in Internet safety such as the Pedagogical Institute, OCECPR, CNTI, *CyberEthics* and a number of ISPs, have issued their own educational material. Moreover, in cooperation with the Cyprus Police Press Office, the O.C.C. prepared a short video related to cyber bullying which is accessible via the Internet and is frequently presented on TV.

DECLASSIFIED

Furthermore, with the cooperation of the Cyprus Police Press Office and the Research and Development Department of the Cyprus Police, the O.C.C. launched in January 2015 the Cybercrime Reporting Platform which is accessible via the website *www.police.gov.cy*. In the same period, the Cyprus Police Press Office launched the Cyprus Police Mobile Application which offers useful information and a connection to the cybercrime reporting platform.

Awareness

Since the adoption of the Cybersecurity Strategy, awareness raising is dealt with horizontally under the coordination of OCECPR. Within Action 14 several sub-working groups are focusing their efforts on specific target groups. In this context the Ministry of Education and Culture has a leading role in drafting and implementing the National Strategy for the Safety of Children/students, teachers and parents on the Internet.

International Cooperation

Cyprus cooperates with EU and third countries on the basis of bilateral and multilateral agreements in this field and other channels for exchange of information. The O.C.C cooperates closely with the following organisations:

- Europol/EC3/AWF/ EMPACTS
- EUCTF (European Union Cybercrime Taskforce)
- CIRCAMP (COSPOL Internet Related Child Abusive Material Project)
- ENISA (European Network and Information Security Agency)
- ECTEG (European Cybercrime Training and Education Group)
- CEPOL (European Police College)
- EUROJUST (European Union's Judicial Cooperation Unit)

DECLASSIFIED

- CERT-EU (Computer Emergency Response Team)
- INTERPOL (International Criminal Police Organization)
- European Commission
- EEAS (European External Action Service)
- USA FBI
- VCACITF (Violence Crime Against Children International Task Force) USA FBI.
- Council of Europe (T-CY Assessment)

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

There is no single statistical report related to cybercrime due to the fact that different police departments deal with cybercrime or other Internet -facilitated offences. According to Police Order No. 3/45, the O.C.C. deals with hacking cases, racism via the Internet and child pornography via the Internet. Fraud and other related economic crimes committed via the Internet are investigated by the District Crime Investigations Departments, the Office for Combating Economic Crime and the District Police Stations depending on the financial losses of the victims.

The O.C.C. maintains numerical statistics related to hacking cases and full statistics related to child pornography cases. According to the statistics maintained by the O.C.C., the main trends related to cybercrime in Cyprus are the following:

- Child Pornography- possession and invitation of children to take part in child pornography
- Police Ransomware (cryptolocker)
- DDos attacks
- Man in the Middle- emails scams
- Phishing sites.

DECLASSIFIED

3.3.2. Number of registered cases of cyber criminality

The O.C.C. is the sole agency responsible for the investigation of cases related to hacking and child pornography via the Internet. The "*CyberEthics*", which operates under the umbrella of "Insafe" and "Inhope" programmes, runs a reporting platform for online offences (*www.cyberethics.info*). Thus, "*CyberEthics*" partners (who are state and non state actors) maintain their own statistical reports related to the reported incidents and at the same time these statistics are forwarded to the O.C.C. The O.C.C. maintains numerical statistics for the all investigated offences and full statistics for child pornography offences.

Statistics on child pornography offences

Category	2014	2015
Invitation to participate in child pornography	19	13
Investigations related to the possession of child pornography	87	103
Total number of inquiries	106	116
Forwarded to competent authorities	14	1
Evidence leading to criminal investigation	20	3
Cases sent to court	19	1
Suspended/withdrawn	18	68
Pending in court	18	1
Convicted	1	1
Acquitted		
Under investigation	38	44

DECLASSIFIED

Statistics on hacking cases/illegal access/interference

Offence	2014	2015
Illegal access/interference	14	22
Computer -related forgery	81	22

3.4. Domestic budget allocated for the prevention of and fight against cybercrime and support from EU funding

There are dedicated funds in the national budget for enhancing public awareness of cybercrime.
At the same time, the O.C.C. has been granted European funding (Internal Security Fund) for purchasing specialized equipment in order to enhance its operational capabilities for fighting cybercrime and improve the information exchange process between all relevant responsible authorities. Furthermore, through European funding, training schemes will be developed so as to enhance operational skills for all officials responsible for investigating and prosecuting cybercrime offenders.

The OCECPR has also a dedicated budget for the implementation of actions under the National Cybersecurity Strategy.

DECLASSIFIED

3.5. Conclusions

- Cyprus laid down the National Cybersecurity Strategy in 2013. The document was adopted by the Ministerial Council. The Office of the Commissioner of Electronic Communications and Postal Regulation was established as a body coordinating its implementation. As part of the Strategy the Steering Committee on Cyber Security, which is considered a key player in the field of coordination, was also set up, albeit mainly to deal with implementation of the Strategy rather than cybersecurity itself. The Strategy covers all fields of cybercrime and comprises 4 basic pillars, namely network information security, cybercrime, cyber diplomacy and cyber defence.

- The document is one of the triggers of public and non-governmental activities in this fields, resulting in the establishment of a complex, multifaceted system composed of various public and private bodies responsible for the implementation of the Strategy and for responding promptly to various cyberspace threats. Therefore, it is regarded as creating an opportunity for providing synergies and maximising readiness as well as reaction capabilities. Together with the legal framework, the implementation of the Strategy is a key factor in the further development of cooperation and capacity building in countering cybercrime and strengthening cybersecurity.

- However, it should be noted that proper implementation of the Strategy means ensuring adequate human and financial resources, which, in the opinion of the evaluators, does not seem to be sufficient. Apart from the number of staff, the quality of the public premises influencing working conditions, and expenditure does not create an environment which could be deemed conducive to the further development of anti-cybercrime activity.[9]

DECLASSIFIED

[9] After the on-site visit the evaluation team was informed that the Republic of Cyprus was until very recently (March 2016) under a financial MoU with the EU. Recruitment of police officers was suspended since 2012. Recently, the Ministry of Justice and Public Order and the Cyprus Police have commissioned a study for the restructuring of the Cyprus Police and the needs in personnel will be re-evaluated within that context.

- On the other hand, it should be underlined that the Cypriot authorities have made remarkable progress in using the European funds for the purpose of equipping law enforcement agencies with modern appliances and hardware, indispensable in the field of countering cybercrime. Special attention should be paid in this regard to DEFL, which is, despite very humble working conditions resulting from low-quality premises, properly and well equipped with the IT tools.

- In the opinion of the evaluators, the effective use of the European funds for equipping law enforcement agencies with IT tools, including forensic hardware and software, could be considered as an example of best practice.

- The evaluation team was informed that statistics on cybercrime are kept by different institutions or departments involved in prevention, detection, investigation and prosecution. However, an integrated statistical approach has not been developed, nor have reliable and exhaustive statistics on persons convicted for different kinds of cybercrime. Therefore, the figures relating to cybercrime should be generally aggregated and quickly converted into statistical information, which should be available to all actors involved in cybersecurity.

- Even though the evaluation team was provided with some statistics on cybercrime, in the evaluators' opinion they are not sufficient to build up an overall perception of this phenomenon in Cyprus. Although their gathering and processing may be considered time-consuming and complicated for the public authorities, the statistics serve to provide an insight into the development of cybercrime in Cyprus and the effectiveness of the actions taken to counter it. Moreover, the statistics should cover all the fields deemed important for this kind of crime.[10]

DECLASSIFIED

[10] The authorities in Cyprus reported that they have recognised this issue and the OCECPR and OCC are in contact with the private sector to explore possible ways for collecting more information.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

Cybercrime offences are tried by District Courts or Felony Courts according to the seriousness of the case. No specialized courts and no prosecutors' offices exist to deal with cybercrime offences.

The principle of separation of powers applies in Cyprus and the judiciary is an independent authority. The Prosecution Service is under the administration of the Attorney General's Office.

No further details of the structure of the judiciary could be given due to the absence of the expert of the Attorney General's Office who, according to the programme of the visit, was expected to present this topic and answer relevant questions from the experts.

4.1.2. Capacity and obstacles to successful investigation

Within the framework of "Prevention of and Fight against Crime Programme" of the European Union (ISEC), Cyprus was granted funding for the establishment of the Cyprus Cybercrime Centre of Excellence (3CE). 3CE will provide short-term, highly focused and specialized training seminars on cybercrime-related issues for public and private sector participants. Modules will be developed especially for judges, prosecutors and law enforcement officers.

Moreover, the Cypriot authorities indicated that international cooperation and contribution from specialised organisations such as Europol are considered very important for the successful investigation of many cases.

DECLASSIFIED

On the other hand, encryption, the limited period for data retention (6 months) and the absence of a legal framework to conduct electronic surveillance of private communication, lack of cooperation of foreign partners and long period of time needed to obtain evidence from foreign jurisdictions were reported as the main obstacles faced during the investigation phase of cybercrime. However, problems such as data retention and encryption seems to have more general nature and are reported also by other member states.

Possible solutions to these problems are currently being examined by the Ministry of Justice and Public Order and the police, who are also preparing the legal framework necessary to conduct electronic surveillance of private communications for a limited number of serious offences and/or for national security reasons.

The extension of the data retention period will also be considered further after analysing the implications of the Supreme Court judgement delivered with reference to Law L. 183(I)/2007.
Additionally, as the majority of cybercrime is transnational crime, there are delays in enforcing MLATs with different countries throughout the world. This also hampers effective investigation.

DECLASSIFIED

4.2. Law enforcement authorities

The O.C.C. and DEFL are the offices in Cyprus capable and responsible for the effective investigation of cybercrime. Both offices are situated at the Cyprus Police Headquarters and are supervised by the same Director.

The Office for Combating Cybercrime (O.C.C.)

The specialised body for cybercrime investigation is the Office for Combating Cybercrime of Cyprus Police. The Office was established in September 2007 based on Police Order No. 3/45 in order to implement the Law on the Convention on Cybercrime (Ratifying Law) L.22(III)/2004. This legislation covers hacking, child pornography and fraud committed via electronic communication and the Internet. According to Police Order No. 3/45, the Office is responsible for the investigation of crimes committed via the Internet or via computers and at the same time it is responsible for the investigation of all offences that violate the rules laid down in Law L.22(III)/2004.

It is also responsible for raising awareness about cybercrime. A member of the office sits on the Advisory Board of the consortium called "*CyberEthics*" which is a project that operates under the "Insafe" and "Inhope" programmes in Cyprus for the prevention of cybercrime. Furthermore, the office has trained staff who deliver around 100 lectures on an annual basis to schools and other organized groups. At the same time, the Office organises public events at central points and distributes leaflets in both Greek and English related to raising awareness of cybercrime. Furthermore, the O.C.C. takes part in Action 14 of the Cybersecurity Strategy of the Republic of Cyprus which deals with cybersecurity awareness, including cybercrime.

