



Council of the
European Union

Brussels, 5 July 2016
(OR. en)

7696/1/16
REV 1 DCL 1

GENVAL 42
CYBER 34

DECLASSIFICATION

of document: 7696/1/16 REV 1

dated: 7 June 2016

new status: Public

Subject: Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"
- Report on Malta

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, 7 June 2016
(OR. en)**

**7696/1/16
REV 1**

RESTREINT UE/EU RESTRICTED

**GENVAL 42
CYBER 34**

REPORT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Evaluation report on the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Malta

Table of Contents

1. EXECUTIVE SUMMARY	5
2. INTRODUCTION	8
3. GENERAL MATTERS AND STRUCTURES	11
3.1. National cyber security strategy	11
3.2. National priorities with regard to cybercrime	12
3.3. Statistics on cybercrime	14
3.3.1. <i>Main trends leading to cybercrime</i>	<i>14</i>
3.3.2. <i>Number of registered cases of cyber criminality</i>	<i>15</i>
3.4. Domestic budget allocated to preventing and fighting cybercrime and support from EU funding	17
3.5. Conclusions	17
4. NATIONAL STRUCTURES	19
4.1. Judiciary (prosecutions and courts)	19
4.1.1. <i>Internal structure</i>	<i>19</i>
4.1.2. <i>Capacity for and obstacles to successful prosecution</i>	<i>19</i>
4.2. Law enforcement authorities	21
4.3. Other authorities/institutions/public-private partnership	23
4.4. Cooperation and coordination at national level	23
4.4.1. <i>Legal or policy obligations</i>	<i>23</i>
4.4.2. <i>Resources allocated to improving cooperation</i>	<i>24</i>
4.5. Conclusions	25
5. LEGAL ASPECTS	27
5.1. Substantive criminal law pertaining to Cybercrime	27
5.1.1. <i>Council of Europe Convention on Cybercrime</i>	<i>27</i>
5.1.2. <i>Description of national legislation</i>	<i>27</i>
<i>A/ Council Framework Decision 2005/222/JHA on attacks against information systems and Directive 2013/40/EU on attacks against information systems</i>	<i>27</i>

<i>B/ Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography.....</i>	<i>29</i>
<i>C/ Online Card fraud</i>	<i>30</i>
5.2. Procedural issues	31
5.2.1. <i>Investigative Techniques.....</i>	<i>31</i>
5.2.2. <i>Forensics and Encryption.....</i>	<i>36</i>
5.2.3. <i>e-Evidence.....</i>	<i>36</i>
5.3. Protection of Human Rights/Fundamental Freedoms	36
5.4. Jurisdiction.....	37
5.4.1. <i>Principles applied to the investigation of cybercrime</i>	<i>37</i>
5.4.2. <i>Rules in case of conflicts of jurisdiction and referral to Eurojust.....</i>	<i>38</i>
5.4.3. <i>Jurisdiction for acts of cybercrime committed in the "cloud"</i>	<i>39</i>
5.4.4. <i>Perception of Malta with regard to the legal framework for combating cybercrime..</i>	<i>39</i>
5.5. Conclusions	40
6. OPERATIONAL ASPECTS	42
6.1. Cyber attacks	42
6.1.1. <i>Nature of cyber attacks</i>	<i>42</i>
6.1.2. <i>Mechanism to respond to cyber attacks.....</i>	<i>42</i>
6.2. Actions against child pornography and sexual abuse online.....	44
6.2.1. <i>Software databases identifying victims and measures to avoid re-victimisation.....</i>	<i>44</i>
6.2.2. <i>Measures to address sexual exploitation/abuse online, sexting, cyber bullying</i>	<i>45</i>
6.2.3. <i>Preventive actions against sex tourism, child pornographic performance and others</i>	<i>45</i>
6.2.4. <i>Actors and measures countering websites containing or disseminating child pornography.....</i>	<i>47</i>
6.3. Online card fraud	48
6.3.1. <i>Online reporting.....</i>	<i>48</i>
6.3.2. <i>Role of the private sector</i>	<i>50</i>
6.4. Conclusions	51
7. INTERNATIONAL COOPERATION.....	53
7.1. Cooperation with EU agencies	53
7.1.1. <i>Formal requirements to cooperate with Europol/EC3, Eurojust, ENISA.....</i>	<i>53</i>
7.1.2. <i>Assessment of cooperation with Europol/EC3, Eurojust, ENISA</i>	<i>53</i>

7.1.3.	<i>Operational performance of JITs and cyber patrols</i>	54
7.2.	Cooperation between the Maltese authorities and Interpol	54
7.3.	Cooperation with third states	54
7.4.	Cooperation with the private sector	54
7.5.	Tools of international cooperation	55
7.5.1.	<i>Mutual Legal Assistance</i>	55
7.5.2.	<i>Mutual recognition instruments</i>	58
7.5.3.	<i>Surrender/Extradition</i>	58
7.6.	Conclusions	60
8.	TRAINING, AWARENESS-RAISING AND PREVENTION	62
8.1.	Specific training	62
8.2.	Awareness-raising	63
8.3.	Prevention	66
8.3.1.	<i>National legislation/policy and other measures</i>	66
8.3.2.	<i>Private Public Partnership (PPP)</i>	67
8.4.	Conclusions	67
9.	FINAL REMARKS AND RECOMMENDATIONS	69
9.1.	Suggestions from Malta	69
9.2.	Recommendations	71
9.2.1.	<i>Recommendations to Malta</i>	71
9.2.2.	<i>Recommendations to the European Union and its institutions, and to other Member States</i>	73
9.2.3.	<i>Recommendations to Eurojust/Europol/ENISA</i>	73
Annex A:	Programme for the on-site visit and persons interviewed/met	74
Annex B:	Persons interviewed/met	77
Annex C:	List of abbreviations/glossary of terms	81

1. EXECUTIVE SUMMARY

The on-site visit in Malta was well prepared by the Maltese authorities and included meetings with the relevant actors with responsibilities in the field of preventing and combating cybercrime as well as in the implementation and operation of European policies, e.g. the National Police, the Malta Communications Authority, Critical Infrastructure Protection, the Attorney General, the Commissioner for Children, the Malta Gaming Authority and the Bank Association.

During the on-site visit, the Maltese authorities did their utmost to provide the evaluation team with complete information and clarifications on legal and operational aspects of preventing and combating cybercrime, cross-border cooperation and cooperation with EU-agencies, and cyber strategy.

Malta has not set up a National Cyber Security Strategy yet. However, the authorities in Malta seem to be fully aware of the need to take measures against cybercrime, including the development of a National Cyber Security Strategy, setting national priorities, fostering coordination to protect national critical digital infrastructure and ensuring a clear delineation and communication of roles and responsibilities, as well as the consolidation of an online mechanism to report cybercrime. The Maltese authorities are looking into the development of a National Cyber Security Strategy, and are in the process of defining the form and details of a governance model for ensuring coordination in the implementation of that strategy.

Work is currently under way to identify the needs and gaps in law enforcement agencies (LEA) and strengthen their capability to investigate and combat cybercrime. The Police Cyber Crime Unit, which is the designated government entity responsible for the prevention, investigation and prosecution of cybercrime offences, consists currently of seven people: one inspector, four police sergeants and two police constables. In general, the limited capacity and obstacles to successful investigations and prosecution are the result of an insufficient budget, a lack of modern equipment and limited human resources. However, by 2020, the number of police officers should increase based on the findings of the gap analysis which was carried out by the Police Force.

Setting up a coherent policy at strategic level and introducing adequate measures against cybercrime should strengthen Malta's resilience against cybercrime. Those steps need to be followed by: implementation of an online reporting system, ongoing alignment of cybercrime legislation with international standards, provision of law enforcement and judicial training on cybercrime and electronic evidence, interagency cooperation, public-private cooperation, measures to protect children online, in particular against online sexual exploitation, and financial investigations, as well as frameworks and mechanisms for efficient international cooperation on cybercrime investigations.

This resilience may be further strengthened by ensuring that financial, human and other resources are available in a coherent manner and by not depending on external funding to implement priorities with regard to cybercrime, including in particular combating cybercrimes committed by organised criminal groups and generating large criminal profits such as online and payment card fraud, cybercrimes which cause serious harm to their victims, such as online child sexual exploitation, and cyber attacks which affect critical infrastructure and information systems in the EU.

Regarding legislation, Malta seems to be compliant with most instruments reviewed. However, full transposition of Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography could be ensured. Furthermore, collection and analysis of statistical information and data on detection, investigation and prosecution of cybercrime cases could contribute to a better understanding of relevant developments and trends in this respect, both for intelligence and for law enforcement purposes, in particular those required by Directive 2013/40/EU.

At national level, procedures used by the Cyber Crime Unit are accepted as standard by courts. At international level, Malta has participated in several international operations in the fight against cross-border crime, particularly in the fight against online child abuse. Moreover, Malta is a member of several networks that share expertise and promote better international cooperation, and it is involved in a number of locally held training courses and meetings on international law enforcement, which have received very positive feedback.

Crime prevention initiatives within the local community are well-received and in very high demand. In 2009 Malta implemented a filter (Child Abuse Internet Filter) which stops local internet users from accessing 'known' websites containing child abuse material.

There is a good relationship established with industry, academia and other stakeholders as regards tackling child sexual abuse and pornographic material. A Memorandum of Understanding with Internet Hotline, operated by Aġenzija Appoġġ, has been concluded. A significant number of measures and projects aim to raise awareness about cybercrime threats and the risk of child sexual abuse and exploitation.

With regard to training, it is important to secure adequate resources to ensure that such measures are carried out in a consistent and sustainable manner, in particular where they rely on external funding. It seems that training on cybercrime and electronic evidence for judges is limited. Judges are, to a large extent, dependent on experts' reports. Considering that any crime can involve electronic evidence, in the evaluators' view, judges and prosecutors should at least have a basic knowledge of such topics. Thus, specialised training should also be available for judges. For the police, it is important to continue advanced technical training for CCU-MT officers through foreign organisations and follow up on the possibility of organising technical training locally.

Considering the size of the country and thus the limited resources available, the good level of cooperation and coordination between different institutions should be highlighted. In this respect, Malta is a good example for other countries that face similar challenges but cannot achieve a good level of cooperation between competent authorities at national level. However, cooperation with the financial sector still needs to be improved.

Taking into account the efforts made by the Maltese authorities to build up cybersecurity, and their awareness of both their strengths and weaknesses when it comes to successfully investigating cybercrime, the general impression of the evaluation team is that the Maltese system functions well and produces good results in countering cybercrime.

2. INTRODUCTION

Following the adoption of the Joint Action 97/827/JHA of 5 December 1997¹, 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 pornography² (transposition date: 18 December 2013) and Directive 2013/40/EU³ on attacks against information systems (transposition date: 4 September 2015) are particularly relevant in this context.

¹ Joint Action of 5 December 1997 (97/827/JHA), OJ L 344, 15.12.1997, 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 2013⁴ 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. Malta was the twelfth 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.

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 Malta were Ms Cristina Schulman (Romania), Mr Florian Kranz (Austria) and Mr Manuel Artuso (Italy). One observer, Mr Koen Hermans (Eurojust), was also present, together with Ms Giovanna Giglio and Mr Slawomir 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 the findings of the evaluation visit that took place in Malta between 16 and 18 September 2015, and on Malta's detailed replies to the evaluation questionnaire and follow-up questions.

DECLASSIFIED

3. GENERAL MATTERS AND STRUCTURES

3.1. National cyber security strategy

Malta's National Cyber Security Strategy (NCSS) is currently being developed and it is expected to be completed by 2016. For this purpose, two documents have been drafted, namely the Malta Cyber Security Strategy Green Paper and a supporting document providing background information and a rationale for the strategic approach of the strategy. The NCSS aims to ensure a safer internet, the protection of critical infrastructure, the rule of law, accountability and privacy. The main responsibility for its adoption lies with the Malta Information Technology Agency (MITA).

The draft Green Paper identifies the following high-level goals:

- Goal 1: Establish a governance framework to attain the Malta Cyber Security Strategy
- Goal 2: Combat cybercrime
- Goal 3: Strengthen national cyberdefence
- Goal 4: Secure cyberspace
- Goal 5: Build capacity
- Goal 6: International cooperation

Moreover, the Green Paper proposes a number of measures which will form the basis for the national stakeholders consultation exercise. The measures proposed under 'Goal 2: Combat cybercrime' seem to take into consideration the ENISA recommendations⁷ by including measures to identify the needs and gaps in law enforcement agencies (LEAs) and strengthen their capability to investigate and combat cybercrime.

⁷ ENISA, An Evaluation Framework for National Cyber Security Strategies, page 28.

The NCSS intends to ensure 'a coordinated, strategic approach rather than piecemeal activities'. Among the measures proposed by the Green Paper, coordination is envisaged at the strategic level⁸ and operational level⁹ in order to ensure clear delineation and communication of roles and responsibilities. The decision regarding responsibility for overall coordination is still subject to further consultation. No approach has been decided yet. The final position will be included in the strategy document to be published in July 2016.

3.2. National priorities with regard to cybercrime

Malta's national priorities relating to cybercrime are in line with the EU's strategic goals set out in the Council Conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017. Thus, while combating cybercrime committed by individuals, Malta's goals also include combating cybercrime committed by organised crime groups, 'such as online and payment card fraud, cybercrimes which cause serious harm to their victims such as online child sexual exploitation, and cyber-attacks which affect critical infrastructure and information systems in the EU'¹⁰.