The Digital Evidence Forensic Laboratory (DEFL)

The DEFL was established in 2009 and is responsible for the effective examination of electronic evidence. DEFL is staffed with specialised officers for the collection and forensic analysis of electronic devices. All members of DEFL are university graduates in academic fields related to their work. Some members also have a Master's degree in the forensic examination of electronic evidence while some of them hold the title of staff trainer. Their mission is the collection and forensic analysis of digital devices as well as the presentation of expert scientific evidence to the courts.

Criminal Investigation Departments

The responsibility for the investigation of fraud via the Internet and other economic crimes committed via the Internet lies with the Criminal Investigation Department of each District. Financial offences committed via the Internet are also investigated by the Financial Crime Unit at Cyprus Police Headquarters.

Within the context of the Convention for Cybercrime, the 24/7 point of contact is the Head of the O.C.C., who is also responsible for the execution of the MLAT requests. The second point of contact is the NCB (Interpol) Nicosia which is responsible for forwarding the requested information to the Head Officer of the Cybercrime Department outside working hours. The Cyprus Police is also the contact point provided for in Law 147(i)/2015 transposing Directive 2013/40/EU.

DECLASSIFIED

4.3. Other authorities/institutions/public-private partnership

The National Cybersecurity Strategy provides scope for using a Public -Private Partnership (PPP) in the prevention of and fight against cybercrime. It is currently under examination by the Cyprus authorities. However, a model of cooperation specifically in the field of prevention and raising awareness has been developed with involvement of the following actors:

- The Office of the Commissioner for Electronic Communications and Postal Regulation
- Non-governmental Organisations such as CNTI and "Hope for Children"
- The Ministry of Education and Culture has the leading role under Action 14 "Awareness" of the National Cybersecurity Strategy
- The Department of Information and Technology Services (Ministry of Finance) functions as the GOV CIRT
- The Ministry of Labour Social Welfare and Insurance is the competent authority for the implementation of Law 91(I)/2014
- The Ministry of Energy, Commerce, Industry and Tourism is the competent authority for the implementation of the E-Commerce Directive
- Internet Service Providers.

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

The Cyprus Police is the only authority in Cyprus responsible for the investigation of cybercrime. As regards prevention and awareness, ever since the National Cybersecurity Strategy was adopted these issues have been dealt with horizontally under Action 14 of the Strategy. The OCECPR is responsible for the coordination of the National Cybersecurity Strategy.

DECLASSIFIED

The OCECPR has also imposed several obligations on Electronic Communications Providers, including Internet Service Providers (ISPs), relating to network and information Security and also to cooperation and the provision of information to emergency services and the police, on related issues. The OCECPR is facilitating discussions between the operators and the police with a view to improving their collaboration in the provision of information, in identifying offenders and blocking websites with illegal content etc. The OCECPR may impose terms and obligations, set by competent authorities, including the police, on related issues, including cybercrime.

According to the Cypriot authorities, there is sufficient cooperation with banks concerning the notification on new payment tools. Banks are making constant efforts to increase security and strengthen the authorisation of online transactions. The OCECPR together with the Central Bank of Cyprus and the Association of Cyprus Banks are facilitating discussions between the operators, the banks and the police with a view to improving their collaboration in the exchange of information.

The Ministry of Education and Culture has the leading role in certain tasks of Action 14 Awareness. The police and other governmental and nongovernmental authorities participate in the work under Action 14.

The Ministry of Justice and Public Order also participates in Action 17 of the National Cybersecurity Strategy where the participants of the 4 Ministries are informed of all work carried out as part of the implementation of the National Cybersecurity Strategy, including awareness-raising activities.

DECLASS

4.4.2. Resources allocated to improving cooperation

In the framework of funding programmes such as Hercule II and Internal Security Fund 2014-2020, both O.C.C. and DEFL were granted funding with the aim of renewing all the necessary hardware and software used for forensic investigation. Moreover, additional funding has been provided to set up a specialized training room at the beginning of 2016. The Hercules II project was finalized on 30/6/2015 while the second project under the Internal Security Fund will be finalized in different phases by 2020. Overall, both offices are at a good level when it comes to capacity building for combating cybercrime. While on the one hand the IT equipment is excellent, the quality of the premises (building) in which the DEFL is located is not.[11]

4.5. Conclusions

- The evaluation team did not have the opportunity to meet members of the Cyprus' judiciary. However, it was reported that there are no specialised prosecutors and judges for cybercrime cases.

- Cyprus Police is responsible for pre-trial proceedings in the area of cybercrime, and for collecting and analysing intelligence information and data. It also provides forensic expertise and is responsible for prevention and deterrence and certain aspects of international cooperation in this field. The O.C.C. is responsible for the investigation of cybercrime as defined in Law L.22(III)/2004. At the same time, the O.C.C. is responsible for the investigation of the cases related to racism and xenophobia via the Internet.

DECLASSIFIED

[11] After the on-site visit the evaluation team was informed on improvements made to the premises visited. New premises are expected to be available by 2016 which will include a training room and new offices.

- During meetings with representatives of the Cyprus Police the latter showed a high level of professionalism and commitment to their work. The representatives of the Cypriot authorities met by the team are involved in investigating and prosecuting cybercrime work in an informal manner, and this works well. Competent persons know their counterparts in the other authorities and therefore get in touch very easily. As such, their work is conducted without unnecessary bureaucratic delays.

- The gathering and admissibility of evidence and the data retention problem in Member States were reported as being the main obstacles to successful investigations. Pursuant to the latest Supreme Court judgment on the impact of the annulment of the EU Directive on data retention on Law 183(I)/2007, the latter is in compliance with the European Convention of Human Rights. Nonetheless, the evaluators recognise the data retention problem as a general one which requires action to be taken at EU level. Moreover, in the evaluators' view, a dialogue with the private sector to seek possibilities to have data retained, as well as to ensure that information is gathered in a way that ensures its admissibility in court, could also be useful.

- It was reported that cooperation with private sector is generally good. There are regular contacts between law enforcement authorities and the private sector. Some difficulties in communication with the banking sector were mentioned.

- However, it was not clear if prosecutors have contacts with the private sector within the existing structure relating to cybersecurity. Therefore, in the opinion of the evaluators, it would be useful to consider the possibility of involving prosecutors in meetings/discussions with the private sector so as to ensure that evidence is gathered in compliance with current legislation and is admissible in court proceedings.

DECLASSIFIED

- Cypriot authorities benefit greatly from using the funding for their projects provided by the EU, e.g. within the framework of "Prevention of and Fight against Crime Programme" of the European Union (ISEC). Thus, the Cyprus Cybercrime Center of Excellence (3CE) was established. In the framework of funding programmes such as Hercule II and Internal Security Fund 2014-2020, both the O.C.C. and the DEFL were granted financial aid with the aim of renewing all the necessary forensic hardware and software used for investigation. Without any such funding they would not be able to function in their fields as effectively as they do. Several authorities, e.g. DEFL, might also benefit from more staff in their offices. Therefore, in the opinion of the evaluators, the use of EU funds is of significant importance in enabling the relevant authorities to work in the most efficient manner and to utilise their full potential. At the same time, the Cypriot authorities should also contribute to providing sufficient funding in the fight against cybercrime.

DECLASSIFIED

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1. Council of Europe Convention on Cybercrime

The Republic of Cyprus is a party to the Council of Europe Convention on Cybercrime (Budapest Convention). The relevant ratification law is L.22(III)/2004.

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

At the time of the evaluation visit, the evaluation team was informed that Law transposing Directive 2013/40/EU on attacks against information system, 147(i)/2015, had been approved by the House of Representatives.

However, prior to the entry into force of the above- mentioned law, Law L22(III) 2004 ratifying the Convention on Cybercrime had criminalised the following acts:

Illegal access to a computer system (Article 4)
A person who intentionally and without entitlement accesses all or part of a computer system by infringing security measures commits an offence punishable by imprisonment not exceeding five years or a fine not exceeding EUR 34,172 or by both penalties.

DECLASSIFIED

Illegal system interference (Article 7)

A person who intentionally and without entitlement seriously hinders or interrupts the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or preventing access to these data commits an offence punishable by imprisonment not exceeding five years or a fine not exceeding EUR 34,172 or by both penalties.

Illegal data interference (Article 6)

A person who intentionally and without entitlement destroys, deletes, alters or conceals computer data commits an offence punishable by imprisonment not exceeding five years or a fine not exceeding EUR 34,172 or by both penalties.

Illegal interception of computer data (Article 5)

A person who intentionally and without entitlement interferes with technical equipment on computer data not broadcast publicly, from or within a computer system, commits an offence punishable by imprisonment not exceeding five years or by a fine not exceeding EUR 34,172 or by both penalties.

Misuse of devices (Article 8)

This article prohibits the intentional and unauthorised production, distribution, procurement for use, import, or provision or possession by any other means of computer misuse tools and makes any such act an offence punishable by imprisonment not exceeding five years or a fine not exceeding EUR 34,172 or by both penalties.

When imposing sentence, courts take into account aggravating or mitigating circumstances related either to the offence (circumstances under which it was committed) or the offender (personal circumstances).

DECLASSIFIED

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

Cyprus transposed Directive 2011/93/EU of 13 December 2011 on combating sexual abuse and sexual exploitation of children and child pornography into national law in July 2014 in the form of Law 91(I)/2014. The implementation is fairly recent and has not yet been evaluated. The Cypriot authorities reported no particular difficulties during the short period since the enactment of the law.
Law 91(I)/2014 states that consenting sexual activities between two children who have not reached the age of consent and who are of a similar age and psychological and physical maturity do not constitute an offence, provided that such activities do not include violence or exploitation (the age of consent is seventeen (17)). Similar provisions are included governing relationships between adults and children between whom the age difference is 3 years or less.

Provisions on aggravated circumstances are included in legislation, such as Law 91(I)/2014, specifying that where the child depicted in child pornography is aged under the age of thirteen (13) years, the offender is subject to imprisonment for life.
Moreover, the following rules were adopted to criminalise child abuse and child pornography:

Production of child pornography

A person who intentionally and without entitlement produces child pornographic material via a computer system commits an offence punishable by imprisonment not exceeding ten years or a fine not exceeding EUR 42,175 or by both penalties (L. 22(III)/2004, Article 11(1)(a))

Offering or making available child pornographic material

A person who intentionally and without entitlement offers or makes available child pornography through a computer system commits an offence punishable by imprisonment not exceeding ten years or a fine not exceeding EUR 42,175 or by both penalties (L. 22(III)/2004, Article 11(1)(b))

DECLASSIFIED

Distributing or transmitting child pornography through a computer system

A person who intentionally and without entitlement distributes or transmits child pornography through a computer system commits an offence punishable by imprisonment not exceeding ten years or a fine not exceeding EUR 42,175 or by both penalties (L. 22(III)/2004, Article 11(1)(c))

Procuring child pornography through a computer system for oneself or for another person through a computer system

A person who intentionally and without entitlement procures child pornography through a computer system for him or herself or for another person commits an offence punishable by imprisonment not exceeding ten years or a fine not exceeding EUR 42,175 or by both penalties (L. 22(III)/2004, Article 11(1)(d))

Possessing child pornography in a computer system or on a computer-data storage medium

A person who intentionally and without entitlement possesses child pornography in a computer system or on a computer-data storage medium commits an offence punishable by imprisonment not exceeding ten years or a fine not exceeding EUR 42,175 or by both penalties (L. 22(III)/2004, Article 11(1)(e))

Possessing child pornography in a computer system or on a computer-data storage medium

Subject to the provisions of Article 12, anyone who obtains or possesses child pornographic material is guilty of a felony and, upon conviction, is liable to imprisonment not exceeding ten years (10) years.
Law 91(I)/2014, article 8(1)

Access to child pornographic material

A person who knowingly accesses child pornography through information technology and communications is guilty of a felony and, upon conviction, is liable to imprisonment not exceeding ten years (10) years (Law 91(I)/2014 article 8(2))
Law 91(I)/2014, article 8(3)
Whoever distributes, disseminates or transmits child pornography is guilty of a felony and, upon conviction, is liable to imprisonment not more than fifteen (15) years.

DECLASSIFIED

Law 91(I)/2014, article 8(4)

Offering or making available child pornographic material

Law 91(I)/2014, Article 8(5)

Subject to the provisions of Article 12, anyone who produces child pornographic material is guilty of a felony and, upon conviction, subject to imprisonment not exceeding twenty (20) years.

Computer- related solicitation or 'grooming' of children

Anyone who causes the participation of a child in pornographic shows or recruits a child so that he/she will participate or gain profit from the child's participation in pornographic shows or exploits the child in other ways for that purpose is guilty of an offence and if convicted is liable to a term of imprisonment not exceeding twenty years.

(2) Forcing a child to act as mentioned in (1) above, 25 years

(3) Watching pornographic shows, 15 years imprisonment

(4) Anyone who causes or proposes through information communication technology or in person the participation of a child who has not reached the age of consent in a pornographic show for the purpose of allowing that show to be watched by either himself/herself or a third person shall be guilty of a felony and, upon conviction, subject to imprisonment not exceeding ten (10) years.

(5) A person who recruits a child for or causes a child to participate in child prostitution for the purpose of gaining profit shall be guilty of a felony, and, upon conviction, subject to imprisonment not exceeding 25 years.

(6) Forcing a child into child prostitution, 25 years

Law 91(I)/2014 Article 7(1)

Law 91(I)/2014 article 9(1)

Subject to the provisions of Article 12, anyone who proposes to a child who has not reached the age of consent, through information, communication technology, to come into contact with intent to perform sexual intercourse with him/her or for the production of child pornography or for the sexual exploitation of a child, and this proposal led to actions that led to a meeting, shall be guilty of a felony and, upon conviction, subject to imprisonment not exceeding ten (10) years.

DECLASSIFIED

Law 91(I)/2014 Article 9(2)

Subject to the provisions of Article 12, anyone who, through information communication technology, invites or approaches a child who has not reached the age of consent, and attempts to acquire, or attempts to have access, or acquires or obtains access to child pornographic material which depict that child, is guilty of a felony, and if convicted, is subject to imprisonment not exceeding ten years.

C/ Online Card fraud

Law 22(III)/2004 ratifying the Convention on Cybercrime lays down rules criminalising computer - related fraud and forgery.

Computer- related fraud

A person who intentionally and without entitlement, acting with intent to defraud, causes a loss to the property of another person by:

a inputting, altering, deleting or suppressing computer data,

b any interference with the functioning of a computer system, with fraudulent intent or intent to procure, without entitlement, an economic benefit for oneself or for another person commits an offence punishable by imprisonment not exceeding five years or a fine not exceeding EUR 34,172 or by both penalties (L. 22(III)/2004, article 10(a)(b))

Computer- related forgery

A person who, intentionally and without entitlement, and with intent to defraud, inputs, alters, deletes, or suppresses computer data, in such a way that non-authentic data created as a result of these interventions are presented or used for legal purposes, as if they were authentic, regardless of whether the data are directly readable and intelligible, commits an offence punishable by imprisonment not exceeding five years or a fine not exceeding EUR 34,172 or by both penalties (L. 22(III)/2004, Article 9).

Sending or controlling the sending of spam

Any person who violates the provisions of Article 10 on spamming shall be guilty of an offence and if convicted liable to a penalty not exceeding EUR 8,250. In the case of repeated offences the penalty may be doubled. It is also an administrative offence. (Law 156 (I)/ 2004, Article 23).

DECLASSIFIED

5.2. Procedural issues

5.2.1. Investigative Techniques

The Ministry of Justice and Public Order has initiated a dialogue with other competent authorities for the preparation of new legislation which will allow surveillance of private communications for the purpose of preventing and investigating serious offences or for national security reasons. Such surveillance will be fully in line with Article 17 of the Constitution which protects the right to privacy.

The Ministry of Justice and Public Order stated that it closely follows all developments with regard to the annulment of the Data Retention Directive and is in close contact with the police and the Cyprus Legal Service for the possible adoption of any future measures.
After the on-site visit the evaluation team was informed that Law for access to recorded data which contain private communications was approved by the House of Representatives and is in force now.

The following investigative techniques are permissible under national law:
• search and seizure of information systems/computer data; (Code of Criminal Procedure)
• preservation of computer data; (Law 22(III)/2004)
• order for stored traffic/content data; however, only for stored traffic data (Law 183(I)/2007)
• order for user information. (Law 183(I)/2007).
National law does not allow for real-time interception/collection of traffic/content data. However, Law 183(I)/2007 forces ISPs to store telecommunication and traffic data for the purpose of investigation for a period of six months. The use of specialised software such as Child Protection System (CPS) and NetClean facilitate cybercrime investigations.

DECLASSIFIED

5.2.2. Forensics and Encryption

The representatives of the police highlighted that encryption currently poses major problems for forensic examiners around the world. Encryption problems are encountered mainly during investigations into hacking cases and illegal gambling cases. Nonetheless, there are tools at the Digital Forensic Laboratory that make it possible to decrypt some forms of encryption such as PRTK via the FTK Platform. However, this is not always effective.

If there is a need to forward evidence to other authorities for decryption, this is always done via the Europol and Interpol channels. Decryption is not carried out in cooperation with private companies. There are no specialised decryption centres in Cyprus. The O.C.C. has therefore proposed the introduction of special legislation to force computer users and administrators to deliver their encryption passwords during an investigation. Refusal will be regarded as an offence. The proposal is being examined in light of the possible impact it might have on the right of silence of the accused.

5.2.3. E-Evidence

There are no special admissibility rules related to e-evidence. The e- evidence is subject to the same rules of evidence as paper documents and is admissible under the Evidence Law, Cap 9. However, the nature of e – evidence, and the ease with which it can be manipulated or falsified, may create issues with regard to admissibility that do not arise with other evidence, for example more evidential material may be needed such as forensic tool analysis or expert evidence by forensic investigators.

E-evidence is collected from the crime scene on the basis of international standards. After collecting and sealing the evidence, the investigator delivers it to DEFL for examination. The procedure of collecting, transporting and examining the e-evidence follows the rules of evidence and the chain of

DECLASSIFIED

custody is always fully documented, based on Police Order 3/17 and the Forensic Lab Manual. For each item of e-evidence, the forensic examiners create a forensic image and then proceed with their analysis, using approved forensic tools such as FTK and IEF. The exported evidence is stored on external drives or CDs/DVDs by the forensic examiner before being delivered for review by the investigator. In child pornography cases, further analysis is carried out by the investigators via the NetClean software and all images are checked against the ICSE database. The exported evidence, along with the investigator's report and the forensic examiner's report, is presented to the court and is available for use during the trial.

5.3. Protection of Human Rights/Fundamental Freedoms

The right to privacy and freedom of communication are protected under Articles 15 and 17 of the Cyprus Constitution. Specific provisions for the protection of fundamental rights and freedoms are also included in the relevant legislation (specified under section 3.2).
Furthermore, the Processing of Personal Data Law 138(I)/2001 regulates the safeguarding of personal data.

In some cases but under very strict conditions, e.g. under Law 183(I)/2007 (Data Retention Law) privacy rights may be limited but a court order is required at all times. Furthermore, the Law only applies to very serious offences punishable by a minimum term of 5 years' imprisonment.

DECLASSIFIED

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

Under Law 22(III)/2004, Article 22 of the Budapest Convention applies to jurisdiction with regard to cybercrime acts committed outside the territory of Cyprus. Additional provisions on jurisdiction are also included in Law 147(i)/2015 transposing Directive 2013/40/EU on attacks against information systems identical to those included in the Directive.

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

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

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

The Cypriot authorities indicated that MLA instruments must be used if the cloud is hosted in other countries. This might cause delays.

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

According to the Cypriot assessment, Law 147(i)/2015 transposing Directive 2013/40/EU on attacks against information systems is expected to further improve the investigation of cybercrime committed outside the national territory since it provides for wider powers on jurisdiction. It also widens the scope of offences committed against information systems instead of computer systems as currently defined in the Budapest Convention.

DECLASSIFIED

5.5. Conclusions

- Cyprus ratified the Council of Europe Convention on Cybercrime in 2004 (Law 22(III)/2004), but has not transposed into national legislation procedural measures which would empower competent national authorities to record content data in real-time in cybercrime cases for criminal offences laid down in Section 1 of this Convention. Consideration should therefore be given to how to adopt legislative or other measures so that they are fully in accordance with Article 21 of the Budapest Convention. [12]

- Law 91(I)/2014 transposes Directive 2011/93/EU on combating the sexual abuse and the sexual exploitation of children and child pornography and provides for the better implementation of the Council of Europe's Convention on the protection of children against sexual exploitation and sexual abuse (Lanzarote Convention).

- Measures to combat computer-related fraud and forgery are provided for in Law L. 22(III)2004. Moreover, sending or controlling the sending of spam is made punishable by Law 156 (I)/ 2004.

- 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 Evidence Law.

DECLASSIFIED

[12] After the on-site visit the evaluation team was informed that the Ministry of Justice and Public Order is examining amendments to Law 92g(I)/1996 which safeguards the confidentiality of private communication. Such amendments would empower the interception of private communication in real time by competent authorities subject to the limitations stated in Article 17 of the Cyprus Constitution.