Malta is actively participating in two of the three EMPACT sub-priorities on cybercrime – namely 'Child Sexual Exploitation' and 'Online Card Fraud'. In 2015, Malta led one of the Operational Actions from the 'Child Sexual Exploitation' sub-priority. Although it is not participating in the other EMPACT sub-priority on cybercrime – namely 'Cyber Attacks' – Malta closely follows the activities of that sub-priority and will participate in any operational actions with local involvement.

⁸ The structure of and responsibility for such coordination is subject to further consultations, with different approaches being discussed: (i) a centralised approach – whereby a national authority has in-house responsibilities with all authorities reporting to it; OR (ii) a decentralised approach whereby roles and responsibilities are spread across a variety of actors who coordinate together to share information and exchange experiences on a voluntary basis; OR (iii) a semi-centralised (hybrid) approach whereby a central ministry coordinates the implementation of the strategy, with designated authorities – which report to the central ministry on a periodic basis – having the necessary roles and responsibilities rather than operators and other stakeholders.

⁹ At the operational level, CSIRTs seem to be responsible for the national coordination of cyber detection and response.

¹⁰ See 12095/13.

Malta is also an active member of several working groups hosted at the European Cybercrime Centre (EC3), namely: the European Union Cybercrime Task Force (EUCTF), the European Cybercrime Prevention Network and the European Computer Training and Education Group (ECTEG).

Capacity building and combating cybercrime is also foreseen in Malta's National Digital Strategy for 2014 to 2020. The strategy, entitled 'Digital Malta', was launched by the prime minister following public consultation with several stakeholders. The Maltese government aims to enforce a National Cyber Security Strategy so as to help ensure a safer internet, the protection of critical infrastructure, the rule of law, accountability and privacy. The main pillars will be designed to:

- combat cybercrime. Law enforcement agencies will identify gaps and strengthen their capability to investigate and combat cybercrime
- strengthen national cyber defence. Public and private entities will be guided and assisted in strengthening their cyber defence capabilities
- secure cyberspace. Higher levels of trust will be instilled through awareness programmes and the delivery of trustworthy, ICT-enabled services that assure confidentiality, integrity, availability and privacy
- build capacity. The skills and educational frameworks required will be identified and developed

The capabilities of the Police Cyber Crime Unit will be enhanced through a project proposed under the Internal Security Funds Programme. The project has been divided into four key areas, namely: (a) search and seizure of digital evidence; (b) laboratory equipment for analysis of digital evidence; (c) IT systems used for internet investigations and technical enquiries; (d) capacity building in investigating online child sexual exploitation.

Regarding the area of online child sexual exploitation, Malta puts an emphasis on the fight against such crime not only through legislation and capacity building, but also through awareness raising, for example through the 'BeSmartOnline!' project. The Police Cyber Crime Unit also regularly partakes in crime prevention activities intended to raise awareness amongst the population on safe internet use. These initiatives, which have been well received, will be continued.

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

The Police Cyber Crime Unit has registered a year-on-year increase in the number of cases investigated. Crime trends are changing at a very fast pace and perpetrators are using advances in technology to their advantage.

An analysis of the statistics on cases involving the Police Cyber Crime Unit indicates that the three crime classifications most commonly dealt with are:

- Computer Misuse
- Fraud
- Insults, Threats and Private Violence (including Defamation)

Table 1: Statistics on cases involving the Cyber Crime Unit

	2013	2014
<i>Adult Pornography</i>	2	15
<i>Child Pornography</i>	7	8
<i>Computer Misuse</i>	180	160
<i>Counterfeit Currency</i>	0	0
<i>Fraud, Forgery and Misappropriation</i>	120	110
<i>Trafficking in Human Beings</i>	0	3
<i>Illegal Gambling</i>	1	2
<i>Incitement of Racial Hatred</i>	13	6
<i>Information Gathering re: Other Police Reports</i>	96	47
<i>Information Gathering re: Missing Persons</i>	2	5
<i>Insults, Threats and Private Violence</i>	137	183
<i>Intellectual Property Rights</i>	4	2
<i>Other Serious Crimes</i>	40	27
<i>Prostitution</i>	1	1
<i>Sexual Offences (including Defilement of Minors)</i>	8	11
<i>Terrorism</i>	5	4

3.3.2. Number of registered cases of cyber criminality

Statistics on cases involving the Cyber Crime Unit have been retained since the unit was set up in 2003. Since it was set up, the Police Cyber Crime Unit has been compiling annual statistics on cases in which it has been involved.

The Maltese authorities pointed out that the presented statistics are the only cybercrime statistics available in Malta.

Table 2: Total number of cases involving the Cyber Crime Unit

YEAR	TOTAL	% INCREASE
2003	51	-
2004	107	109.80 %
2005	103	-3.74 %
2006	172	66.99 %
2007	170	-1.16 %
2008	279	64.12 %
2009	317	13.62 %
2010	375	18.30 %
2011	372	-0.80 %
2012	576	54.84 %
2013	616	6.94 %
2014	584	-5.19 %

With regard to the percentage share of cybercrime in the overall criminality picture, the only data available is on reports of computer misuse received by the police. The percentage share of computer misuse reports is as follows:

Table 3: *The percentage share of computer misuse reports received by the police*

<i>Year</i>	<i>Total Police Reports</i>	<i>Reports re: Computer Misuse</i>	<i>% Share</i>
2002	17043	2	0.01
2003	17773	4	0.02
2004	18377	11	0.06
2005	18578	11	0.06
2006	16538	29	0.18
2007	15150	40	0.26
2008	13800	87	0.63
2009	11951	92	0.77
2010	13306	153	1.15
2011	14248	159	1.12
2012	15618	243	1.56
2013	17584	211	1.20
2014	16648	193	1.16

Table 4: *Equipment delivered to the Cyber Crime Unit for analysis*

	2013	2014
<i>Computer Systems</i>	93	40
<i>Hard Disks (Internal/External)</i>	123	70
<i>Compact Discs/DVDs</i>	726	78
<i>3.5" Floppy Disks</i>	16	0
<i>Other Media</i>	93	40
<i>Documents/Logs/Paper Evidence, etc.</i>	3	0

However, the statistics collection system does not involve the collection and management of statistical data on investigations and prosecutions or convictions relating to cybercrime.

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

The Maltese authorities reported on the lack of specific funds allocated for the prevention of and fight against cybercrime. The funds allocated to the Cyber Crime Unit are derived from the police department's general budget. The unit submitted a proposal for funding under the Internal Security Fund (ISF) Programme for the following:

- The provision of investigative tools and equipment for gathering digital evidence in a more efficient manner
- The provision of laboratory equipment for analysing digital evidence
- The provision of IT systems to facilitate internet investigations
- The provision of resources to enhance the capacity of the Police Cyber Crime Unit to investigate online child sexual exploitation

3.5. Conclusions

- The Maltese authorities have a comprehensive overview and understanding of the main features and characteristics of the cybercrime phenomenon and environment. They have identified their main goals in terms of the prevention of and fight against cyber-related offences, and the measures required to achieve them.
- The Maltese authorities seem to be fully aware of the need to develop a National Cyber Security Strategy through a thorough process that involves the relevant institutions, considers relevant international experiences and ensures consultation with stakeholders. Malta's national priorities were confirmed during the on-site visit.

- In the opinion of the evaluators, NCSS should ensure at strategic level a coherent policy and adequate measures against cybercrime including: implementation of an online reporting system for cybercrime, alignment of cybercrime legislation with international standards, institutional set-up (e.g. high-tech crime or other specialised units), provision of law enforcement and judicial training on cybercrime and electronic evidence, interagency cooperation, public-private cooperation, measures to protect children online, in particular against online sexual exploitation, and financial investigations, as well as frameworks and mechanisms for efficient international cooperation on cybercrime investigations.
- At the time of the on-site visit, it was unclear to what extent the Maltese authorities are considering putting in place a structured mechanism ensuring the cooperation of all relevant authorities and stakeholders involved in the prevention of and fight against cybercrime and/or the establishment of a single entity with coordination functions for this purpose.
- Therefore, the evaluators encourage the Maltese authorities to continue their efforts with a view to developing a national cybersecurity strategy, which should also be aligned with the European Agenda on Security in the area of the prevention and repression of cybercrime. While establishing a strategy, it would be also useful to develop an action plan identifying concrete actions and measures for its implementation.
- The Police Cyber Crime Unit compiles annual statistics on cybercrime and the number of cases involving the Police Cyber Crime Unit. These are the only cybercrime statistics available in Malta.
- Taking into account the increase in cybercrime-related offences, improving the collection and analysis of statistical information and data on detection, investigation and prosecution of cybercrime cases could contribute to a better understanding of relevant developments and trends in this respect, for both intelligence and enforcement purposes.
- Therefore, in the evaluators' view, an integrated information system facilitating the collection and management of statistical data at the level of investigations and prosecutions, on the one hand, and convictions relating to cybercrime, on the other, is needed in order to have a complete overview of the progress of cybercrime in Malta. Its establishment should be considered for strategic purposes, e.g. national and training strategies.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

In Malta, the prosecution of a criminal action is done by the police, *ex officio*, who also act as prosecutors before the inferior courts, i.e. the Court of Magistrates, whether as a court of criminal inquiry or a court of criminal judicature. Although the Attorney General does not play a role of prosecution before the Court of Magistrates, the police may be assisted before that court by the Attorney General or its officials. In cases where intricate legal or constitutional issues might be raised, the assistance of the office of the Attorney General is sought.

The courts of criminal competence are the Court of Magistrates, the Criminal Court and the Court of Criminal Appeal. The Court of Magistrates may function as a court of criminal judicature and has full competence to decide the merits of the charge in respect of offences which may be tried summarily only, or in respect of offences which may be tried either way, subject to the direction of the Attorney General and the consent of the person charged.

Criminal offences may be tried on indictment only or summarily only, or offences may be tried either by the Criminal Court or by the Court of Magistrates depending on the decision of the Attorney General and sometimes on the consent of the person charged.

There is no specialised court for cyber-related offences. Should the court deem it necessary, it can appoint experts in the field to assist in the proceedings.

4.1.2. Capacity for and obstacles to successful prosecution

The Malta Police Academy is responsible for police training in Malta. The role of the academy is to train recruits, inspector cadets and serving police officers to fulfil their role in the Malta Police Force with ability, knowledge, expertise, integrity and impartiality. The academy offers courses for new police recruits and these include a module on cybercrime awareness. That module incorporates cybercrime investigations, basic collection and handling of digital evidence, and report-taking. Matters relating to child victims of sexual abuse or exploitation are also included in the curriculum of training for Continuous Professional Development of Police Officers and Higher Officials.

The representatives met reported that the Police Cyber Crime Unit is facing an increase in the number of cases registered on a yearly basis, which has not been accompanied by a parallel increase in resources. This has led to:

- a longer turn-around period for conducting technical enquiries and reporting findings to investigators
- a backlog in digital equipment which has been brought to the Police Cyber Crime Unit for analysis
- a reduction in pro-active investigations that are initiated by the Police Cyber Crime Unit
- officers being burdened with tasks which are not carried out in other sections due to lack of technical knowledge
- the Police Cyber Crime Unit making use of computer systems and equipment which are several years old and some equipment which is now obsolete.

The police also face difficulty in gathering information from service providers located overseas. Some states can only transfer information subject to court authorisation. It is believed that the process is very lengthy and in some cases, it may also jeopardise the successful outcome of the police investigations.

In cases where the information has been provided directly to the police by service providers located abroad, exceptions were raised regarding the admissibility of the information. This was largely based upon the defence that the information had been obtained in an informal manner. This creates difficulties, in that the required information is either unavailable, not made available or sometimes considered inadmissible.

One of the major challenges of cybercrime is undoubtedly the fact that the investigation of transnational crime requires cooperation from different states. The Police Cyber Crime Unit has experienced some difficulties in obtaining information from other states. These difficulties mainly relate to delays in receiving the requested information. This hinders the successful completion of investigations.

The existing national legislation on data retention, providing for a six-month data retention period, continues to apply. After the invalidation by the Court of Justice of the European Union on 8 April 2014 of Directive 2006/24/EC of 15 March 2006 (the 'Data Retention Directive'), the Maltese authorities began to explore the possible revision of the national data retention regime, taking into account the principles enshrined by the Court in joint cases C-93/12 and C-594/12. They also highlighted the uncertainty deriving from the current absence of a common legal framework for data retention at EU level.

4.2. Law enforcement authorities

The Police Cyber Crime Unit was set up in 2003. The Malta Police Force is the designated government authority responsible for the prevention, investigation and prosecution of cybercrime offences. The Cyber Crime Unit is a unit within the Police Force whose main task is to provide technical assistance in investigations. It currently consists of seven people: one inspector, four police sergeants and two police constables. However, by 2020, the number of police officers should increase based on the findings of the gap analysis which was carried out by the Police Force.

The powers of the police are derived from the Criminal Code – Book Second – Laws of Criminal Procedure – Part I (Articles 346 – 366), 'Of the Powers and Duties of the Executive Police in Respect of Criminal Prosecutions'. Those powers are as follows:

<i>Police Powers</i>	<i>Legislation</i>
<i>Power to stop and search</i>	<i>Criminal Code, Articles 351 - 354</i>
<i>Power of entry, search and seizure under warrant</i>	<i>Criminal Code, Articles 355E – 355J</i>
<i>Power of entry and search without warrant</i>	<i>Criminal Code, Articles 355K -355O</i>
<i>Power of arrest and detention</i>	<i>Criminal Code, Articles 355V – 355AF</i>
<i>Power to summon a person accused when not arrested</i>	<i>Criminal Code, Article 360</i>
<i>Power to subpoena witnesses</i>	<i>Criminal Code, Article 365</i>

The Police Cyber Crime Unit's main functions are laid down by General Headquarters Circular 66/2003:

- To provide technical assistance in the detection and investigation of offences, in which the means used is the computer
- To collect and preserve evidence and to present it before the judicial authorities
- To provide 24/7 support to international law enforcement agencies
- To monitor local internet use for potential production and dissemination of unlawful material, specifically child sexual abuse material
- To develop a network amongst local IT industry and to generate awareness of good practices
- To monitor and document any developments related to legislation that may be required both locally and internationally
- To promote safe use of the computer and to educate the general public on ways to protect themselves against cybercrime
- To block access to websites containing child sexual abuse material. This is done in collaboration with all the local internet service providers.