- Encryption is considered to be a challenge. However, the O.C.C. has proposed the introduction of special legislation to force computer users and administrators to deliver their encryption passwords during an investigation. Refusal will be regarded as an offence. The proposal is being examined in the light of the impact it might have on the right of silence of the accused.

- There are no special provisions on Cyprus jurisdiction concerning cybercrime. The newly adopted Law 147(i)/2015 transposing Directive 2013/40/EU on attacks against information systems is expected to further improve the investigation of cybercrime committed outside the national territory since it provides for wider powers on jurisdiction.

- Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of jurisdiction in criminal proceedings was transposed into the national law. No conflicts of jurisdiction have been registered so far.

DECLASSIFIED

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1. Nature of cyber attacks

Among its duties the Department of Information Technology Services (DITS) performs the role of the Internet Service Provider (ISP) for the Cyprus Public Service. As far as the nature of recent attacks is concerned, no major/serious incidents were reported.

The categories of attack were the following:

- Invalid packets

- Malformed HTTP Filtering

- Botnet Prevention

- TCP SYN Flood Detection

- ICMP Flood Detection

All those attacks were automatically blocked with no user intervention by our DDOS system.

6.1.2. Mechanism for responding to cyber attacks

The Department of Information Technology Services (DITS) was designed by the Government as the Government CIRT (Computer Incident Report Team) of Cyprus (Cyprus GOVCIRT). With the assistance of the ITU – IMPACT and the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR), DITS set up the technical infrastructure needed and the CIRT portal (http://www.cirt.gov.cy). Furthermore, extensive training was delivered by ITU – IMPACT regarding CIRT. Currently, DITS is in the process of defining the internal policies regarding the governance of the Cyprus GOVCIRT.

DECLASSIFIED

The development of a National CERT is under examination within the framework of the implementation of the National Cybersecurity Strategy. The setting up of a National CERT would be in line with Action 38 of the Pillar III of the Europe 2020 Strategy that incentivises Member States to establish by 2012 a well-functioning network of CERTs at national level covering all of Europe, as well as the NIS Directive The European Commission invited Member States to strengthen cooperation between the existing National CERTs and to expand existing cooperation mechanisms like the European Governmental CERTs Group.

The police cooperate with private companies reporting a cyber attack to help them resolve problems and investigate the offence.

DITS, even though it is not a law enforcement agency, takes all actions necessary to prevent cyber attacks and also carries out data – analysis depending on the case. However, analysis of high – volume data may not always be feasible. DITS is in close contact with the O.C.C.

Moreover, critical infrastructure operators in the field of electronic communications have specific legal and regulatory obligations on network and information security which cover availability, cyber attacks, prevention and mitigation measures. Operators also have reporting obligations related to incidents affecting availability of networks and services and data breaches.

In the opinion of the Cypriot authorities, further work is needed in order to ensure that operators provide all necessary information to the police, including IP addresses, filtering tools, and that they restrict access to illegal content and access to other information during investigations etc.
Efforts are also focused on precautions to the public and private confidentiality of the banks. However, the banks and the financial sector are under no general obligation to report card fraud or forgery offences. This may be put down to the low number of cases detected. According to the statistics given by the O.C.C. for serious cases involving Internet fraud, 36 cases were registered in 2013, 52 cases in 2014 and 64 cases in 2015 (until November 2015). Credit card fraud is at a very low level, with only 3 cases for 2015 (until November 2015). However, the O.C.C. has noticed an increasing number of such cases from year to year.

DECLASSIFIED

According to the latest Europol Quantitative Reports on Cybercrime for Q3 2015, the top 5 malware threats to Cyprus were Conficker, Brontok, Ammyy, Gamarue and Scar, the last being a Trojan that redirects web browser navigation away from certain online financial websites to another IP address and the destination server and page could host an imitation logon screen for the purpose of capturing user-entered credentials.

6.2. Actions against child pornography and sexual abuse online

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

Cyprus uses the NetClean software to identify victims of child pornography.
If images/videos are not deleted, an entity commits an offence as laid down in Article 30 of Law 91(I)/2014. This states that anyone who fails to report a case of child pornography that was made known to him/her commits an offence and is liable to imprisonment of up to (15) years.
Under the provisions of Article 11(3) (a) of the same Law, ISPs which offer services or Internet access within the territory of Cyprus have an obligation, when notified, to take appropriate action to interrupt access by Internet users of such material. If the ISP fails to delete or block access to this material, it commits an offence and is liable to imprisonment not exceeding three years or to a fine not exceeding 170,000 euro or to both penalties.

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

Sexual exploitation/abuse online, sexting and cyber bullying are addressed through general content and educational activities.

Regarding cyber bullying, Cyprus submitted two proposals for European funding under the Daphne call in order to address the issue in more depth.

DECLASSIFIED

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

Article 10(2) of the Law of 2014 on the Prevention and Combating of Sexual Abuse and Sexual Exploitation of Children and Child Pornography Law provides that anybody who organizes trips for the purpose of any form of sexual exploitation and/or sexual abuse of children is guilty of a crime. It also provides for sanctions up to 10 years' imprisonment.

Moreover, on 15/04/2014 Cyprus enacted a revised legal framework on the prevention and combating of human trafficking and exploitation of persons and the protection of victims (Law 60(I)/2014).

No specific measures have been developed to counteract real -time, web-based child pornographic performance.

Through the Safer Internet Programme forming part of the Connecting Europe Facility (CEF) and more specifically the *CyberEthics*project funded by the European Commission Innovation and Networks Executive Agency (INEA) a helpline and hotline are available. The helpline and hotline were run by the Pancyprian Coordinating Committee for the Protection and Welfare for Children (PCCPWC), one of the *CyberEthics* project partners, although since last January 2015, in the recent project contract, CNTI a non-profit organisation runs the two lines. With the ending of the current contract in June 2016, it is considered that the Ministry of Education and Culture (taking advantage of its Educational Psychology Services) can support the helpline and hotline.

DECLASSIFIED

Content and tools have been developed and are constantly being updated and enriched for the safe use of the Internet along with educational programmes for pupils, teachers and parents. All content is available under Creative Common License on the Cyprus Pedagogical Institute portal www.pi.ac.cy/internetsafety, and an educational package has been given out to all schools (which is also available in digital form on www.pi.ac.cy/InternetSafety/eSafeSchool.html). At the same time, content that is being produced by pupils and teachers through the various *Safe Internet* programmes is shared online, such as the short videos produced by students on the yearly competition and the material and tools produced by the Young Coaches for the Internet [13].

The Ministry of Education and Culture collaborates closely with other organisations and promotes content and tools produced by partners such as Microsoft, the Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR), the non-profit organisation CNTI, the Cyprus Telecommunications Authority, and the MTN telecommunications provider etc.
Content and tools emphasize the critical and responsible use of the Internet so as to be safe online while at the same time they aim at any online behaviour on the part of the pupils that could be illegal and harm others. Going further and approaching the pupils as victims or actors, the content and tools aim at the pupils' role as witnesses in order to prevent and/or report of cybercrime.

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

The O.C.C. deals with child pornography. It is concerned with the investigation of serious crimes committed through the Internet, with offences related to computers and with conducting Internet searches in connection with the distribution of child pornography in violation of Laws 22(III)/2004 and 91(I)/2014.

DECLASSIFIED

[13] www.pi.ac.cy/InternetSafety/drastiriotites_diagonismoi.html and www.pi.ac.cy/InternetSafety/YoungCoaches.html

The main duty of the O.C.C. is the investigation of child pornography and hacking cases as well as the following:

- monitoring of the cases that might be under investigation by other departments and are connected with Internet-related crimes;
- co-operation with investigators from other departments;
- co-operation with officers from other organizations;
- organisation of training sessions;
- preparation of statistical reports;
- participation in events and lectures;
- keeping up-to-date with the latest technology in the area.

The O.C.C. is staffed by 5 investigators who work shifts (0700-1900) and two administrative officers.

The provisions of Article 11 of Law 91(I)/2014 authorise the police and courts to block access/removal of content and/or to take down web pages. In practice, after receiving information regarding material involving child sexual abusive, the O.C.C. proceeds with the examination of the material. Upon confirming that the material that is related to CSE, the O.C.C. immediately sends the information via email to all the ISPs in Cyprus in order to interrupt access and at the same time to provide them with log files and other information. There is no automated procedure which is followed for communication between police and ISPs.

However, under the provisions of Article 11(3) (a) of Law 91(I)/2014, ISPs who offer services or Internet access within the territory of Cyprus, have an obligation when notified to take appropriate action to interrupt access by Internet users to such material (child pornographic material). If the ISP fails to delete or block access to this material, it commits an offence for which the penalty is imprisonment not exceeding three years or a fine not exceeding EUR 170,000 or by both penalties
Some ISPs in Cyprus use specialised filters like Clean Field in order to filter websites for child pornographic material.

DECLASSIFIED

If the material is hosted in a country outside Cyprus, LEAs are informed via Europol and/or Interpol so that they can act accordingly. At the same time, ISPs in Cyprus are informed via email so that access to the material by users in Cyprus can be blocked.

6.3. Online card fraud

6.3.1. Online reporting

Citizens and companies report online card fraud offences to the police except when the cases concern very small sums of money. In such cases they prefer to cooperate with the banks to solve the problem.

All ISPs are supervised by OCECPR under L. 112(I)/2004. Furthermore, Law 187(I)/2007 obliges the ISPs to keep traffic and user identification data for a period of six months. Moreover, pursuant to Article 11 of the Law 91(I)/2014, the police and courts can order the ISPs to block access/remove content/take down web pages.

6.3.2. Role of the private sector

There is sufficient cooperation with banks and the private sector, especially concerning the notification of new payment tools. Banks are making constant efforts to increase security and strengthen the authorisation of online transactions.

DECLASSIFIED

The OCECPR has imposed several obligations on Electronic Communications Providers, including ISPs on Network and Information Security, and as regards cooperation and the provision of information to emergency services and the police, on related issues. The OCECPR is facilitating discussions between the operators and the police to improve their collaboration in the provision of information, in identifying offenders, in blocking websites with illegal content etc. OCECPR may impose terms and obligations set by competent authorities, including the police, on related issues, including cybercrime.

The role of the financial sector for the Cypriot economy is crucial. According to widely available sources, it generates roughly 45% of the country's GDP. It may explain complex relations between the public authorities and the financial institutions and the government's rather consensual rather than commanding approach to that sector. Therefore, in the evaluators' view, close cooperation between these actors should be achieved to improve the effectiveness of cybercrime policy, specifically with regard to cyber frauds and cyber attacks.

DECLASSIFIED

6.4. Conclusions

- The police cooperate with private companies reporting a cyber attack to help them resolve problems and investigate the offence. It is also in close contact with DITS to prevent cyber attacks and to receive data – analysis, depending on the case.

- Cyprus established a governmental CIRT which is operational. DITS set up the technical infrastructure needed and the CIRT portal. However, it does not play the role of a national CERT to provide protection for private companies and citizens offering immediate response services to victims of cyber attacks, publishing alerts concerning online threats or offering other information to improve computer and network security. Therefore, consideration should be given to establishing a national CERT as a central body to prevent threats to the security of public information systems and strengthening the resilience of the Cyprus cybersecurity system.

- Critical infrastructure operators in the field of electronic communications have specific legal and regulatory obligations relating to network and information security. These cover cyber attacks, prevention and mitigation measures. Operators have also reporting obligations related to incidents affecting the availability of networks and services and data breaches. However, in the opinion of the Cypriot authorities, further work is needed in order to ensure that operators provide the police with all necessary information, including IP addresses, filtering tools, restricting access to illegal content and access to other information during investigations etc.

- The courts and the police are the authorities that can coordinate the blocking of access/removal of content/take down of web pages. However, there is no legal provision that forces the ISPs to filter child pornography on the Internet (Article 11 of Law 91(I)/2014).

- Cyprus has an excellent system for educating children in cybercrime matters, with professionals strongly devoted to the issue, using modern techniques, such as children teaching children (young coaches). In the opinion of the evaluators, this should be regarded as an example of best practice.

- According to the statistics on the number of cybercrime reported to the police or by the police, the majority of cases are related to online child abuse. There are far fewer cases of cyber attacks and payment card frauds reported. Taking that into account, in the opinion of the evaluators, Cyprus does not fully reflect current cybercrime threats.

- Multifaceted cooperation between public authorities and the financial sector could work to the benefit of both and significantly increase the level of cybersecurity in Cyprus. At the moment, the public authorities do not cooperate directly with the banks and other financial institutions. Interaction between these entities is left to the central bank, playing the role of intermediary. The evaluators believe ,that such an approach seems to hamper the effectiveness of the cooperation specifically when countering cybercrime.

DECLASSIFIED

- Therefore, in the evaluators' view, Cyprus should foster cooperation between law enforcement authorities, prosecutors and the private sector, especially banks, in order to establish a sustainable reporting mechanism for cyber attacks affecting both citizens and the private sector.

- One of the priorities of the SOCTA 2013 is cybercrime which covers three sub-priorities: child sexual abuse, card fraud and cyber attacks. Cyprus takes part in the EMPACT operational action plan child sexual abuse sub-priority. However, Cyprus should consider joining the cyber attacks sub-priority as well. Regarding the actions to be carried out in 2016, the emphasis is on close cooperation between law enforcement agencies, CERTs, industry and academia and there are some tailor-made activities on the promotion of best practices in the area of information and intelligence exchange between banks and law enforcement agencies. According to the information forwarded to the evaluation team, the O.C.C. participates in EMPACT cyber attacks since 1.1.2016.

DECLASSIFIED

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

Law 102(I)/2011 regulates all formal requirements and specific procedures for cooperation with Europol.

Law 112(I)/2004, as amended, does not contain any specific procedures in relation to cybercrime cases. However, it contains general provisions for the representation of Cyprus in international organisations like ENISA through OCECPR, ITU and ICANN etc., depending on competencies.

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

The Cypriot authorities consider the role and contribution of Europol/EC3, Eurojust and ENISA as very important in dealing with cybersecurity and cybercrime due to the nature of these offences. In their opinion, they can actively support the European Commission and the Member States in international cooperation based on their experience and expertise in their field. They can act as advisors and participate in related activities to support the competent European authorities.

DECLASSIFIED

Europol's contribution is regarded crucial for the investigation of cybercrime. The Darkode case is a recent example of the close cooperation between the Cyprus Police and EC3. During this operation, the Cyprus Police traced and questioned a suspect in Cyprus related to the case while there was a direct communication with all involved parties, Member States and third countries. Upon analysis, all information packages were disseminated via EC3 with the information exchange process with EC3 still ongoing. Overall, the Darkode case is generally considered as a successful international operation. Another recent example of the cooperation between the Cyprus Police and Europol is the Daylight Operation related to child pornography which took place within the context of EMPACT CSE Action 5.2. The cooperation between the Cyprus Police and EC3 is of the utmost importance and the Cyprus Police are satisfied with the level of cooperation.

OCECPR represents Cyprus on the ENISA Management Board and in other ENISA Committees and it is responsible for cooperating with the Agency on security- and cyber -related issues. It cooperates with ENISA and has already received general assistance on related issues. Although there has not yet been any cooperation on a specific case, OCECPR is seeking more operational cooperation with ENISA in the near future on specific issues, including the handling of cyber attacks and other incidents which affect networks and personal data.

DITS and OCECPR had cooperated with ENISA in the creation of the Cyprus GOVCIRT.
Furthermore, ENISA provided assistance to the Cyprus authorities in conducting the national cyber risk assessment which is currently ongoing. OCECPR considers the ENISA activity in the fields of security and cybersecurity, including cooperation on cybercrime, as very positive It pointed out, however, that ENISA should seek active cooperation with Europol/EC3 and Eurojust where necessary, assisting their respective activities and avoiding overlap.

The Head of the O.C.C. participates in the Europol EUCTF. A member of the O.C.C. also participates in the EMPACT CSE.

DECLASSIFIED

7.1.3. Operational performance of JITs and cyber patrols

Cyprus has not yet participated in JITs. OCECPR has participated only in ENISA cyber exercises on NIS.

7.2. Cooperation between the Cyprus authorities and Interpol

Interpol is the channel used for exchanging operational information and requests with third countries. Moreover, for the last four years the ICSE database for victim identification has been used by the O.C.C.

7.3. Cooperation with third states

The cooperation with third countries regarding the investigation of police cases is based on bilateral and multilateral agreements. In the area of cybercrime and more specifically in the areas of investigating and raising awareness on child pornography, the O.C.C. has participated in different initiatives such as:

- Innocent Images International Task Force (IIITF) or Violent Crimes Against Children International Task Force (VCACITF);
- Global Alliance Against Child Sexual Abuse Online; and
- Council of Europe TC-Y.

Moreover, Cyprus has made use of operational and strategic agreements signed by Europol/EC3 with third countries and other organisations. Within the context of these agreements, the analysis and exchange of information regarding cybercrime has speeded up, with positive results for the investigation of cybercrime. There are a lot of examples of successful operations that have taken place within this framework.

DECLASSIFIED

7.4. Cooperation with the private sector

When private companies have their headquarters in third states, the O.C.C. applies directly to the local branch that is responsible pursuant to national legislation in order to deliver the requested information. If deemed necessary, a court search warrant can be issued for purposes of effective investigation.

Cyprus tries to overcome obstacles to cross-border cooperation in the specific area of online card fraud by strengthening channels of cooperation with other member states.

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

Law 23(I)/2001 on International Cooperation in Criminal Matters is the national law applicable to MLA requests. In addition, MLA is carried out on the basis of bilateral agreements and conventions such as the European Convention on Mutual Assistance in Criminal Matters, Law 2(III)/2000 and the Convention on Cybercrime Law 22(III)/2004.

The Ministry of Justice and Public Order is the central authority for receiving and sending requests for mutual legal assistance. For the purpose of simplifying and improving international cooperation a Unit for International Legal Cooperation has been established within the Ministry of Justice and Public Order. A written letter of request must be sent by email, fax or post.

The Ministry of Justice and Public Order receives incoming requests from abroad and sends out MLA requests. Incoming requests are evaluated by the Ministry and forwarded for execution to the competent judicial authority in Cyprus. Regarding outgoing requests, the Ministry also collects requests received internally and sends them abroad.

DECLASSIFIED

The Ministry of Justice and Public Order uses the EJN very frequently, as it seems to be quite efficient and contributes to swift and smooth cooperation among Member States. Eurojust is also used in order to obtain fast responses.

The most common reason for the MLA requests is the gathering of evidence leading to the end user. Urgent requests are treated with priority. Depending on the requested actions, the response time may vary from several months to over a year.

For the purpose of executing requests, the O.C.C. seeks information and evidence related to IP addresses, date and time of access, creation details, log files or other data relevant to the identification of end user details. Furthermore, the O.C.C. requests written statements from computer systems administrators if needed.

If there is a need for data preservation before the official MLA is sent, the O.C.C. contacts the requested country via the Interpol or Europol channel. At the same time, under the Budapest Convention the O.C.C. has the ability to request certain information via direct communication or by using the Interpol channel. Furthermore, in cases where the requested hosting administrator is able to cooperate, the O.C.C. can apply directly to him/her via email and request data preservation.

The contact point (Head of the O.C.C.) follows the instructions of the Director of Department C at police headquarters and is responsible for the execution of all requests related to cybercrime as defined by Police Order 3/45. The second point of contact (NCB Interpol Nicosia) acts on the instructions of the Director of the European Union and International Police Cooperation Directorate and is not authorized to execute such requests. Instead, its role is limited to sending the requests.
In cases where the request is sent directly to the point of contact (Head of the O.C.C.), the request is then evaluated and executed. This procedure is followed when there is no need for a MLAT request.

DECLASSIFIED

Upon the execution of the request, the NCB Nicosia is informed for coordination purposes only. In cases where a MLAT request is required, the NCB Nicosia is informed in order to forward the official answer to the country which has sent the request. Generally, the requests that can be answered without the need for a MLAT are only those where the police possess all information and there is no need to apply to the court in order to get authorisation to access the information requested.

Regarding statistics on the number of MLA requests received on cybercrime: 12 requests were received in 2014 and 6 in 2015.

Certain obstacles were mentioned in relation to the swift cooperation with the USA. The representatives met underlined that in terms of international assistance, the key factor is smooth and fast cooperation with the USA, as many popular Internet servers are situated within its jurisdiction. They complained about quality of this cooperation, especially in the field of data retention and the disclosure of the IP addresses of Facebook and other social networks' accounts holders. In the opinion of the evaluators, the issue of database accessibility of the Internet social networks originating in America is a constant problem that affects all Member States.

7.5.2. Mutual recognition instruments

Cyprus has not used mutual recognition instruments for the purpose of cybercrime cases.
However, Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence has been used in the course of requests submitted by other Member States to the relevant authorities in Cyprus, which are the Ministry of Justice and Public Order and the Unit for Combating Money Laundering-MOKAS. Indeed, in a number of cases, freezing orders obtained in other Member States have been registered and enforced in Cyprus following the procedure provided for in the abovementioned Framework Decision.