The Police Cyber Crime Unit is the designated contact point for the following networks:

- Council of Europe Convention on Cybercrime - 24/7 Network
- G7 24/7 Cybercrime Network Points
- INTERPOL National Central Reference Points for Computer-Related Crime

Whilst the Cyber Crime Unit does not have a special post for IT forensic examiners, it strives to ensure that all its members receive regular specialised training on criminal investigation and the technical aspects of obtaining computer-based evidence.

4.3. Other authorities/institutions/public-private partnership

In addition to the police, the other national authorities with competence in preventing and combating cybercrime are as follows:

- The Malta Communications Authority (MCA) is the authority responsible for regulating the electronic communications sector, in particular internet services;
- Aġenzija Appoġġ (Foundation for the Social Welfare Services) is the national agency for children, families and the community, and it aims to promote the well-being of these persons through the development and provision of psycho-social welfare services;
- The Directorate for Quality and Services in Education (DQSE) was established to ensure the effective and efficient operation and delivery of services to the state school Colleges within an established framework of decentralisation and autonomy;
- The Office of the Commissioner for Children is responsible for promoting the welfare of children and compliance with the UN Convention on the Rights of the Child, as ratified by Malta on 26 January 1990, and such other international treaties, conventions or agreements relating to children as are or may be ratified or otherwise acceded to by Malta.

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

Currently there is no legal framework for inter-agency cooperation in cases concerning cybercrime.

In case of a cyber attack there is no coordinated multidisciplinary mechanism currently in place to respond to such an attack. However, Malta is currently conducting its first National Risk Assessment (NRA) exercise. The NRA exercise will consider the potential risk of serious cyber attacks and the required treatment mechanisms.

There is a good level of cooperation in the process of implementing prevention, education and awareness measures in this area. As an example of the latter, the Malta Communications Authority, in collaboration with the Foundation for Social Welfare Services (Aġenzija Appoġġ), the Directorate for Quality and Standards in Education (DSQE) and the Office of the Commissioner for Children, has embarked on a project called 'BeSmartOnline!'. The project, which is co-funded by the European Union through the Connecting Europe Facility (CEF), aims to:

- raise awareness, empower and educate children, teens, carers and educators on the safe use of the internet
- organise a Youth Forum (a panel) where children and young people can express their views and exchange knowledge and experiences about their use of social networking sites and other websites
- combat illegal and harmful behaviour
- offer a means to the public to report illegal content or inappropriate material, particularly in relation to child sexual abuse material. This is done through a tool known as Hotline (<http://www.fsws.gov.mt/en/onlineabuse/Pages/report-online-abuse.aspx>). This tool allows individuals to report illegal websites anonymously
- offer support services to victims through the helpline and 'kellimni.com'. Support line 179 is the national helpline, which is there to offer support and information to the victims of cybercrime. In conjunction with that service, the online service 'kellimni.com' provides free anonymous, confidential support to young people

4.4.2. Resources allocated to improving cooperation

The Police Cyber Crime Unit has very limited search and seizure capabilities. It does not have the capacity to carry out on-site extractions of data from large-scale computers. It also has no capacity to carry out proper computer network investigations. The identification of illegal material and categorisation of images/videos is still carried out manually. In order to keep pace with developments in the criminal world in terms of the use of information technologies, investments in hardware, software and human resources are to be considered.

According to the representatives met, the police do not have sufficient tools to analyse seized mobile phones and have to consult experts. That slows down the investigations and increases costs.

4.5. Conclusions

- Malta has a common law system in place applicable to criminal proceedings. In most cases the police prosecute the cases and represent the prosecution in court. The Attorney General's Office is responsible for keeping a general overview of cases prosecuted by the police in the area of criminal law. It does not regularly act as a prosecutor, apart from cases before the Superior Courts (Criminal Courts and the Court of Criminal Appeal), and acts as central judicial authority in all matters falling within the field of international legal cooperation.
- The Malta Police Force is the designated government authority responsible for the prevention, investigation and prosecution of cybercrime offences. The Cyber Crime Unit is a unit within the Police Force whose main task is to provide technical assistance in investigations. It currently consists of seven people (one inspector, four police sergeants and two police constables). The Maltese authorities are aware of the shortcomings regarding human resources assigned to cybercrime, and are taking measures to increase the number of staff specialised in the area. The evaluation team was told that an increase in police staff is expected by 2020.
- However, in the opinion of the evaluators, the Police Cyber Crime Unit suffers not solely from limited human resources but also from insufficient technical equipment, such as hardware and software, to fulfil its statutory tasks. Therefore, investments in hardware, software and human resources could increase the resilience of the Maltese cybersecurity system.
- The Maltese authorities also referred to certain difficulties in international cooperation as regards investigation and prosecution of cross-border cybercrime cases. These included delays and constraints in providing and obtaining electronic communication data from other Member States based on the existing data retention period of six months, due to complex and lengthy MLA procedures that might often require more time to be completed.

- Currently there is no formal legal framework for inter-agency cooperation in cases concerning cybercrime. However, there is undoubtedly a good level of cooperation between different institutions in Malta in terms of implementing prevention, education and awareness measures in this area.
- Nonetheless, no coordinated multidisciplinary mechanism is currently in place to respond to cyber attacks. In the opinion of the evaluators, this situation may be improved once the National Cyber Security Strategy is adopted and the form and details of a governance model for ensuring coordination between actors involved in countering cybercrime is defined.

DECLASSIFIED

5. LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on Cybercrime

Malta ratified the Council of Europe Convention on Cybercrime on 12 April 2012. During the on-site visit the Maltese authorities stated that cybercrime legislation in Malta is based on the Cybercrime Convention.

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

Malta transposed Directive 2013/40/EU on attacks against information systems and reported that no problems were encountered during its implementation.

The Criminal Code (Chapter 9 of the Laws of Malta), under Sub-title V Computer Misuse, Articles 337B-337H, deals with various offences covering illegal access to information systems, illegal system interference, illegal data interference, illegal interception of computer data, misuse of devices and others.

Maltese legislation extends liability to cover legal persons. Article 121D of the Criminal Code states that whosoever is vested with the legal representation of a company, such as the director, manager, secretary or other principal officer of a body corporate, shall be held liable for any offences concerning cybercrime. However, the liability attached to a body corporate does not derive from the act itself but from the benefit acquired by such body.

Aggravating circumstances in Maltese law are in line with Directive 2013/40/EU and include where the offence:

- (a) constitutes an act which is in any way detrimental to any function or activity of Government, or hampers, impairs or interrupts in any manner whatsoever the provision of any public service or utility, whether or not such service or utility is provided or operated by any Government entity;

- (b) causes serious damage;
- (c) is committed against a critical infrastructure facility information system;
- (d) is committed within the framework of a criminal organisation within the meaning of Council Framework Decision 2008/841/JHA of 24 October 2008 on the fight against organised crime;
- (e) is committed through the misuse of personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner.

According to the evaluators, some concerns can be raised regarding conduct criminalised under 'unlawful access to, or use of, information' (Article 337C), which comprises different offences, e.g. illegal access, illegal interception, data interference, system interference, misuse of devices, etc. A preliminary analysis seems to indicate a number of overlapping substantive law provisions, raising questions with regard to their practical application. In addition, some of the crimes described may not be necessarily committed in the form of cybercrimes, e.g. hindering or impairing the functioning or operation of a computer system without manipulating data.

The Maltese authorities stated that given that recent amendments had been introduced through Act VIII of 2015¹¹, no additional amendments were foreseen in the immediate future. However, the 'National Digital Strategy 2014 – 2020' identifies the challenges posed by new technologies related to cloud services, portability and social media. Consequently, the Maltese government will review existing legislation so as to ensure its relevance and effectiveness in the cyber world, especially as regards crimes related to cyber bullying. Further to this, the Maltese government plans to implement measures to maintain privacy, safety and security while surfing, transacting and operating online. The new legislation will address issues related to intellectual property rights, patents, sensitive and personal information, cloud computing, net neutrality, online contracts and licence agreements, and vendor lock-in and exit management strategies.

¹¹ <http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=26727&l=1>

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

Malta reported that it had transposed most of the provisions of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA into the Criminal Code (Chapter 9 of the Laws of Malta).

With regard to the protection of children against sexual violence, Article 208A of the Criminal Code sets out offences related to pornographic or obscene articles (e.g. producing, distributing, disseminating, importing, exporting, offering, selling, supplying, transmitting, making available, procuring, showing or permitting the production of indecent material). Article 208A(1B) of the Criminal Code criminalises the act of acquiring, knowingly obtaining access through information and communication technologies to, or possessing any indecent material which shows a minor/minors.

Solicitation of persons under age (article 208AA) and other related offences (Article 204A - Instigation with violence of persons under age to prostitution or to participation in a pornographic performance, Article 204B - Inducing persons under age to prostitution or to participation in a pornographic performance, etc.) are covered by the Criminal Code transposing the substantive criminal law provisions of Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography.

The punishment may be exceeded in cases where the offence is committed by any ascendant related by consanguinity or affinity, or by the adoptive father or mother, or by the tutor, or by any person charged with the care, education, instruction, control or custody of the person. In addition, the criminal law provides for more severe penalties in the following situations:

- The minor's life is wilfully or recklessly endangered by the offender
- The offence involves violence or grievous bodily harm
- The offence is committed with the involvement of a criminal organisation
- The offender has a position of trust, authority or influence over the minor.

The term 'indecent material' includes photographs, images, audio or video recordings, digitally created or electronic images, drawings, cartoons, text and simulated representations or realistic images of a minor, or any material that visually depicts any person appearing to be a child, even if the minor is non-existent, or of the sexual parts of a child for primarily sexual purposes.

The Juvenile Act sets up a Juvenile Court and regulates matters relating to children and young persons (*'child or young person' means a person who is under the age of sixteen years*). Thus juvenile offenders are heard before the Juvenile Court, where proceedings are carried out in a more informal and private manner in order to protect the privacy of the minor.

Chapter 462 of the Commissioner for Children Act (5 December 2003, Act VII of 2003) lays down the requirements and procedure for appointing the Commissioner for Children, who has the power to investigate any breaches or infringements of the rights of children.

Other types of cybercrime refer to traditional offences, such as stalking, defamation, harassment and threats. In these cases, the general provisions of law that apply when such offences are conducted in their traditional form shall also apply when they are committed via the internet.

C/ Online Card fraud

Articles 308-310BA of the Criminal Code criminalise fraud and Articles 166-190 of the Criminal Code criminalise forgery. Regulation 9 of Subsidiary Legislation 440.01 (Processing of Personal Data (Electronic Communications Sector) Regulations) deals with sending or controlling the sending of spam.

Under the Cybercrime Convention, computer-related offences (fraud and forgery) are specific ways of manipulating computer systems or computer data. Traditional criminal law may not be sufficiently broad to be extended to situations involving computer networks (visual readability of statements, or declarations embodied in a document, which does not apply to electronically stored data; undue manipulation in the course of data processing with the intention to effect an illegal transfer of property). It seems that the Maltese approach was to extend the traditional criminal law provisions to cover new forms of interferences and attacks (for example, Article 189A: *'For the purposes of this Title, "document", "instrument", "writing" and "book" include any card, disc, tape, soundtrack or other device on or in which information is or may be recorded or stored by mechanical, electronic or other means'* and Article 310BA, paragraph 3: *'For the purposes of this article: "article" includes any document, program or data held in electronic form.'*)

5.2 Procedural issues

5.2.1 Investigative Techniques

The following investigative techniques apply in Malta:

Search and seizure of information system/computer data

In order for the police to be able to collect data for evidence, they need to enter the premises and search for computers or data. To do so, they are requested to obtain a warrant of entry and search, which shall be issued by a magistrate as per Article 355E of the Criminal Code. However, there are circumstances in which the police may exercise their power of entry and search without a warrant. Article 335E provides for the following exceptions:

- (a) the offence is a crime other than a crime punishable under the Press Act and there is imminent danger that the said person may escape or that the corpus delicti or the means of proving the offence will be suppressed;
- (b) the person is detected in the very act of committing a crime other than a crime punishable under the Press Act;
- (c) the intervention of the police is necessary in order to prevent the commission of a crime other than a crime punishable under the Press Act; or
- (d) the entry is necessary for the execution of any warrant or order issued by any other competent authority in the cases prescribed by law; or
- (e) the arrest is for the purpose of apprehending a person who is unlawfully at large after escaping from lawful arrest or detention; or
- (f) the entry is necessary for purposes of:
 - (i) executing the arrest, or ascertaining the whereabouts, of a person in respect of whom an alert has been entered in the Schengen Information System and there is an imminent danger that the said person may escape; or

(ii) discovering any property in respect of which an alert has been entered in the Schengen Information System and there is an imminent danger that the property may be concealed, lost, damaged, altered or destroyed.

Furthermore, the law enables the police to act without a warrant of entry and search if the property being searched belongs to a person who is under arrest.