DECLASSIFIED

7.5.3. Surrender/Extradition

Offences listed in the Framework Decision on the European Arrest Warrant are punishable and extraditable under national law. Cybercrime offences include, sexual exploitation of children and child pornography, computer- related crime, forgery of means of payment, racism and xenophobia committed through the Internet.

The Ministry of Justice and Public Order is the central authority for receiving, sending and deciding on requests for surrender/ extradition. A formal request for extradition needs to be sent either directly or through diplomatic channels.

No specific procedures or conditions need to be fulfilled for requests related to cybercrime. Urgent requests are treated with priority.

Regarding statistics, 12 EAWs have been issued in 2014 for cybercrime offences. 1 extradition request was received for a cybercrime offence in 2014.

Moreover, one extradition request has been received from the USA. It was based on the Extradition Treaty between the United States of America and Cyprus, signed on 17/6/1996, and the instrument as referred to in Article 3(2) of the Agreement on Extradition between the United States of America and the EU, signed on 15/6/2003 as to the application of the Extradition Treaty between the United States of America and Cyprus with Annex signed on 20/1/2006.

DECLASSIFIED

7.6. Conclusions

- Law 102(I)/2011 and Law 112(I)/2004 regulate formal requirements for the cooperation with Europol, Eurojust and ENISA. However, they do not contain any specific procedures in relation to cybercrime cases.

- Cyprus acknowledges the support provided by all EU agencies. The Cypriot authorities consider the role and contribution of Europol/EC3, Eurojust and ENISA as very important in dealing with cybercrime due to the nature of these offences.

- Cyprus seems to cooperate closely with ENISA and makes wide use of the services offered by Europol with regard to cybercrime. The representatives met, in particular from the police, are very well aware of the role of Europol/EC3. However, Eurojust seems to be used to a lesser extent.

- Cyprus has a very centralised system of judicial cooperation in criminal matters. The Ministry of Justice and Public Order is allocated the role of central authority, both for a number of multilateral international agreements that Cyprus has acceded to and in relation to the application of MLA requests. For the purpose of simplifying and improving international cooperation, a Unit for International Legal Cooperation has been established within the Ministry of Justice and Public Order. All requests for judicial cooperation are processed by the Ministry of Justice and Public Order before they are sent to judicial authorities. It evaluates all aspects of a request or its execution and if needed, corrects any errors.

- The Ministry of Justice and Public Order uses the EJN very frequently, which seems to be quite efficient and contributes to swift and smooth cooperation among Member States. Eurojust is also used in order to obtain fast responses. In the evaluators' view, the process whereby the Ministry of Justice and Public Order uses the EJN and the assistance its contact points can offer in order to facilitate judicial cooperation in criminal matters can be regarded as an example of best practice.

DECLASSIFIED

- Certain obstacles were mentioned in relation to the quality of the cooperation with the USA, since many popular and widely used Internet servers are located within their jurisdiction. The Cypriot authorities stated that judicial cooperation in criminal matters in the field of cybercrime and child pornography with the USA is quite complicated. Execution of MLA requests generally takes too long and often data is not supplied. Since the headquarters of social media sites in particular are usually located in the USA, cooperation with the USA is crucial for investigating cybercrime.

- Therefore, in the opinion of the evaluators, tools available through Eurojust could be used more frequently. Eurojust's role in assisting practitioners could be more specifically explored, e.g., the possibilities provided by the Liaison Prosecutor for the USA,in order to obtain faster responses to MLA requests to the USA. On the other hand, the EU should continue improving relations with the USA, especially with regard to MLA requests and their execution following requests from Member States.

DECLASSIFIED

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

No special training on cybercrime for prosecutors or judges is in place. Within the context of the funding programme "ISEC- Annual Programme 2014" Cyprus was granted funding in order to develop and organise training sessions for prosecutors and/or judges under the 3CE Project.[14]

The personnel of the DEFL and the O.C.C. follow special training courses each year in the investigation of cybercrime. The majority of these training courses are organised by CEPOL, FBI, OLAF and ECTEG. As for the field officers, there is a specialised training session organised by the Cyprus Police Academy on cybercrime investigation (collection of e-evidence, investigative procedures) and legislation. Police training in international cooperation and cybercrime is provided to all recruits at basic level at the Police Academy. Furthermore, police officers benefit from further training in international police cooperation from the EU and international organisations such as Europol and CEPOL, according to their duties. Refresher seminars are also organised by the Police Academy.

Moreover, once a year the O.C.C. organises a training session for a group of fifteen officers who are responsible for seizing the e-evidence from crime scenes. This session covers the collection of evidence, pre-search procedures, memory dump and other issues. The subjects covered are the following:

- cybercrime legislation
- collection of digital evidence
- first step to network investigation
- investigative tools
- procedures

The National Cybersecurity Strategy provides in Action 13 for the further engagement of universities, educational centres and other stakeholders in the provision of training, special courses and university courses related to cybersecurity and cybercrime.

DECLASSIFIED

[14] After the on-site visit the evaluation team was informed that the Cyprus Cybercrime Centre of Excellence 3CE Project is at the final stage of implementation. On 27.5.2016 a training session took place for 50 members of the police and joint training of judges and prosecutors took place on 10.6.2016. Another training for lawyers took place on 14.6.2016.

8.2. Awareness-raising

The National Cybersecurity Strategy provides for a systemic approach on cybersecurity awareness, the implementation of which is coordinated by the Office of the Commissioner of Electronic Communications and Postal Regulation. Action 14 of the Strategy refers to awareness and a committee and several sub-committees have been established to bring all national efforts into a shared vision.

Awareness of and education on cybercrime started in the Ministry of Education and Culture with the introduction of ICT into the educational system.

Cyprus uses national as well as European funds, along with the support of companies from the private sector, semi-governmental organisations, other public bodies, academia, and non-profit organisations and organised social groups to implement awareness content, tools and activities. Collaboration with the media also allows a broader awareness approach with short video clips, discussions and presentations, especially during the Safe Internet Day activities that take place in the month of February.

In 2004 the first European funding under the *Safe Internet Programme* was received for awareness raising, including helpline and hotline through the *SafeWeb* project coordinated by the University of Cyprus; until now European funding has been received under the same programme and the project *CyberEthics*.

CyberEthics, a project with a consortium of 5 partners (public and private partners including CNTI the Cyprus Pedagogical Institute, Cyta, which at a later stage was replaced by MTN), has been operating since 2006 with co-funding from the EU through the Safer Internet and CEF Programmes, and it comprises an awareness node, hotline and helpline. *CyberEthics* is the National Representative of Cyprus at the European Network of Awareness Centres and Helplines - Insafe and of the Worldwide Association of Hotlines for reporting illegal content on the Internet - Inhope.

DECLASSIFIED

It collaborates with several stakeholders from the public and private sector in Cyprus, as well as with stakeholders from overseas focusing on ensuring a better internet for all. The project ends by the end of June 2016. The activities of the project will be covered by a similar project under the coordination of the Cyprus Pedagogical Institute.

The Awareness Node aims at implementing attention-grabbing, targeted awareness campaigns informing the public about Internet Safety and Online Dangers; educating students, teachers, parents, other professionals and the public in the safer use of the Internet and creating promotional material and other awareness tools on internet safety that can be used for children, teenagers, teachers and parents.

Specifically, the activities of the Awareness Node implemented by the *CyberEthics* partners focusing on children include presentations, seminars, implementation of experiential workshops, delivery of theatrical shows, puppet shows, treasure hunting, organization of competitions, certification campaigns and research on internet use by minors. The topics covered by the above-mentioned activities and which educators, schools, social workers, parents and other organized bodies can request are grooming; cyberbullying; hacking; child sexual abuse material (child pornography); sexting; revenge porn; racism/xenophobia; identity theft.

Education about other adult-related dangers such as phishing and sextortion is also provided and includes two major services for assisting the public. These are the Hotline and the Helpline.
The Hotline allows the public, especially teenagers and young adults, to assist the effort to create a safer internet environment by reporting illegal content for cases of child sexual abuse and racism / xenophobia. The public can report illegal content to the hotline through:
1. The online form from the website at: www.cyberethics.info
2. Telephone at: 22674747
3. Email at: reports@cyberethics.info
4. The "*CyberEthics* HotHelp" mobile application

DECLASSIFIED

The Helpline provides people with the opportunity to have their questions and concerns answered in matters of harmful conduct, harmful contact and harmful content. The public can contact the Helpline through:

1. Chat from the website at: www.cyberethics.info (3pm-7pm, Monday to Friday)
2. Telephone at: 70000 116 (9am-7pm, Monday to Friday)
3. Email at: helpline@cyberethics.info
4. Offline message through the chat facility available 24/7
5. The "*CyberEthics* HotHelp" mobile application.

"Hope For Children" UNCRC Policy Center has a consistent and inspirational approach to protecting and promoting the rights of the child and to supporting the active participation of children and youth in society. The aim is to advocate and to protect children's rights based on the standards and principles of the UN Convention on the Rights of the Child and European Union law, regardless of a child's background. The programmes and activities that the Center operates related to the prevention of cybercrime are the following:

- the European Helpline for Children and Adolescents, 116111, which provides direct psychological support to children and adolescents free and confidentially;
- the "Beat Bullying" programme that aims to raise public awareness and equip the educational community and children with knowledge through the development of methods of identification, prevention and handling of bullying incidents;
- the ONE in Five Campaign, aiming to stop sexual violence against children and the number of actions that have been undertaken, addressing children, parents, teachers and the general public;
- the development of the mobile application "HFCBeatBullying" as a tool to prevent and tackle bullying which can be used in 23 EU countries and which not only contains practical advice but also offers direct access to the European Helpline for Children and Adolescents 116111.

DECLASSIFIED

In the framework of these programmes, "Hope For Children" UNCRC Policy Center delivers seminars to parents, workshops and provides training courses in schools, in order to inform, educate and empower students on issues of bullying, sexual abuse and cybercrime, with the cooperation of the Ministry of Education and Culture and the Observatory for School Violence. Moreover, there has been a training course for hotel staff on the issue of child safe tourism (including child pornography).

Hope for Children has also conducted academic research into online grooming; the first of its kind in Cyprus (http://uncrcpc.org.cy/index.php?id=47).

Hope For Children submitted a report, in response to the call made by the Committee on the Rights of the Child in relation to its' General Comment on the Rights of Adolescents, that included information on the best practices of "Hope For Children" UNCRC Policy Center sociological studies in relation to the prevalence of various problems that adolescents face, including bullying, online grooming, sexual abuse and sexual exploitation.

"Hope For Children" UNCRC Policy Center, as a player active in this field at national level, participates in the Steering Group for the ONE in Five Campaign and in the parliamentary meetings for the ratification and implementation of the Lanzarote Convention (that requires the criminalisation of all kinds of sexual abuse against children and which sets out that states in Europe and beyond must adopt specific legislation and take measures to prevent sexual violence, protect child victims and prosecute perpetrators).

In addition, the upcoming project "JudEx +: Towards a child-friendly justice in cases of sexual violence against children" (submitted under the EC call JUST/2014/RCHI/AG/PROF), is funded by the European Commission. "Hope For Children" UNCRC Policy Center will be the coordinator of the project, together with 6 other partners from EU countries. Partners were selected from countries that have recently (in the last 3 / 4 years) ratified the Lanzarote Convention, and where an urgent need has been identified to train professionals involved in judicial procedures in cases of child abuse in light of the Convention. The project began in January 2016 and will last for 2 years.

DECLASSIFIED

8.3. Prevention

8.3.1. National legislation/policy and other measures

Prevention efforts are reflected in both Cyprus' law and policy, and a special emphasis is laid on the prevention of child pornography. The Ministry of Education and Culture (MOEC) is involved in the prevention of cybercrime with a focus on *Content-related criminal acts* by educating children from an early age to recognise these dangers, avoid and prevent their exposure to them and, if they experience or witness any cybercrime, to be able to deal with it and report it.

The department responsible for safe Internet issues at MOEC is the Cyprus Pedagogical Institute (CPI). The CPI collaborates with the education departments in outlining policies and running programmes that have to do with the critical and responsible use of the Internet. The actions related to the safe Internet area include the following:

- inclusion of *Safe Internet* in the school curriculum;
- provision of school-based workshops for pupils, teachers and parents;
- presentations in conferences and other events;
- sustaining school programmes supported by the Cyprus Pedagogical Institute -such as the *Safe School for the Internet*, the *Production of short videos by students* competition, *Young Coaches for the Internet*, *eSafety Label* etc. in collaboration with other stakeholders[15]) ;
- participation in nationwide implementations of *Safe Internet* European- supported programmes such as the Safer Internet Programme by the Connecting Europe Facility (CEF) and the project *CyberEthics* funded by the European Commission Innovation and Networks Executive Agency (INEA) which also supports a helpline and hotline;
- the organisation of conferences and other events (for example on the *Safe Internet Day* a national conference is co-organised by MOEC with the Cyprus Telecommunications Authority that accommodates about 800 pupils while public awareness events are organized around the island in collaboration with other profit and non-profit organisations);

DECLASSIFIED

[15] www.pi.ac.cy/internetsafety

- an awareness campaign with short videos clips, discussions and presentations on the media;
- the design and production of educational content, activities and tools;
- the administration of a central safe internet filter in all schools;
- teacher training in cybercrime and protection issues.

The MOEC works in close collaboration with various stakeholders (public and private). For example, a number of presentations were given to schools by the Cyprus Telecommunications Authority, the CNTI and the Office of the Commissioner of Electronic Communications and Postal Regulation, while a number of Media Literacy workshops were delivered together with the Cyprus Radio Television Authority.

Since last year the Ministry of Education and Culture has been asked to coordinate Action 14 sub-group targeting awareness and education of children/ students, teachers and parents under the National Cybersecurity Strategy of Cyprus coordinated by the Office of the Commissioner of Electronic Communications and Postal Regulation. Action 14 aims at the development of a comprehensive national awareness programme for cybersecurity matters, covering all users of electronic systems, from governmental workers to ordinary citizens. In this context, an open invitation was sent for all stakeholders interested in being involved and the committee established under Action 14 is in the process of developing a national awareness and education strategy that will accommodate all existing measures and provide opportunities for new ones.
Law 91(I)/2014 includes provisions that legally oblige teachers to report suspicious cases and there is a reference to the Ministry's responsibility to ensure that pupils are educated with regard to the dangers of sexual abuse and in how to be protected.

DECLASSIFIED

On 30/9/2015, a body was established by a decision of the Ministerial Council, under Article 47 of the Prevention and Combating of the Sexual Exploitation of Children and of the Child Pornography Law (L.91(I)/2014), for the supervision of persons convicted of sexual offences against children. It is presided over by the Permanent Secretary of the Ministry of Justice and Public Order. It consists of representatives of the Ministry of Justice and Public Order, the police, the Legal Service, the Ministry of Health, the Ministry of Labour, Welfare and Social Insurance, the Ministry of Education and Culture, the Prisons Department, the Parole Board and the Youth Organization.

Moreover, an ad hoc Committee was recently appointed by a ministerial committee tasked with delivering a National Strategy for the Protection of Children from Sexual Exploitation and Child Pornography.

Prevention activities are also undertaken for criminal acts unique to information systems, in particular those related to cyber attacks. The MOEC departments and services are quite sensitive regarding students' and teachers' personal data and they comply with the Cyprus regulations as specified by the Office of the Commissioner for Personal Data Protection. At the same time, a team from the Information Technology Services Department (government level) has been seconded to the Ministry to assist with the security of information systems. Furthermore, there is a plan to request the IT Audits Unit at the Internal Audit Service (IAS) of Cyprus to carry out penetration tests at certain departments (the Cyprus Pedagogical Institute in particular) .

In addition, collaboration with the Cyprus Telecommunications Authority allows the Ministry to have a centralised web filtering system for the Internet access in schools.

There is close collaboration with the O.C.C. to inform and train pupils, teachers and parents in cybercrime laws and reporting procedures.

DECLASSIFIED

Programmes that deal with the *Content-related criminal acts* are introduced in early education (primary education level). These programmes are in the form of activities and form part of the school curriculum (for example, through ICT lessons) or school interventions and certifications (for example, the *eSafety label*), or competitions (short video production competition by students) or involve pupils taking an active role (for example the *Young coaches for the Internet* programme).

Through the proposal for the creation of a *Safe Internet Centre* (this proposal derives from the committee working on Action 14 of the National Cybersecurity Strategy), the aim is to provide courses for different audiences that can take place at the centre premises, online, in collaboration with universities and other training establishments (for example, for public servants).

Universities, through their collaboration with other partners in European -funded projects, have already started operating special courses on cybercrime and exploiting the possibilities for awarding diplomas in the area of cybercrime (for example, the European University of Cyprus, as a partner in the Cyprus Cybercrime Centre of Excellence for Training, Education and Research *(3CE)* project, offers a course syllabus for law students).

8.3.2. Public Private Partnership (PPP)

In the context of the National Cybersecurity Strategy the use of the Public- Private Partnership (PPP) model is considered crucial in the prevention of and fight against cybercrime. It is currently under examination by the Cyprus authorities.

DECLASSIFIED

8.4. Conclusions

- Cyprus uses internal and also external funding to organise training. Within the context of the funding programme "ISEC- Annual Programme 2014" Cyprus was granted funding in order to develop and organise training sessions for prosecutors and/or judges under the 3CE Project.

- The personnel of DEFL and the O.C.C. seems to be well trained. They follow special training courses each year in the investigation of cybercrime and the majority of these training courses are organised by CEPOL, FBI, OLAF and ECTEG and by the Cyprus Police Academy. As a consequence, the police officers also train other practitioners.

- However, there is no special training for prosecutors or judges in this area. Taking into account that perpetrators of cybercrime should end up in the court, judges and prosecutors are the group of practitioners which is expected to be specifically targeted by training. Obviously, training should not be obligatory for the judiciary and the prosecution service. However, participation in such events could be considered as an advantage by management in the matter of promotion of any kind. The introduction of such an incentive would encourage the judiciary and prosecutors to participate in specialised training courses, without affecting their independence.

- Since cybercrime is a relatively new phenomenon, training in cybercrime and the achievement of excellence seems to be of crucial importance. In the opinion of the evaluators, the best results could be achieved by joint training courses that include judges and prosecutors, court registrars, police officers and IT specialists. The evaluation team was, however, informed that this kind of training was not organised and members of the judiciary are generally reluctant to take such initiatives. Therefore, the Cypriot authorities should consider organising joint training courses for judges, prosecutors and police officers, with attendance made more mandatory. Making information on the support provided by Eurojust, EJN and Europol part of these courses could form an additional contribution to creating a better understanding of current developments and new trends in cybercrime, of the roles of the relevant actors responsible for detection, investigation and prosecution and of ways to foster and/or improve cooperation.

DECLASSIFIED

- The Cypriot authorities stated that the issue of training courses will be resolved in the future with the setting up of 3CE which will provide short-term, highly focused and specialized training seminars on cybercrime-related issues for public and private sector participants. Courses will facilitate the exchange and diffusion of tacit knowledge, familiarise participants with new technologies and tools, and improve their day-to-day capabilities in the cybercrime area. In the future modules could be developed especially for judges, prosecutors and law enforcement officers. The evaluators believe that while the establishment of a highly specialised centre of excellence to provide training is to be recommended, it should also be provided with sufficient human and financial resources to perform its tasks.

- Lots of work has been done and excellent practices have been established in Cyprus with regard to awareness raising and prevention, especially targeting pupils and young children. Cyprus has a well-developed system of educating children in cybercrime matters with professionals strongly focused on the issue. The Ministry of Education and Culture (MOEC) is involved in the prevention of cybercrime, focusing on *Content-related criminal acts* by educating children from an early age. The MOEC works in close collaboration with various stakeholders (public and private). For example, a number of presentations were given to schools by the Cyprus Telecommunications Authority, the CNTI and the Office of the Commissioner of Electronic Communications and Postal Regulation, while a number of Media Literacy workshops were delivered together with the Cyprus Radio Television Authority. All means of teaching children, including the system of young coaches, educational videos and the use of various social media tools seem to be worthwhile and productive.

DECLASSIFIED

- There are many programmes to be mentioned which are aimed at society in order to raise the awareness about the safe use of the Internet. Some of them, such as *CyberEthics*, eSafeSchools and Young Coaches for the Internet, were perceived by the evaluation team to be very valuable since they encourage pupils to take responsibility for their own education and for the training of their peers, parents, teachers. In the opinion of the evaluators, it is advisable to introduce the above- mentioned programmes and Safe Internet as regular school subjects, or make them part of IT education, following the Cypriot experience with the use of young coaches to educate children about threats resulting from use of the Internet.

- Moreover, Cyprus has set up a sex offender registry, which allows for a better protection of children from any possible future harm caused by persons already recognised as sex offenders. This can also serve as an inspiration for a useful system of protection of children, especially from sex offenders.

DECLASSIFIED

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Cyprus

The National Cybersecurity Strategy is the instrument that steers the efforts of Cyprus to prevent and combat cybercrime. It has provided structures for cooperation between all competent authorities, including public, private and non- governmental agencies, especially when it comes to awareness, an area in which the Cyprus devotes a great deal of effort to combat this form of crime.