The police are vested with the power to enter and search any premises, house, building or enclosure used, occupied or controlled, even temporarily, by a person who is under arrest, if they have reasonable grounds for suspecting that there is evidence, other than items subject to legal privilege, that relates to the offence or a connected offence, and such search shall be limited to the extent that is reasonably necessary for discovering such evidence (as per Article 355L(1) of the Criminal Code).

The Criminal Code grants the police the power to seize and retain data or a computer system. Any object which may facilitate the investigation and the prosecution by the police shall be seized and retained as evidence. Article 355Q grants the power to the police to 'require any information which is contained in a computer to be delivered in a form in which it can be taken away and in which it is visible and legible'. This provision of law has important implications as it allows the police to seize data which is not available on the system's internal drive and it also enables the police to track data which is stored on networked computers situated outside Malta. This provision also caters for instances in which the data has been maliciously encrypted so as to hide its real content. In such a scenario, it is the duty of the police to request that the owner/possessor of the computer produce data which is decrypted and legible. However, the capacity of the police is limited when it comes to carrying out on-site extraction of data from large-scale computers, mainly due to a lack of knowledge and equipment.

Real-time interception/collection of traffic/content data

The concept of interception is dealt with in the Security Service Act (Chapter 391 of the Laws of Malta). Interception is defined as follows: 'in relation to a warrant, includes the obtaining possession of, disrupting, destroying, opening, interrupting, suppressing, stopping, seizing, eavesdropping on, surveilling, recording, copying, listening to and viewing of communications and the extraction of information from such communications'.

The national competent authority can intercept communications in two ways:

1. Collecting and analysing metadata (traffic data): this data merely reveals the parties' identity, the duration of the communications and the localisation of the parties;
2. Collecting and analysing the content of the data: this goes beyond metadata as the national competent authority would be in possession of the contents of the communications, for example emails and chat logs.

In terms of the Security Service Act, the power to intercept can only be directly exercised by the Malta Security Service (MSS) and the minister responsible for the MSS. By means of an application, the MSS shall request that the minister issue a warrant authorising the exercise of an act which involves the interception of communications data. The warrant must be in the form of a certificate and it must be issued for six months, which can be renewed for a further six months.

The Cyber Crime Unit is not empowered to carry out interception and online undercover work. The police may, however, request the court to carry out a Magisterial Inquiry in order to collect and preserve evidence which cannot be collected through the general police powers.

Data retention

Regulation 18 of S.L. 440.01 'Processing of Personal Data (Electronic Communications Sector) Regulations' states that the service provider of electronic communication services or of a public communications network is not obliged to retain the content of communications. On the other hand, Regulation 19 states that traffic data shall be retained and in such case 'shall be disclosed only to the police or to the Security Service, as the case may be, where such data is required for the purpose of the investigation, detection or prosecution of serious crime'. The term 'serious crime' is understood to mean offences punishable by a term of imprisonment of not less than one (1) year and/or offences of a criminal nature specific to electronic communications as defined by the Electronic Communications (Regulations) Act (Chapter 399 of the Laws of Malta), Part VII, Article 48(1)(d) and Article 49. Moreover, Regulation 19 imposes an obligation upon the service provider to make data traffic available in a legible and comprehensive manner. The police must make the request for information in writing. Nonetheless, if the information is urgently needed, the police may make the request orally.

Regulation 20 specifies the categories of data which must be retained by the service providers (summarised below). Traffic data relating to internet access and email shall be retained for a period of six (6) months.

Categories of Data	Type of Data concerning Internet Email and Internet Telephony
Data necessary to trace and identify the source of a communication	(i) The user ID allocated; (ii) The user ID or telephone number allocated to any communication entering the public telephone network; (iii) The name and address of the subscriber or registered user to whom an Internet Protocol address, user ID or telephone number was allocated at the time of the communication.
Data necessary to identify the destination of a communication	(i) The user ID or telephone number of the intended recipient of an internet telephony call; (ii) The name and address of the subscriber or registered user and user ID of the intended recipient of the communications.
Data necessary to identify the date, time and duration of the communication.	(i) The date and time of the log-in and log-off of the internet access service, based on a certain time zone, together with the Internet Protocol address, whether dynamic or static, allocated by the internet access service provider to a communication, and the user ID of the subscriber or registered user; (ii) The data and time of the log-in and log-off of the internet email service or internet telephony service, based on a certain time zone.
Data necessary to identify the type of communication.	The internet service used.
Data necessary to identify users' communication equipment or what purports to be their equipment.	(i) The calling telephone numbers for dial-up access; (ii) The digital subscriber line or other end point of the originator of the communication.

The Maltese authorities stated that the law on data retention is under review and is to be aligned with the requirements of the Decision of the Court of Justice of the European Union dated 8 April 2014, which declared Directive 2006/24/EC invalid. The intention is to maintain the data retention law with some amendments, in particular to include specific mechanisms providing for an independent review and to address proportionality issues.

Preservation of computer data

Data is preserved through the conservation order, which is explained in further detail in the section dealing with orders for traffic data.

Order for stored traffic/content data

Regulation 22 of S.L. 440.01 'Processing of Personal Data (Electronic Communications Sector)¹² Regulations' specifies that traffic data may be stored subject to the issue of a conservation order. The order must be served on the service provider within the retention period applicable to the traffic data, i.e. six months following the date of the communication. It can cover only existing data and not future communications. The conservation order may request that the service provider conserve that data for various periods of time.

The Maltese authorities reported that due to the geographical size of the country, it is relatively easy to correlate information found through open sources, such as social networking sites, with other information held in government databases. An example of this is the identification of an offender involved in a case of a child abuse. The police had collected information from the offender's computer and social networking sites. That information was cross-checked with a database belonging to the government's Education Department.

¹² In view of the CJEU judgment annulling the Data Retention Directive, these Regulations are being examined with a view to assessing whether any amendments are necessary.

5.2.2 Forensics and Encryption

The forensic procedures conducted by the Police Cyber Crime Unit involve 'dead-box forensics', i.e. analysis of computer systems which have been seized and preserved by the Cyber Crime Unit laboratory. This is carried out through the use of forensic write-blockers and forensic software available at the Cyber Crime Unit. Remote forensics is currently not carried out by the Cyber Crime Unit.

In all cases encountered by the Cyber Crime Unit, the encryption of data was only possible in instances where the suspect had cooperated with the police and willingly provided the password of the computer. Any difficulties encountered in this area should be dealt with by the EU Cyber Crime Centre (EC-3) within Europol.

5.2.3 e-Evidence

Malta does not have e-evidence rules and for this reason, it relies on the general evidence rules applicable to traditional offences. Nonetheless, when collecting and preserving digital evidence, the police refer to 'Guidelines on the Handling of Digital Evidence by the Association of Chief Police Officers'.

The general rules on admissibility are extended to cover digital evidence. It is the duty of the police to preserve and store e-evidence.

5.3 Protection of Human Rights/Fundamental Freedoms

Malta is a signatory to the European Convention on Human Rights, and all the procedural safeguards that apply in criminal proceedings and investigations are also applicable to investigations of cybercrime. Search and seizure, and other investigative measures, are subject to judicial supervision as provided for in the Criminal Code (Chapter 9 of the Laws of Malta). Real-time collection of data is in part regulated by the Criminal Code and Subsidiary Legislation 440.01 'Processing of Personal Data (Electronic Communications Sector) Regulations'. The applicable provisions are set out in Article 335E *et seq.* of the Criminal Code (in particular Article 355Q).

In accordance with Article 17(1) of the Data Protection Act (Chapter 440 of the Laws of Malta), any data relating to offences, criminal convictions or security measures may only be processed under the control of a public authority, unless specifically provided by another law. Therefore, in this case, the police are the sole authority responsible for gathering, processing and storing personal data. Whilst recognising the need to protect and preserve the right to freedom of expression and the right to privacy, it is also important to take into consideration certain factors which may override such rights, for example the need to prevent, suppress, investigate, detect and prosecute cybercrime.

Subsidiary Legislation 440.05 'Data Protection Regulations' is the legislation which regulates the collection of personal data for police purposes, where such is necessary for the prevention, suppression, investigation, detection and prosecution of crime. Those regulations are in line with the principles established by the Recommendation No R (87) 15 of the Council of Europe¹³. Their objective is to ensure a high level of protection and security in the police sector and to safeguard the rights of data subjects.

5.4 Jurisdiction

5.4.1 Principles applied to the investigation of cybercrime

Article 337E of the Criminal Code enables the Maltese courts to assert jurisdiction over computer-integrity offences: 'If any act is committed outside Malta which, had it been committed in Malta, would have constituted an offence against the provisions of this Sub-Title, it shall, if the commission affects any computer, software, data or supporting documentation which is situated in Malta or is in any way linked or connected to a computer in Malta, be deemed to have been committed in Malta'. Furthermore, Section 5(31) of the Schedule to the Extradition Act (Chapter 276 of the Laws of Malta) holds that any offence under the law relating to computer misuse shall be considered to be an extraditable offence.

¹³ Recommendation of the Committee of Ministers to Member States regulating the use of personal data in the police sector.

Furthermore, Article 310B deals with the jurisdictional issues related to cyber-related offences (fraud). The Maltese Courts can exercise jurisdiction on offences which are committed outside Malta when:

1. the offence took place, even only in part, in Malta or on the sea in any place within the territorial jurisdiction of Malta; or
2. the gain to the prejudice of another person has been received in Malta; or
3. a person in Malta knowingly assisted or induced another person to commit the offence; or
4. the offender is a Maltese citizen or a permanent resident in Malta and the fact also constitutes an offence according to the laws of the country where it took place.

The Maltese Courts may also exercise jurisdiction over offences concerning child pornography. Article 208B(5) provides that the Maltese Courts may have jurisdiction in a case if any of the below conditions is present:

- (a) Only part of the action giving execution to the offence took place in Malta; or
- (b) The offender is a Maltese national or permanent resident in Malta or the offence was committed for the benefit of a body corporate registered in Malta; or
- (c) The offence was committed by means of a computer system accessed from Malta notwithstanding that such computer system may be outside Malta; or
- (d) The offence was committed against a Maltese national or permanent resident in Malta.

If there is no special provision of law conferring jurisdiction upon the court in Malta to try any specific form of cybercrime, the general provision of jurisdiction (Article 5 of the Criminal Code) applies.

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

Subsidiary Legislation 9.20 'Prevention and Settlement of Conflicts of Exercise of Jurisdiction in Criminal Proceedings Regulations' transposes Council Framework Decision 2009/948/JHA into the laws of Malta. The regulation establishes the procedure to be applied in case of an offence which may be prosecuted in two or more Member States. It imposes a duty on the Attorney General to establish communications with the competent authorities of the other Member States.

The purpose of such contact is to confirm the existence of parallel criminal proceedings in terms of the person involved and the facts of the case. Once it is established that the same crime may be prosecuted twice, the competent authorities of the respective Member States must immediately initiate direct consultations so as to find the best practical and effective solution. During that consultation process, the competent authorities must keep each other constantly informed of any relevant procedural measures and provide information as needed. If no solution can be found, then the issue must be referred to Eurojust, which is the competent authority to decide on such procedural matters.

However, Malta has never used the provisions related to Council Framework Decision 2009/948/JHA.

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

Article 337E of the Criminal Code states that 'if any act is committed outside Malta which, had it been committed in Malta, would have constituted an offence against the provisions of this Sub-Title, it shall, if the commission affects any computer, software, data or supporting documentation which is situated in Malta or is in any way linked or connected to a computer in Malta, be deemed to have been committed in Malta'. So far, the Maltese authorities have interpreted this as meaning that the police may investigate and prosecute cybercrime offences committed in the 'cloud' only if such data is accessible from Malta.

5.4.4 Perception of Malta with regard to the legal framework for combating cybercrime

The main difficulty for the police is gathering information from internet service providers located overseas. Some states can transfer information only if the court authorises them to do so. The Maltese authorities stressed that whilst it is legally possible to gather such information, the process is very lengthy and in some cases may jeopardise the successful outcome of police investigations.

5.5 Conclusions

- The legal framework in Malta for cybercrime seems to be inspired by the Convention on Cybercrime and relevant EU instruments, as well as other sources. Malta ratified the Council of Europe Convention on Cybercrime on 12 April 2012 and has transposed Directive 2013/40/EU on attacks against information systems.
- Malta stated that it has transposed most of the provisions of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. However, since not all the instruments provided for in the Directive are reflected in Maltese legislation, full implementation of the Directive should be reviewed.
- Fraud and forgery are criminalised in the Criminal Code. Regulation 9 of Subsidiary Legislation 440.01 'Processing of Personal Data (Electronic Communications Sector) Regulations' deals with sending or controlling the sending of spam.
- Malta declared that it has launched a complex process to identify the needs and gaps in law enforcement agencies and to strengthen their capability to investigate and combat cybercrime. In this context, the evaluators recommend reviewing the existing legislation to ensure its relevance and effectiveness in the cyber world.
- Malta has implemented legislation providing for computer searches, real-time collection of computer data, orders for stored traffic/content data and preservation of computer data. The Cyber Crime Unit is not empowered to carry out interception and online undercover work. The police may, however, request the Court to carry out a Magisterial Inquiry in order to collect and preserve evidence which cannot be collected through the general police powers.