The Cyprus Police has created a specialised office for combating cybercrime, the O.C.C., thus achieving the necessary expertise in dealing with the particularities of these offences. The establishment of an ad hoc Technical Committee under the OCECPR with the participation of law enforcement experts and representatives of ISPs strengthens the capacity to resolve technical problems. The 3CE Programme, currently ongoing, will develop training material for prosecution, law enforcement and judicial authorities.

The school interventions, with an active role of students in the critical and responsible use of the Internet, as users and creators, are crucial for children's education. Programmes such as the *Safe school for the Internet* where the school unit takes responsibility for creating a culture of Internet safe use for pupils, teachers, parents and the greater community, the *Young Coaches for the Internet* where pupils take responsibility for their own education as well as for the training of their peers, parents, teachers and the greater community are considered good practices for preventing cyber threats

One practical measure that could enhance the creation of an awareness culture is the adoption of a regulation that would request ISPs to have an awareness plan for their customers and would include the provision of web filters.

Moreover, direct European funding could be allocated to Member States specifically for the priorities laid down by the EU policies in order to achieve a good level of cybersecurity.

DECLASSIFIED

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 Cyprus was able to satisfactorily review the system in Cyprus.

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

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

DECLASSIFIED

9.2.1. Recommendations to Cyprus

1. Cyprus is encouraged to continue implementation of the National Cybersecurity Strategy, specifically carrying out organisational and structural activities to be complemented by increasing expenditures and human resources to improve the working environment of the O.C.C. and DEFL; (3.1, 3.2 and 3.5)

2. Cyprus should work out a method of collecting integrated statistics on investigations, prosecutions and convictions relating to cybercrime broken down into specific cybercrime areas, preferably those identified at the EU level, namely online child sexual abuse, online card fraud and cyber attacks; (cf. 3.3 and 3.5)

3. Cyprus should consider adopting legislative or other measures allowing for real-time interception/collection of traffic/content data, facilitating the effectiveness of the police while investigating cybercrime; (cf. 5.2.1 and 5.5)

4. Cyprus should take into consideration the possibility of involving prosecutors in the meetings/discussions with the private sector in a way that ensures that evidence is gathered pursuant to current legislation and is admissible in court proceedings; (cf. 4.5, 6.1.2 and 6.4)

5. Cyprus is encouraged to establish national CERT as a national body for the prevention of and protection from computer threats to the security of public information systems; (cf. 6.1.2 and 6.4)

6. Cyprus should foster cooperation between law enforcement authorities and the industry, especially the financial sector, in order to establish a sustainable reporting mechanism on cyber attacks affecting both society and the private sector; (cf. 6.1.2, 6.3.2 and 6.4)

7. Cyprus should consider including in training programmes information on the support Eurojust and the EJN can offer to national authorities, specifically regarding terms of cooperation with third states; (cf. 7.1.2, 7.5.1 and 7.6)

8. Cyprus is encouraged to maintain the concept of 3CE and *CyberEthics* by providing them with appropriate financial and human resources; (cf. 8.1, 8.3.1, and 8.4)

9. Cyprus should take the necessary steps to organise joint training courses on cybercrime for professionals, involving police officers, prosecutors and judges and to encourage judges to attend those training courses; (cf. 8.1 and 8.4)

DECLASSIFIED

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

1. Member States are encouraged to explore the possibility of applying for financial support from the EU for IT equipment, up-to-date forensic software and hardware; (cf. 3.5 and 4.5)

2. Member States are encouraged to involve representatives of the judiciary, in particular public prosecutors and judges, in the evaluation visits; (cf. 4.1.1 and 4.5)

3. Member States should engage in a dialogue with the private sector to seek possibilities to have data retained, as well as to ensure that the gathering of information takes place in a way that allows its admissibility in court; (cf. 4.1.2 and 4.5)

4. Member States should consider using the EJN and the assistance of its contact points in order to expedite judicial cooperation in criminal matters; (cf. 7.5.1 and 7.6)

5. Member States are encouraged to explore the possibility of making more frequent use of Eurojust and the tools available through Eurojust, in particular the Liaison Prosecutor for the USA at Eurojust, in order to obtain faster responses to MLA requests from the USA; (cf. 7.5.1 and 7.6)

6. Member States should be encouraged to involve a wide range of actors and programmes in preventing cybercrime, including institutions responsible for the education of pupils and students, as exemplified by actions taken by the Cypriot authorities on educating children; (cf. 8.3.1 and 8.4)

7. Member States should strengthen their policies regarding protection of children from any possible harm caused by persons already recognised as sex offenders; (cf. 8.4)

8. The EU Institutions should address the issue of data retention as soon as possible; (cf. 4.1.2 and 4.5)

9. The EU should continue improving relations with the USA in the area of combating cybercrime, especially with regard to MLA requests and their execution ; (cf. 7.5.1 and 7.6)

DECLASSIFIED

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT

7th round of mutual evaluations GENVAL

Cybercrime Evaluation Visit

Nicosia, 18 -20 November 2015

Programme of the Evaluation Visit

17th of November 2015

Arrival of delegates at Larnaca Airport (Transport by CYPOL)

1800 - 1830 Start of meeting at the hotel in Nicosia

18th of November 2015

0830 Departure from the hotel (Transport by CYPOL)

0845Arrival at the Ministry of Justice and Public Order

0900 – 0915 Welcome speech by the Permanent Secretary of the Ministry of Justice and Public Order

0915– 0930Introductory Presentation – Key stakeholders and Structures *(***Ministry of Justice and Public Order)**

0930 – 1030 National Cybersecurity Strategy , Q &A (**Office of the Commissioner for Electronic Communication and Postal Regulation)**

1030 – 1100 Coffee break

1100 – 1130 Government CSIRT, Q &A(**Department of Information Technology**)

1130 – 1200 Law on Preventing and Combating Sexual Abuse and Sexual Exploitation of Children and Child Pornography, Q &A (**MLSI**)

1200 – 1400 Prevention and Awareness - **Cyprus Pedagogical Institute** (**MOEC**)

DECLASSIFIED

(Prevention and awareness presentations will cover:

-Current situation

- eSafe schools programme (material, good practices)

- Young coaches for the Internet programme (material, good practices, video)

- Short video production completion

Coffee break

- Hotline and Helpline

- Safer Internet for Children – National Strategy

- Safer Internet Centre

1430 Buffet lunch hosted by the Permanent Secretary of the Ministry of Justice and Public Order, Venue TBC (transport by CYPOL)

1600 Transfer to the hotel (transport by CYPOL)

End of Day 1

19th of November 2015

0830 Departure from hotel (transport by CYPOL)

0845 Arrival at the European Union and International Police Cooperation Directorate, Cyprus Police Headquarters

0900-0915 Welcome speech by the Assistant Chief of Police

0915 –1000 Legal Framework Q & A (**Attorney General's Office TBC**)

100– 1030 Mutual Legal Assistance Q &A (**MJPO)**

1030- 1115 Coffee break

DECLASSIFIED

1115 – 1145 Structure of the Cyprus Police, Structures for EU and International Police Cooperation **(EUIPCD, Cyprus Police Headquarters**)

1145– 1215 Police training in International Police Cooperation and Cybercrime, Q & A (**Cyprus Police Academy, Cyprus Police Headquarters)**

1215 – 1315 Cybercrime Unit of the Cyprus Police (**DEPT C, Cyprus Police Headquarters**)

- Mandate/ Investigations
- International Cooperation
- Training (Available exclusively for the members of the OCC)
- Statistics
- "Darkcode" case study

1315 – 1345 Q & A

1345 – 1445 Buffet lunch on premises

1515 –1615 Visit to the Cybercrime Unit of the Cyprus Police, including a presentation on forensic examination (transport by CYPOL)

1615 Transfer to hotel (transport by CYPOL)

1930 Dinner hosted by the Cyprus Police, venue TBC

20th of November 2015

10 00 -11 00Wrap up meeting with evaluators at the hotel (if needed)

Departure of delegates(transport by CYPOL)

DECLASSIFIED

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 18 November 2015

Venue: Ministry of Justice and Public Order

Person interviewed/met	**Organisation represented**
Andreas Mylonas	Permanent Secretary Ministry of Justice and Public Order
Loizos Hadjivasiliou	Ministry of Justice and Public Order
Marios Djiapouras	Government CSIRT (Department of Information Technology Services)
Iliada Spyrou,	Helpline, Hotline and 3CE
Elena Aristodemou	Helpline, Hotline and 3CE
Antonis Antoniades	Commissioner for Electronic Communications and Postal Regulation
Costas Efthymiou	Commissioner for Electronic Communications and Postal Regulation
Anastasia Economou	Ministry of Education and Culture
Andreas Anastasiades	Head of the Office for Combating Cyber Crime and Digital Forensic Lab Police Headquarters
George Karkas	Crime and Criminology Office for Combating Cybercrime & Forensic Lab Cyprus Police Headquarters

DECLASSIFIED

Meetings on 19 November 2015

Venue: Cyprus Police Headquarters

Person interviewed/met	**Organisation represented**
Lambros Themistokleous	Assistant Chief of Police
Andreas Anastasiades	Head of the Office for Combating Cyber Crime and Digital Forensic Lab Police Headquarters
George Karkas	Crime and Criminology Office for Combating Cybercrime & Forensic Lab Cyprus Police Headquarters
Maria Mounti	Ministry of Justice and Public Order (MLATs)
Maria Kyrmizi	Senior Counsel, Attorney General's Office, MOKAS Financial Intelligence Unit
Kyriaki Lambrianidou	Cyprus Police Academy
Andreas Papadopoulos	International Cooperation Directorate, Cyprus Police Headquarters

DECLASSIFIED

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	CYPRUS OR ACRONYM IN ORIGINAL LANGUAGE	CYPRUS OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CEF	*CEF*		Connecting Europe Facility
CIRT	*CIRT*		Computer Incident Report Team
CNTI	*CNTI*		Cyprus Neuroscience and Technology Institute, NGO
CPI	*CPI*		Cyprus Pedagogical Institute
CyberEthics	*CyberEthics*		Cyprus Neuroscience & Technology Institute
DEFL	*DEFL*		Digital Evidence Forensic Laboratory, Cyprus Police
DITS	*DITS*		Department of Information Technology Services, Ministry of Finance
IAS	*IAS*		Internal Audit Service
INEA	*INEA*		European Commission Innovation and Networks Executive Agency
ISPs	*ISPs*		Internet Service Providers
PCCPWC	*PCCPWC*		Pancyprian Coordinating Committee for the Protection and Welfare for Children
O.C.C.	*O.C.C.*		Office For Combating Cybercrime, Cyprus Police
OCECPR	*OCECPR*		Office of the Commissioner of Electronic Communications and Postal Regulation
3CE	*3CE*		Cyprus Cybercrime Center of Excellence

DECLASSIFIED