- The Maltese representatives said that search and seizure capabilities were limited. As an example, the police do not have the capacity to carry out on-site extraction of data from large-scale computers, mainly due to a lack of knowledge and equipment.
- Regulation 20 specifies the categories of data which must be retained by service providers. Traffic data relating to internet access and email must be retained for a period of six months. The Maltese authorities expressed a need to harmonise the retention period throughout the EU.
- Malta does not have e-evidence rules and for this reason, it relies on the general evidence rules applicable to traditional offences. Therefore, the general rules on admissibility are extended to cover digital evidence. In the opinion of the evaluators, collection, analysis and usage of electronic evidence not only in relation to crimes against and by means of computers but also in relation to any crime could strengthen the Maltese criminal justice system since any offence may involve electronic evidence.
- Subsidiary Legislation 9.20, 'Prevention and Settlement of Conflicts of Exercise of Jurisdiction in Criminal Proceedings Regulations' transposes Council Framework Decision 2009/948/JHA into the laws of Malta. However, it has never been used in practice.
- The Criminal Code enables the Maltese courts to assert jurisdiction over computer-integrity offences if any act committed outside Malta constitutes an offence against the provisions specified therein and affects any computer, software, data or supporting documentation situated in Malta.

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

No recent cyber attacks within the Maltese monitoring area have been reported to the Critical Infrastructure Protection Unit and/or CSIRT-Malta.

6.1.2 Mechanism to respond to cyber attacks

The Maltese authorities stated that there is currently no coordinated multidisciplinary mechanism to respond to a serious cyber attack in place in Malta. However, Malta is currently conducting its first National Risk Assessment (NRA) exercise. The NRA exercise will consider the potential risk of serious cyber attacks and the required treatment mechanisms.

Moreover, the Electronic Communications Networks and Services (General) Regulations, L.N. 273 of 2011, impose an obligation upon the undertaking providing the network elements or service concerned to report cyber attacks/incidents in the case of attacks leading to a breach of security or loss of integrity with severe implications for the operation of services or resulting in the failure or serious degradation of international connectivity. In such cases, the Malta Communications Authority (MCA) is obliged to inform the police and the European Network and Information Security Agency (ENISA). The MCA may also inform the public if it deems that disclosing the breach is in the public interest.

In relation to the laws administered by the MCA, network and services operators are required to take appropriate measures to manage the risks and safeguard the security of their networks and services and stored personal data. Where there is a significant risk of failure or serious degradation of international connectivity, network and service providers are to notify MCA.

The role of operators of critical infrastructure is regulated by L.N 434 of 2011, 'Critical Infrastructures and European Critical Infrastructures (Identification, Designation and Protection) Order'. That order is the transposition of Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In performing its role, the Critical Infrastructure Protection (CIP) Directorate provides cyber security alerts and warnings to stakeholders and its constituents via CSIRT-Malta's services. CSIRT-Malta's services include information on how to protect critical information assets from cyber threats and vulnerabilities. In addition, it also cooperates and exchanges non-sensitive information on cyber security with CSIRTs in other countries to promote and improve security on the internet. Another function of the CIP Directorate is to inform local IT security experts about the latest cyber threats and the handling of cyber accidents; this is also a knowledge sharing exercise. In fact, in 2014, the CIP organised two 'Cyber Incident Handling' workshops in collaboration with ENISA. The Directorate is planning to organise a similar event in the last quarter of 2015.

In addition, the Malta Gaming Authority (MGA) ensures that current and prospective licensees have certain procedures in place. Operators are required to submit documents outlining their system architecture, including details about the security of the system and the network infrastructure. The role of the MGA is to ensure that its licensees have the necessary systems and processes in place to minimise cyber attack threats and mitigate their effects. To that end, the MGA also examines operators' agreements with payment gateways, payment service providers, software providers, co-location service providers and any providers of services outsourced by the operator. In the case of failures of the licensee's systems or other similar issues, including when this is due to cyber attacks, the licensee is obliged to report the incident to the MGA under Regulation 48 of the Remote Gaming Regulations (S.L. 438.04 of the Laws of Malta). The licensee must follow the procedures laid down by the Authority in a guidance note entitled 'Remote Gaming Incident Reporting/Addition of Hardware/Decommissioning of Equipment Procedures', which requires the licensee to draw up a report in writing, indicating the cause of failure of the game and the steps taken by the licensee to remedy such failure. It must show that the licensee's actions were consistent with the aforementioned Regulation 48 of the Remote Gaming Regulations.

With regard to financial institutions, there is no legal provision requiring them to report cyber attacks. However, the Maltese authorities claim that if a financial institution experienced any event of a significant nature which could adversely affect the institution, or its compliance with regulatory and legal requirements, or its operations or customers, then it would be expected to report the event to the Malta Financial Services Authority (MFSA). A report may also be made to the police but that is at the discretion of the institution.

The main obstacles when responding to cyber attacks reported by the Police Cyber Crime Unit are as follows:

- limited technical knowledge when dealing with certain forms of cybercrime. In such instances, the police have to rely on the knowledge of the IT administrators of the affected institution/organisation. Hence, this would undermine the efficacy of the police investigations
- limitations in terms of the availability of tools
- lack of proper cooperation from foreign internet service providers and LEAs. In some instances, the requested data is not provided within the established timeframes. Such delays compromise the investigation and/or can make it difficult to block an attack effectively.

6.2 Actions against child pornography and sexual abuse online

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

Currently, Malta does not have any software database identifying victims. However, the Cyber Crime Unit has submitted proposals for funding under the Internal Security Fund (ISF) to upgrade the equipment used in the Cyber Crime Unit's laboratory. These funds shall be allocated to the purchase of computers and network equipment required for the Cyber Crime Unit to access the International Child Sexual Exploitation Database, which is managed by Interpol networks.

Malta is represented and actively participates in meetings of the European Cybercrime Task Force (EUCTF). Malta is also participating in the EMPACT sub-priority on cybercrime 'Online Child Abuse'.

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

As regards sex exploitation/abuse online, one of the tools used is the Hotline Reporting Mechanism.

With regard to sexting and cyber-bullying, individuals are provided with tips on how to prevent sexting and cyber-bullying through educational campaigns. Information and support can be obtained via the National Helpline (179) and the website 'kellimni.com'.

A number of Memoranda of Understanding between the Social and Welfare Service Organisation (Aġenzija Appoġġ) and the Malta Police are also in place relating to several measures including:

- child protection cases
- hotline reporting and filters
- review of standard operating procedures

Child pornography investigations are dealt with by the Cyber Crime Unit and the Vice Squad. The composition of the Vice Squad is made up of thirteen officers, namely: four inspectors, one sergeant major, two police sergeants and six police constables.

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

Through the project 'BeSmartOnline!', Aġenzija Appoġġ is currently maintaining and coordinating the 'hotline' tool. That mechanism is an online reporting system which provides a secure and confidential environment where the public can report any websites containing child sexual abuse material. Following receipt of a report, Aġenzija Appoġġ reviews it and verifies whether the website contains illegal material. If the website contains unlawful material, the Aġenzija Appoġġ analyst team duly informs the Police Cyber Crime Unit. It also notifies states which are hosting illegal content on their servers. International cooperation is facilitated through membership of the International Association of Hotlines (Inhope). The objective of the hotline is to:

- block websites hosting child sexual abuse content

- protect children from repeated victimisation and take all the necessary measures to protect the identity of the child
- prevent Maltese internet users from accessing websites containing such inappropriate material related to child abuse

The table below shows the number of reports received through of the hotline

Period	Total Number of Reports	Total Number of Reports relating to Child Sexual Abuse Material
October 2010 – September 2012	192	107
October 2012 – September 2014	368	245
October 2014 – 15th July 2015	130	86

Information on how to make complaints is available online on the website www.childwebalert.gov.mt. Further information can be obtained by contacting Aġenzija Appoġġ, the Malta Communications Authority, the Cyber Crime Unit and/or the Office of the Commissioner for Children.

Moreover, various events are organised to educate children about the safe use of the internet. The following are examples of those events, which are held annually:

- The Office of the Commissioner for Children organises an event to mark World Children's Day. During the event, children are invited to participate in workshops. One of those workshops focuses on encouraging safe use of the internet
- Each year, 'BeSmartOnline!' organises various activities to mark the celebration of 'Safer Internet Day'. Several fun activities are organised, with the aim of providing children with information on how to be safe online
- The Office of the Commissioner for Children organises an annual children's rights course, 'Right 4U'. This is a live-in course, in which young people aged between thirteen and fifteen years participate in various activities and discussions related to their rights. One of the themes selected for 2015 was the safe use of new technologies

Through the project 'BeSmartOnline!', many awareness-raising initiatives have been successfully implemented through a widespread educational campaign. Educators have organised interactive lessons specifically designed to empower and encourage children to use the internet safely. Children are also informed about the possibility of using the free National Helpline (179) and the website kellimni.com. Those services allow children to ask questions and report any difficulties they may have. They also serve as tools to support children through one-to-one interventions.

Furthermore, the Commissioner for Children, in collaboration with MCAST students of Art and Design, has produced material to educate children about internet safety. That material includes: (a) an activity book to be used by children aged between five and seven; (b) a comic book to be used by children aged between eleven (11) and fifteen (15); and (c) a video clip to be viewed by teenagers aged between sixteen (16) and eighteen (18).

Moreover, information campaigns have been organised to educate the public, parents, educators and carers about the consequences of harmful/illegal behaviour online. Companies offering internet services are encouraged to provide information about inappropriate online behaviour.

Through Article 208AB(1) of the Criminal Code, Malta has incorporated measures related to sex tourism including the dissemination of child abuse material or materials advertising the opportunity to commit any of the offences under Articles 204, 204A to 204C, both inclusive, 208A(1) and 208A(1A), and involvement in the organisation of travel arrangements with the aim of committing any of the said offences.

6.2.4 Actors and measures countering websites containing or disseminating child pornography

The Cyber Crime Unit is the authority responsible for coordinating the blocking of web pages. There are no legal obligations on internet service providers to filter websites. Yet, through a Memorandum of Understanding, all local internet service providers have voluntarily agreed to block access to websites containing child sexual abuse material. The intention is to formalise the cooperation in place concerning the Child Abuse Internet Filter, the objective of which is to block access to websites that host or encourage the distribution of child abuse-related material by implementing a DNS filter that redirects requests for access to known child abuse-related websites to a stop page.

The Malta Police Force maintains a 'stop-list' which blocks any access to websites containing child sexual abuse material. The 'stop-list' is used in the implementation of a Child Abuse Internet Filter, which is operated in cooperation with the local internet service providers. As a participatory member of the COSPOL Internet-Related Child Abuse Material Project (CIRCAMP) and the Global Alliance against Child Sexual Abuse Online, Malta blocks only web domains disseminating child sexual abuse files.

Since 2009, the Malta Cyber Crime Unit started using the Child Abuse Internet Filter (CAIF) as a mechanism to block Maltese internet users from accessing websites known to contain child sexual abuse material. If any local websites are found to contain unlawful material, the police immediately commence investigations. In such cases, they may request the issuance of a court order to take all the necessary measures. However, Malta has never had any cases of locally hosted child abuse websites.

In the case of websites hosted overseas, the websites are added to the 'stop-list' and the respective law enforcement authorities are notified accordingly. Moreover, the Malta Cyber Crime Unit immediately notifies the respective law enforcement authorities. If necessary, the LEAs are contacted through the Interpol or Europol networks. Moreover, since Malta is part of the collaborative INHOPE network, it can also notify that network.

6.3 Online card fraud

6.3.1 Online reporting

In Malta, it is very common for private citizens to report online card fraud. According to the Maltese authorities, they normally do so through their banks. In contrast, private companies rarely report online card fraud cases, particularly if the perpetrators are foreigners. Whilst the reasons for this are not known, it is presumed that private companies, in particular online betting ones, consider online card fraud to be a normal business risk. Another possible reason is that companies might think that reporting such case to the LEAs is a waste of time, particularly if the case concerns another jurisdiction. Yet, companies are more willing to report online card fraud if the offender is a Maltese national. In fact, the police have received some reports involving Maltese individuals defrauding local companies through online trade.

The police use the equipment in the cybercrime laboratories, which is normally used for copying and analysing computer data forensically. However, other than this, the police do not have any special equipment used specifically for online card fraud. Despite this, the police have the expertise and skills needed to deal with such technical offences. In fact, the police try to keep up-to-date with any developments by participating in international fora and seminars. The police are actively involved in the Europol Focal Point Terminal.

As regards fraud committed through gaming channels, fraud management procedures must be submitted for scrutiny at the application stage and their adequacy is re-assessed during each compliance audit carried out on the licensee. With respect to card fraud, licensees are required to register players before allowing them to play. Regulation 32 of the Remote Gaming Regulations (Legal Notice 176 of 2004) stipulates that an application for registration must at least include a declaration that the player is over eighteen years of age, the player's identity, the player's place of residence, and the player's valid email address.

Moreover, under Regulation 36 of the Remote Gaming Regulations, a licensee cannot make a payment in excess of €2 329.37 out of a player's account to the player until the player's identity, age and place of residence have been verified. If the player wishes to withdraw a lesser amount, Regulation 37 of the Remote Gaming Regulations allows licensees to delay the remission of funds for such time as is reasonably necessary for the purpose of:

- (i) verifying the player's registration as a player;
- (ii) verifying the playing of a game by the player;
- (iii) conducting security and other internal procedures in relation to the player's account; and
- (iv) ensuring that the rules that are approved relating to the award of the prizes to players have been complied with.

This ensures that the operator has the necessary tools to identify instances of card fraud where it is suspected. Possibly the most important defensive tool against online card fraud in remote gaming is Regulation 37(2) of the Remote Gaming Regulations. This states that a licensee can only remit funds to the player into the same account from which the funds deposited by the player into his or her account originated. Hence an online card fraudster would be unable to have the funds remitted into his or her personal account, as the funds would only be remitted by the remote gaming operator into the card account which was used to make the deposit.

Furthermore, from the perspective of the EU Electronic Communications Regulatory Framework, operators of electronic communications networks provided to the public are obliged to take appropriate measures to manage risks and safeguard the security of their networks and services.

6.3.2 Role of the private sector

The Maltese authorities reported that there was a very good relationship between the police and the banking industry. That relationship is based upon cooperation, which facilitates the process of investigating and prosecuting online card fraud cases. In fact, whenever an abuse involving a payment tool is detected, the banks immediately refer the case to the police.

The evaluation team was informed that the Maltese banks are very proactive in implementing security measures aimed at reducing and preventing abuse. In the past, the police have given input on possible new strategies and security measures which could be adopted in securing the ATM network (suggestions which were often implemented). However, at present, the police are not very involved in enhancing the security of non-cash payments and transaction authorisations.

Following consultations with the police, the Maltese banking sector has introduced a series of measures to limit such criminal activities. Almost all ATMs within the Maltese banking network are of the latest generation, and most are equipped with Card Protection Kit (CPK) jammers. All financial institutions are EMVII compliant, and all merchant terminals and cards are equipped with chip and pin technology. The banks have also embarked on a customer profiling programme, and some have also implemented authentication methods for cards sent by post to customers.

In the opinion of the evaluators, cooperation with the private sector seems to be good, especially with the banking sector and ISPs. For the most part, a formal framework for cooperation seems to be missing.

6.4 Conclusions

- A coordinated multidisciplinary mechanism for responding to cyber attacks in Malta has not been established. This may be because Malta has not set up a national cyber security strategy yet. However, the Maltese authorities said that they were currently conducting their first NRA exercise to examine the potential risk of serious cyber attacks and the required treatment mechanisms accordingly.
- The Electronic Communications Networks and Services (General) Regulations oblige the undertaking providing the network elements or service concerned to report cyber attacks/incidents. The Critical Infrastructure Protection (CIP) Directorate provides cyber security alerts and warnings to stakeholders and its constituents via CSIRT-Malta services.
- Malta has implemented a broad range of measures to tackle sexual abuse and sexual exploitation of children, including prevention and awareness campaigns, legislative measures and the blocking of websites with illegal content.
- In the field of child pornography and sexual abuse prevention, Malta has established valuable tools such as the 'stop-list' and the project 'BeSmartOnline!'. Such measures aim to educate the public, parents, educators and carers about the consequences of harmful/illegal behaviour online. Moreover, companies offering internet services are encouraged to provide information on inappropriate online behaviour. In the opinion of the evaluation team, the involvement of the national authorities and other partners (such as academia) in the above-mentioned projects and the positive role they play should be regarded as an example of best practise.
- Internet service providers are requested to provide information on child abuse materials disseminated online. The Cyber Crime Unit has managed to establish direct contact with representatives of all the ISPs. Consequently, all local ISPs have voluntarily signed the Memorandum of Understanding in order to block access to Maltese local users from accessing any website containing child abuse material. Since blocking web pages with illegal content seems to be efficient, Malta could share its experience with other countries.

- Malta is one of the few countries left to connect to the Interpol Child Sexual Exploitation (ICSE) Database. Since it is a powerful intelligence and investigative tool which allows specialised investigators to share data with colleagues around the world, in the opinion of the evaluators, Malta's lack of the access to the ICSE Database hinders its capacity to investigate child sexual exploitation and to cooperate with external partners who could benefit from Malta's experience.
- There is no specific obligation of reporting on either financial institution, critical infrastructure or in cases related to child abuse. Reporting obligations do not specifically relate to cybercrime, but rather to operations and obligations towards clients, for example the loss of service in the case of internet service providers. Under the Maltese legal system, very few categories of persons are obliged to report a crime (e.g. public officers, doctors, etc.). Thus, there is no general legal obligation to report a crime.
- It is very common for private citizens to report online card fraud. They normally do so through their banks. In contrast, private companies rarely report online card fraud cases, particularly if the perpetrators are foreigners. This may be due to the lack of a memorandum of understanding to facilitate cooperation. Therefore, in the opinion of the evaluators, Malta should strengthen its policy vis-à-vis the financial sector so as to encourage it to report cybercrime more frequently and in a more structured manner. Moreover, Malta could consider making the practice more mandatory.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

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

In accordance with Article 117 of the Police Act (Chapter 164 of the Laws of Malta), the police may, directly or through regional or international police organisations, cooperate with any state agency having similar powers and duties in any country. However, Maltese legislation does not impose any formal requirements or specific procedures for cooperation with Europol/EC3, Eurojust or ENISA. Nonetheless, the Cyber Crime Unit offers its assistance and advice 24/7.

At the time of the on-site visit, Malta's National Member at Eurojust was also its Deputy Attorney General. In addition, the Deputy National Member and the assistant to the National Member are prosecutors within the Attorney General's Office. Their position within the Maltese judicial system as prosecutors before the criminal courts, as well as the role of the Attorney General's Office as the central judicial authority in all matters falling within the field of international legal cooperation, is crucial for carrying out Eurojust's tasks in Malta.

The Attorney General's Office also has the task of assisting the police in prosecutions when the need arises, since the police are also prosecutors before the Court of Magistrates. This has been pivotal to achieving the cooperation and coordination requested with respect to both incoming and outgoing requests for legal assistance.

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

Malta's experience of cooperation with Eurojust involved a request made to Hungary, and the intervention of the Hungarian desk was considered instrumental. The requested information was given to the Maltese authorities within a relatively short time-frame. The offence in question was a threat of terrorist activity.

In the opinion of the Maltese authorities, Eurojust offers great potential for coordinating investigations and prosecutions and, more importantly, it plays a fundamental role in JITs. It therefore represents a necessary framework and capacity which should be utilised more by Member States. More funding for JITs could be warranted, given the increase in requests for joint investigations on the back of the success of Eurojust in that field.

The Maltese authorities spoke of a very positive relationship with Europol and EC3, largely due to two reasons: (1) it serves as a point of reference whenever difficulties are encountered by the police; and (2) it is a very convenient platform for sharing experiences and practices.

The Maltese authorities appreciate the work being carried out by EC3 and participate in most activities organised by the centre. Malta participates in Europol's FP Terminal, and collaborates with and gives assistance to all international authorities when requested.

7.1.3 Operational performance of JITs and cyber patrols

Malta has not yet been part of a JIT concerning cybercrime and has no experience with participation in cyber patrols.

7.2 Cooperation between the Maltese authorities and Interpol

Interpol channels are used to communicate with counterparts in foreign countries. In Malta's experience, very little information is forthcoming and it is not provided quickly enough to conclude investigations successfully.

7.3 Cooperation with third states

Requests to third countries are sent via Interpol channels when cooperation is required from law enforcement agencies there. According to the Maltese authorities, collaboration with third countries needs to be developed further.

7.4 Cooperation with the private sector

The private sector – mainly internet service providers – is requested to provide information and retain data which is needed for any police investigation. The Cyber Crime Unit has managed to establish direct contact with all the ISP representatives responsible for the provision of information and data retention.

Moreover, the remote gaming sector is urged by the MGA to contribute any relevant information or evidence requested during the investigation of any offence. As the regulator, the MGA also cooperates with the Executive Police when required to do so. According to Article 20 of the Lotteries and Other Games Act (Chapter 438 of the Laws of Malta), the MGA is obliged to provide any information, confidential or otherwise, in the course of any investigation or prosecution by the Executive Police for offences against the Act or when requested to do so during civil or criminal proceedings relating to offences against the Act.

In addition, in an effort to combat the online dissemination of child abuse material, all local ISPs have voluntarily signed the Memorandum of Understanding. The objective of that is to adopt the measure known as the 'Child Abuse Internet Filter', which is coordinated by the Cyber Crime Unit. The filter prevents local Maltese users from accessing any website containing child abuse material.

The Cyber Crime Unit contacts ISPs located abroad directly, with the aim of informally obtaining information which is relevant to any investigation being conducted by the police. The Cyber Crime Unit generally tries to create a template for such requests which is acceptable to both parties. It has sought to establish direct contact with Google, Facebook, Ask.fm and Microsoft. This would facilitate the investigative process by making it more efficient and effective.

7.5 Tools of international cooperation

7.5.1 Mutual Legal Assistance

Mutual legal assistance is mainly provided for by national laws, namely:

- the Criminal Code (such as Articles 435B-E, 628A-B, 647B, 649), which applies to all offences without distinction
- the Prevention of Money-Laundering Act (Chapter 373 of the Laws of Malta), which lists as predicate offences all offences, thus including cybercrime offences (Articles 9-11)
- the Dangerous Drugs Ordinance (Articles 24B-D)

By virtue of these laws, requests by a foreign judicial, prosecuting or administrative authority are made pursuant to, and in accordance with, any treaty, convention, agreement or understanding between Malta and the country from which the request emanates or which applies to both such countries or to which both such countries are a party. Even without a treaty, convention, agreement or understanding, Malta may still extend mutual assistance on the basis of the principle of reciprocity.

On this basis, international courts and any authority situated outside Malta which is vested with judicial, prosecuting or administrative powers may request Malta's assistance in the process of investigations concerning cybercrime. They may apply to the Criminal Court for the issuance of an investigation order, attachment order and/or monitoring order. These orders enable foreign authorities or international courts to carry out investigations in Malta in respect of any person suspected to have committed a crime.

The Attorney General plays an important role in providing mutual legal assistance. He or she may in particular:

- (i) consent, with the agreement of the Minister for Justice, to the temporary surrender of a person in custody in a foreign state for the purpose of investigations to be carried out or being carried out in Malta. Consent may also be requested where the foreign authorities or international courts request the temporary surrender of a person in custody in Malta for the purpose of an investigation to be carried outside Malta;
- (ii) apply to the Criminal Court for the issuance of a temporary seizure of all or any of the moneys or property, movable or immovable, of a person charged or accused in proceedings before a court situated outside Malta;
- (iii) authorise the Executive Police and, if necessary, the Customs Authorities to allow a controlled delivery to take place with a view to identifying suspects who may be involved in the commission of a criminal offence under the laws of Malta or under the laws of other states. Further to this, the Attorney General may give authorisation for the investigations to be carried out by officers acting under covert or false identity;
- (iv) authorise a magistrate to examine on oath any witnesses present in Malta and to conduct investigations through a search and/or seizure order.

Whilst the nature of the offence is not a factor in determining the relevant authorities, requests for legal assistance can be made either by the police in the course of investigations or by any of the parties during the criminal proceedings. The Attorney General's Office has been designated as the central judicial authority in all major agreements dealing with mutual legal assistance. The same designation has also been made for the purposes of the receipt and implementation of European Arrest Warrants, extradition requests, freezing orders, confiscation orders and the enforcement of financial penalties and other instruments on mutual recognition orders. In the course of the investigations, Interpol, Eurojust and the EJM may also be called on if warranted in view of the urgency of the matter, or when additional information is required.

The statistics on Mutual Legal Assistance cases concerning cybercrime are presented below.

<i>Statistics on Mutual Legal Assistance cases concerning cybercrime</i>			
<i>Year</i>	<i>Child pornography online</i>	<i>Attacks on information systems</i>	<i>Credit card fraud</i>
<i>2011</i>	<i>0</i>	<i>0</i>	<i>3</i>
<i>2012</i>	<i>0</i>	<i>0</i>	<i>14</i>
<i>2013</i>	<i>0</i>	<i>4</i>	<i>12</i>
<i>2014</i>	<i>1</i>	<i>0</i>	<i>9</i>
<i>2015*</i>	<i>0</i>	<i>0</i>	<i>13</i>

**end of August 2015*

All requests for MLA were received from signatories of the 1959 MLA Convention and almost all were from EU member states, thus also signatories of the 2000 EU Convention. The actions that can be requested via MLA depend on the area of cybercrime being addressed. The most common cases relate to online fraud and match fixing (online sports fraud). Actions requested are generally investigative, ranging from the identification of 'end-users' basic information to the interrogation of suspects.

With regard to the average response time, requests are usually processed within a week and executed within a maximum of three to six months. However, this depends on the complexity of the case, the measures requested and the urgency of the case. Therefore, the Maltese authorities expressed a wish for requests to be handled more swiftly.

Informal communications are made through the police to other police channels or through Eurojust, if the case so warrants.

Malta has used the bilateral 'Treaty on Certain Aspects of Mutual Legal Assistance in Criminal Matters between the Government of the United States of America and the Government of Malta' to make requests related to the investigation and prosecution of cybercrime. In some cases, the requests made by Malta have been refused on the basis that they would violate fundamental human rights provisions. For example, Malta requested information on users of specific accounts in relation to human trafficking, but the request was turned down on the basis that it infringed data privacy and due to the lack of probable cause. Other requests for information were refused due to a possible breach of freedom of expression.

7.5.2 Mutual recognition instruments

Malta reported that it has never used any mutual recognition instruments with regard to cybercrime. Nonetheless, the Maltese authorities raised the need to work on an updated handbook on the application of European freezing orders at European level, based on Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, to facilitate the work of practitioners.

7.5.3 Surrender/Extradition

Given that all cybercrime offences carry a maximum punishment of imprisonment of at least one year or more, all offences are extraditable crimes and thus a cause for surrender.

There are no specific procedures or conditions that need to be fulfilled in cases of cybercrime. By virtue of Article 14(1)(b) of the Extradition Act (Chapter 276 of the Laws of Malta), Maltese legislation enables the magistrate to issue a provisional arrest warrant. This shall be issued only if the magistrate is informed that a person accused of an extraditable offence, or alleged to be unlawfully at large after conviction of such offence, is in Malta or is believed to be on the way to Malta. Article 9 of S.L 276.05 states that any provisional warrant must be executed by a police officer. Urgent requests are given priority and when specific timelines for action are indicated, the Maltese authorities strive to ensure that they are met.

In urgent cases, and as dictated by the relevant instruments providing for extradition, Interpol can be used. Requests for extradition are made via diplomatic channels to the Ministry of Justice. European Arrest Warrants are sent directly to the Attorney General's Office in its capacity as central judicial authority or via SIRENE channels. Only a Court of Committal can decide on extradition requests in terms of the Extradition Act (Chapter 276, Laws of Malta).

The table below shows statistics on extradition cases concerning cybercrime.

Statistics on extradition cases concerning cybercrime			
Year	Child pornography online	Attacks on information systems	Credit card fraud
2011	0	0	0
2012	2	0	0
2013	0	0	0
2014	1	0	0
2015*	0	0	0

**end of August 2015*

7.6 Conclusions

- The police may, directly or through regional or international police organisations, cooperate with any state agency having similar powers and duties in any country. However, Maltese legislation does not impose any formal requirements or specific procedures for cooperating with Europol/EC3, Eurojust, ENISA.
- The evaluation team saw that there was close cooperation between Europol/EC3 and the police at national level. The Attorney General is in charge of ensuring smooth cooperation with Eurojust. The representatives of the National Desk at Eurojust are prosecutors from the Attorney General's Office. Although the Maltese representation at Eurojust seems to be sufficient, the evaluation team did not observe much cooperation in cybercrime cases.
- Malta does not have any experience of participating in a JIT. In the opinion of the Maltese authorities, Eurojust offers great potential for coordinating investigations and prosecutions and, more importantly, it plays a fundamental role in JITs. It therefore represents a necessary framework and capacity, which should be utilised more by Member States. More funding for JITs could be warranted, given the increase in requests for joint investigations on the back of the success of Eurojust in that field. Moreover, the added value Eurojust may offer in providing judicial assistance in complex, cross-border cases should, in the evaluators' view, be broadly advertised.
- The Maltese authorities consider cooperation with the private sector at national level to be good, in particular with internet service providers. The Cyber Crime Unit has managed to establish direct contact with all the ISP representatives responsible for the provision of information and data retention. Moreover, in an effort to combat the online dissemination of child abuse material, all local ISPs have voluntarily signed the Memorandum of Understanding. Furthermore, the remote gaming sector is urged by the MGA to contribute any relevant information or evidence requested during the investigation of any offence. Nonetheless, the obligation to cooperate with public authorities is not equally established for private companies representing crucial sectors of the Maltese security system, such as financial institutions.

- Malta provides mutual legal assistance on the basis of its national legislation and in accordance with any treaty, convention, agreement or understanding between Malta and the country from which the request emanates or which applies to both such countries or to which both such countries are a party. However, even without a treaty, convention, agreement or understanding, Malta may still extend mutual assistance on the basis of the principle of reciprocity. Most cybercrime-related MLA requests are linked to credit card fraud. The Maltese authorities would like MLA requests to be handled more swiftly. However, in the evaluators' opinion, if Malta were to participate more actively in international efforts to increase the efficiency of the MLA process, it would establish direct contacts with counterparts from other countries.
- Malta reported that it has never used any mutual recognition instruments with regard to cybercrime. Nonetheless, the Maltese authorities raised the need to work on an updated handbook on the application of European freezing orders at European level, based on Council Framework Decision 2003/577/JHA of 22 July 2003, to facilitate work of practitioners.
- Requests for extradition are made via diplomatic channels to the Ministry of Justice. European Arrest Warrants are sent directly to the Attorney General's Office in its capacity as central judicial authority or via SIRENE channels. In urgent cases, and as dictated by the relevant instruments providing for extradition, Interpol can be used.

8 TRAINING, AWARENESS-RAISING AND PREVENTION

8.1 Specific training

The Police Academy is responsible for training the police. The academy trains recruits, inspector cadets and serving police officers. It offers courses for new police recruits, and these include a module on cybercrime awareness. That module incorporates cybercrime investigations, basic collection and handling of digital evidence, and report-taking. Matters relating to child victims of sexual abuse or exploitation are also included in the training curriculum for Continuous Professional Development of Police Officers and Higher Officials.

Officers assigned to the Police Cyber Crime Unit receive on-the-job training, as well as other training provided by European Law Enforcement Agencies. These training initiatives include CEPOL courses, ISEC courses and OLAF courses. Officers typically attend 2-3 training courses a year. The specific subjects and frequency depend upon the availability of such courses.

Special cybercrime-related courses/programmes are still being developed by the University of Malta. However, the Department of Criminology within the University of Malta's Faculty of Social Wellbeing offers study units on cybercrime.

The Malta Police Academy does not have a specific budget allocated to cybercrime training. However, police officers attend training which is EU-based and refunded.

The Judicial Studies Committee organises training courses for the Maltese judiciary on a regular basis. So far, members of the judiciary who have shown a specific interest in cybercrime issues have been given training. The evaluation team was informed that preparations are currently under way for a training seminar on cybercrime for the entire judiciary, to be held in early 2016. It is envisaged that the training seminar will involve the University of Malta and the Attorney General's Office, with financial support from the Malta Communications Authority. However, no reliable data have been provided to the evaluation team regarding the involvement of judges in training on cybercrime.

8.2 Awareness-raising

There are a number of initiatives and projects in Malta aimed at raising awareness, empowering and educating children and teens, carers and educators on the safer use of the internet, combating illegal and harmful behaviour, facilitating reporting of illegal content or inappropriate material, particularly in relation to child sexual abuse material, ensuring that the operator has the necessary tools to identify instances of card fraud, etc.

As an example, the 'BeSmartOnline!' project is aimed at raising awareness of the risks commonly associated with the use of ICT, particularly the internet. It seeks to tackle those risks which could be detrimental to a child's physical and mental well-being at the expense of an enjoyable online experience. In view of this, the project does not deal with cybercrime leading to direct or indirect financial loss, such as viruses, malware, fraud, etc. The range of themes often includes cyber-bullying, sexting and self-exposure, among others – which, in some cases, could also constitute cybercrime. For the past five years, the MCA has acquired funds for the implementation of the project through three different calls. The project is currently co-funded (50 % European Commission, 50 % national funds) through the Connecting Europe Facility (previous funds were acquired through the European Commission's Safer Internet Programme).

Awareness efforts include:

- School campaigns: in collaboration with DQSE, a lesson on 'Online Critical Thinking' has been delivered to both primary and secondary school students
- Public Information Days: 'BeSmartOnline!' participates in various family events such as the 'Welcome Spring Festival' and 'Maratona Roti', in order to distribute resources to children and parents
- Community sessions: in collaboration with a number of local councils, 'BeSmartOnline!' organises free community sessions to discuss good digital parenting with parents
- Production and dissemination of resources: a large number of resources, such as tip sheets, have been produced and distributed to all students in all schools;
- Seminars: a number of seminars have been organised (often including foreign speakers) for educators and school management
- Media marketing campaigns.

In addition to the above, the members of the Cyber Crime Unit promote safe use of the internet through various educational campaigns. The campaigns consist of: (a) educational presentations for teaching staff, parents, young children and students; and (b) media appearances.

The statistics below relate to the educational campaigns run by the Cyber Crime Unit.

<i>Period</i>	<i>Teachers</i>	<i>Parents</i>	<i>Young children & Students</i>	<i>Others</i>	<i>Media: Radio & TV</i>	<i>Total</i>
<i>Oct – Dec 2007</i>	<i>1</i>	<i>1</i>	<i>3</i>	<i>1</i>	<i>1</i>	<i>7</i>
<i>Jan – Dec 2008</i>	<i>3</i>	<i>16</i>	<i>17</i>	<i>3</i>	<i>12</i>	<i>51</i>
<i>Jan – Dec 2009</i>	<i>10</i>	<i>16</i>	<i>26</i>	<i>1</i>	<i>8</i>	<i>61</i>
<i>Jan – Dec 2010</i>	<i>6</i>	<i>23</i>	<i>32</i>	<i>1</i>	<i>6</i>	<i>68</i>
<i>Jan – Dec 2011</i>	<i>3</i>	<i>13</i>	<i>35</i>	<i>1</i>	<i>24</i>	<i>76</i>
<i>Jan – Dec 2012</i>	<i>2</i>	<i>13</i>	<i>34</i>	<i>4</i>	<i>27</i>	<i>80</i>
<i>Jan – Dec 2013</i>	<i>4</i>	<i>7</i>	<i>38</i>	<i>7</i>	<i>13</i>	<i>69</i>
<i>Jan – Dec 2014</i>	<i>2</i>	<i>19</i>	<i>35</i>	<i>6</i>	<i>16</i>	<i>78</i>

A number of other awareness and prevention measures have been taken by the authorities to raise awareness of cybercrime threats, such as: educational campaigns held by the Cyber Crime Unit, involvement of 'Personal, Social and Career Development' (PSCD) in the 'BeSmartOnline!' project for three years to give lessons to primary and secondary school students, and training for teachers on online safety sponsored by the Malta Communications Authority (MCA).

Secondary Education: the PSCD Department has revamped the syllabus of Forms 3, 4 and 5 in order to include more digital citizenship objectives. The learning outcomes of the syllabus are as follows:

Form 3 syllabus (students aged between 13 and 14 years):

- To enable students to understand the risk of inappropriate sharing of personal information
- To enable students to reflect on their responsibility to protect the privacy of others when posting information about them online

Form 4 syllabus (students aged between 14 and 15 years):

- To enable students to appreciate the good use of technology in one's life and how it can unite a community
- To enable students to explore the similarities and differences between face-to-face and online communication, and how to write respectful messages
- To enable students to explore how to handle online situations or behaviour which may make them feel uncomfortable

Form 5 syllabus (students aged between 15 and 16 years):

- To enable students to reflect on how to avoid risky online relationships
- To enable students to identify strategies to avoid sexting, whilst enhancing positive relationships

Post-Secondary Education: the Malta College of Arts, Science and Technology (MCAST) offers Bachelor of Science courses, which relate to the use of ICT. The learning outcomes of these courses are as follows:

Courses related to Software Development:

- Utilise advanced data structures and algorithms
- Develop internet mobile technology applications
- Develop software securely
- Manage complex professional activities or projects with autonomy and responsibility

Courses related to Computer Systems and Networks:

- Apply the principles of network security and digital forensics to ensure a secure networking environment
- Administer a database with autonomy and responsibility
- Explain the inner workings of operating systems
- Design and deploy advanced LAN and WAN systems

In addition to the above, during each academic year, MCAST invites various speakers, such as the Systems Auditors and members of the Police Cyber Crime Unit, to give educational talks to MCAST students and to make them aware of cybercrime-related threats. Given the popularity of such talks, MCAST invites all its students, not just those undertaking the B.Sc. courses.

Tertiary Education: the Department of Criminology within the University of Malta's Faculty for Social Wellbeing offers study units on cybercrime. These are taught by a full-time academic, who is the former head and founder of the Police Cyber Crime Unit.

8.3 Prevention

8.3.1 National legislation/policy and other measures

In terms of legislation: Article 9(g) of the Commissioner for Children Act (Chapter 462 of the Laws of Malta) makes provision for the Commissioner for Children to 'promote the protection of children from physical or mental harm and neglect, including sexual abuse or exploitation;' and Article 11 (a) provides that 'in order to promote the welfare of children and to monitor the conditions under which children develop the Commissioner shall: provide public education and information designed to promote an understanding of the rights of children.'

Moreover, the Office of the Commissioner for Children provides ongoing education and awareness programmes/seminars, including:

- BeSmartOnline!
- Seminar on the portrayal of children in the media
- Online Safety for Children
- Digital Competence
- Internet Safety.

8.3.2 Public-Private Partnership (PPP)

The public-private partnership is based on the Memorandum of Understanding which has been signed by all the local internet service providers¹⁴.

8.4 Conclusions

- Cybercrime training is provided to practitioners dealing with cybercrime cases. In the first place, it is given to the cadets and police officers. Special cybercrime-related courses/programmes are still being developed by the University of Malta. Malta has not established any centre of excellence for that purpose.
- The Maltese Police Academy does not have a specific budget allocated to cybercrime training. Therefore, in the opinion of the evaluators, it is important that adequate resources be secured to ensure that such measures are carried out in a consistent and sustainable manner, in particular where they rely on external funding, and to extend such measures to other types of offences related to use of computer systems and the internet.
- The evaluation team was informed that courses are organised for representatives of the judiciary, and participation is voluntary. Judges are to a large extent dependent on experts' reports. Considering that any crime can involve electronic evidence, even civil cases, it has been internationally recognised for quite some time that all judges and prosecutors should have at least a basic knowledge of such topics. However, in the opinion of the evaluators, it seems that training for judges on cybercrime and electronic evidence is limited.
- In the field of child pornography and sexual abuse prevention, the police and Aġenzija Appoġġ run educational programmes and initiatives to promote the safety, welfare and well-being of children and the skills required to respond appropriately.

¹⁴ For more information, please refer to section 6.2.4.

- The police maintains a 'stop-list' to block access to websites containing child sexual abuse material. Officers assigned to the Police Cyber Crime Unit receive on-the-job training, as well as other training provided by European Law Enforcement Agencies. Moreover, the Office of the Commissioner for Children provides ongoing education and awareness programmes/seminars.
- For three years, through the 'BeSmartOnline!' project, Aġenzija Appoġġ has been giving lessons to primary school and secondary school students, with teachers invited to attend training on online safety. In the opinion of the evaluators, Malta's robust policy on the safe use of the internet and its awareness-raising campaigns targeting teens, parents, teachers, and society as a whole, should be regarded as an example of best practise.

DECLASSIFIED

9. FINAL REMARKS AND RECOMMENDATIONS

9.1 Suggestions from Malta

The Maltese authorities set forth the positive and negative aspects of the Police Cyber Crime Unit's experiences in handling cybercrime cases.

The strengths of the Cyber Crime Unit are as follows:

- Effective and efficient in its response to several high-profile cases;
- Adoption of crime prevention initiatives organised in conjunction with other local organisations and entities;
- Adoption of the 'Child Abuse Internet Filter'. Malta is one of the few states to have successfully implemented a filter to stop local internet users from accessing websites containing child abuse material;
- Good relationships with industry, academia and other stakeholders;
- Participation in several international operations that have made Malta an active participant in the fight against cross-border crime, particularly in the fight against online child abuse;
- Participation in several formal and informal networks that allow expertise to be shared and promote better international cooperation;
- Attendance at various local and international training courses and meetings.

The weaknesses of the Cyber Crime Unit are as follows:

- Not enough officers to deal with the increase in the number of cases related to cybercrime;
- Limitations in terms of the availability of equipment;
- Very limited search and seizure capabilities. It does not have the capacity to carry out on-site extraction of data from large-scale computers. This is mainly due to a lack of knowledge and equipment';
- No capacity to carry out proper computer network investigations;
- Identification of illegal material and categorisation of images/videos is still being carried out manually;
- No capacity to carry out forensic analyses of mobile phones and other handheld devices (e.g. GPS);

- Equipment seized for the collection and preservation of data is not always cloned. This is mostly due to the lack of storage space and the fact that 'loose' hard disks are still being used for this process;
- No access to the Interpol Child Sexual Exploitation (ICSE) Database.

In addition, the Maltese authorities shared their experience and views with regard to successful investigations and prosecutions, and the facilitation of international cooperation on cybercrime.

Good Prosecution Practice: All technical reports drawn up by the analysts of the Cyber Crime Unit are reviewed prior to being presented to the investigative officer or the judiciary. This ensures that all forensic analysis reports are explained in a manner which can be easily understood by a person with no technical expertise, and that all the reports contain a thorough descriptive analysis of the procedure used.

Another example of good prosecution practice in cybercrime cases is the use of visual aids during testimony. In very complicated cases, the police (prosecution) prepare and deliver presentations in order to provide a clearer picture of the investigations carried out to detect such crime. Moreover, in cases related to the possession of child sexual abuse material, the illegal material is classified using the 'Combating Paedophile Information Networks in Europe' (COPINE) scale. During the court proceedings, the police compile a report based on the material collected from the computer of the accused. The report classifies the type of material in accordance with the COPINE scale and also highlights if the children depicted in the pornographic material are under the age of nine years. This allows the judge/magistrate to have a clear overview of the type and seriousness of material found on the computer of the accused.

Good Investigation Practice: The Cyber Crime Unit ensures that its assistance is available 24/7 to all other foreign officers responsible for police investigations. Apart from international assistance, the Cyber Crime Unit provides technical advice and assistance to local police officers working within other specialised police departments. In the exercise of its duties, the CCU ensures that its assistance and advice are provided without undue delay. This has strengthened the quality of investigations, both in terms of efficiency and effectiveness.

Furthermore, the Maltese authorities emphasised that measures to enhance international cooperation are needed, so as to ensure that information retained by internet service providers located overseas is duly communicated to the police authorities making requests for information. This would make investigations more efficient, effective and less time-consuming.

9.2 Recommendations

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

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

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

9.2.1 Recommendations to Malta

1. Should be encouraged to finalise and adopt the National Cyber Security Strategy to establish the key coordination structures at strategic and operational level in order to protect national critical digital infrastructure and ensure clear delineation and communication of roles and responsibilities; (cf. 3.1 and 3.5)
2. Should set up an integrated information system on statistics to facilitate collection and management of statistical data on investigations and prosecutions, on the one hand, and on convictions relating to cybercrime, on the other, preferably collecting information for each type of offence criminalised under Directive 2013/40/EU so as to provide a complete picture of the situation in Malta to be used for strategic purposes, e.g. training strategies, methods and trends; (cf. 3.3.2 and 3.5)

3. Should enhance the capacity of the Cyber Crime Unit in terms of countering cybercrime by providing the necessary tools to ensure that any evidence collected maintains its integrity and reliability and by increasing the number of staff assigned to fulfil its tasks; (cf. 4.2, 4.4.2 and 4.5)
4. Should examine methods to increase investment in the hardware, software and human resources involved in countering cybercrime so as to raise its capacity to, inter alia, carry out proper computer network investigations, identify illegal material and categorise images, carry out forensic analysis, etc.; (cf. 4.4.2, 4.5, 9.1)
5. Should ensure full transposition of Directive 2011/93/EU on combating sexual abuse and sexual exploitation of children and child pornography; (cf. 5.1.2 and 5.5)
6. Should establish a coordinated multidisciplinary mechanism to respond to cyber attacks, including by strengthening its cooperation with the financial sector and considering making such cooperation more mandatory; (cf. 5.1.2 and 5.5)
7. Should consider analysing the range of the police's search and seizure powers to facilitate investigative work performed by the police, in full respect of human rights; (cf. 5.2.1, 5.5 and 9.1)
8. Should be encouraged to participate more actively in international initiatives which may help address some of the issues identified or to be dealt with in the future, e.g. accessing data from cloud services, direct cooperation with internet service providers abroad, facilities provided by, inter alia, Interpol, the Council of Europe (Cybercrime Convention Committee) or Eurojust; (cf. 7.1, 7.6 and 9.1)
9. Should secure adequate financial and human resources to carry out continuous training on cybercrime; (cf. 8.1 and 8.4)
10. Should continue training programmes for practitioners and strengthen its policy on cybercrime training, specifically targeting judges; (cf. 8.1 and 8.4)

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

1. It is recommended that Member States use tools to counter child abuse and child pornography online through developing tools that allow for online reporting of illegal content on the internet, such as Malta's 'BeSmartOnline!' project; (cf. 3.2, 4.4.1, 6.2.3, 6.4, 8.2 and 8.4)
2. Member States should examine methods of speeding up and enhancing the quality of responses to MLA requests; (cf. 4.1.2 and 4.5)
3. Member States should consider providing cybercrime training to practitioners also at the preparatory stage of their careers; (cf. 8.1 and 8.4)
4. It is recommended that Member States develop tools addressed to children and minors so as to present to them in a simple and friendly manner the basic rules for safe use of the internet and the threats relating thereto, such as the tool developed by the Office of the Commissioner for Children in Malta; (cf. 8.3.1 and 8.4)
5. EU institutions should address the issue of data retention; (cf. 5.2.1 and 5.5)

9.2.3 Recommendations to Eurojust/Europol/ENISA

1. Eurojust should raise awareness of the added value it can offer in providing judicial assistance in complex, cross-border cases; (cf. 7.1.2 and 7.6)

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

Date	Time	Event
15/09/2015		Arrival at MIA
		Transport from MIA to Hotel
16/09/2015	08h30	Transport from Hotel to Police Headquarters
	09h00-9h15	Welcome by MHAS/Police executives and Presentation 1 – Introduction of programme and stakeholders
	09h15 – 10h00	Presentation 2 – Economic Crime Unit and Bankers Association
	10h00 – 10h30	Coffee break
	10h30 – 11h15	Presentation 3 – Police Cybercrime Unit
	11h15 – 12h00	Presentation 4 – Police Cybercrime Unit
	12h00 – 14h00	Lunch break
	14h00 – 14h45	Presentation 5 – Vice Squad
	14h45 – 15h15	Coffee break
	15h15 – 16h00	On site visits to Specialised Police Branches and the International Relations Unit
	16h00 – 16h30	Departure back to hotel /drafting time

RESTREINT UE/EU RESTRICTED

	19h30	Dinner
17/09/2015	08h30	Transport from Hotel to the Office of the Commissioner for Children
	09h00	Welcome by Commissioner for Children
	09h15 – 10h00	Presentation 1 - BeSmartOnline! – General Overview and Past Awareness Campaigns
	10h00 – 10h30	Coffee break
	10h30 – 11h00	Presentation 2 – Maltese Internet Hotline and Helpline
	11h00 – 11h20	Presentation 3 – Advisory Board and Future Plans
	11h20 – 11h40	Presentation 4 – Internet Safety Educational Campaigns and Initiatives
	11h40 – 12:00	Q&A
	12h00 – 13h00	Lunch
	14h00 – 14h30	Tour MITA Data Centre
	14h30 – 15h00	Presentation 1 - Digital Malta
	15h00 – 15h15	Presentation 2- Article 13 of the Electronic Communications Framework Directive
	15h15 – 15h30	Presentation 3- Malta Gaming Authority against Cybercrime.
	15h 30 -	Presentation 4- National Cyber Security Strategy

RESTREINT UE/EU RESTRICTED

	16h 00	
	16h 00- 16h30	Presentation 5- CIPD (CIIP & CSIRTMalta)
	16h 30 - Onwards	Transport back to hotel and free time
	20h00	Dinner hosted by Ministry for Home Affairs and National Security
18/09/2015	08h30	Transport from Hotel to Venue
	09h00	Welcome and introductions by representative from Attorney General
	09h15 – 10h00	Meeting with representative from the Attorney General with special reference on extraditions and mutual legal assistance.
	10h00 – 10h15	Coffee break
	10h15 – 10h45	Meeting with Data Protection Commissioner
	10h45 – 11h45	Wrap-up session
	11h45 – 13h00	Lunch break and departure

Annex B: Persons interviewed/met

Meetings on 16 September 2015

Venue: the Police Headquarter

Person interviewed/met	Organisation represented
Dr. Josette Zerafa	Director Operations
Stephen Gatt	Assistant Commissioner of Police, International Relations Unit
Silvio Valetta	Assistant Commissioner of Police, Crime
Ian Joseph Abdilla	Senior Inspector of Police, Economic Crimes Unit
Mario Cuschieri	Senior Inspector of Police, International Relations Unit
Christopher Galea Scannura	Senior Inspector of Police, International Relations Unit
Denis Theuma	Senior Inspector of Police, Vice & Drugs Squad
Timothy Zammit	Inspector of Police, Cyber Crime Unit
Joseph Busuttil	Inspector of Police Vice Squad

Venue: the Police Headquarter

Person interviewed/met	Organisation represented
James Bonello	Secretary General of the Malta Bankers Association
Ivo Camilleri	Representative from the Bank of Valletta
Mark Drago	Representative from HSBC Bank
Gavin Brewes	Representative from Banif Bank
Etienne Vella	Representative from APS Bank
Steve Theuma	Representative from Global Payments
Sonia Gauci	Representative from Lombard Bank
Carmelo Ebejer	Representative form Nemea Bank

Meetings on 17 September 2015

Venue: The Office of Commissioner for Children

Person interviewed/met	Organisation represented
Helen D'Amato	Commissioner for Children
Suzanne Garcia Imbernon	Task Manager, Office of the Commissioner for Children
Ruth Sciberras	Operations Director, Foundation for Social Welfare Services
Graziella Castillo	Services Manager, Agenzija Appogg
Svetlana Buttigieg	Service Area Leader, Agenzija Appogg (Internet Hotline)

Venue: MITA Data Centre

Person interviewed/met	Organisation represented
Mark Spiteri	Malta Communications Authority (re: Be Smart Online Project)
Carl Brincat	Malta Gaming Authority
Andrew Meli	Malta Communications Authority (re: Regulatory Matters)
Antoine Sciberras	Malta Communications Authority (re: Regulatory Matters)
Mark Bartolo	Enterprise Architect, Governance, Risk and Compliance Department MITA
Rodney Naudi	Head of Department, Governance, Risk and Compliance Department MITA
Keith Cilia DeBono	Consultant, Governance, Risk and Compliance Department, MITA
Emanuel Darmanin	Head of Department, Strategy and Business Department, MITA
John Agius	Director, Head of Critical Infrastructure Protection Unit Malta
George Chetcuti	Technical analyst within the Infrastructure Protection Unit Malta

Meetings on 18 September 2015

Venue: Attorney General

Person interviewed/met	Organisation represented
Donatella Frendo Dimech	Deputy Attorney General, Attorney General's Office of Malta
Davida Flores	Director Strategy Support Ministry for Social Dialogue, Consumer Affairs, and Civil Liberties
David Cauchi	Compliance Executive Office of the Information and Data Protection Commissioner
Saviour Cachia	Commissioner for Information & Data Protection Office of the Information and Data Protection Commissioner
Ian Deguara	Director Programme implementation and Operations, Office of the Information and Data Protection Commissioner

Throughout the on-site visit the evaluation team was accompanied by:

Person interviewed/met	Organisation represented
Timothy Zammit	Inspector of Police, Cyber Crime Unit
Mario Cuschieri	Senior Inspector of Police, International Relations Unit
Kathleen Sammut	Junior Legal Officer, Ministry for Home Affairs and National Security
Annette Cassar	Principal officer, Ministry for Home affairs and National Security

Annex C: List of abbreviations/glossary of terms

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	MALTESE OR ACRONYM IN ORIGINAL LANGUAGE	MALTESE OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CIP	<i>CIP</i>		Critical Infrastructure Protection
CIRCAMP	<i>CIRCAMP</i>		COSPOL Internet Related Child Abuse Material Project
DQSE	<i>DQSE</i>		The Directorate for Quality and Services in Education
EC3	<i>EC3</i>		the European Cybercrime Centre at Europol
ECTEG	<i>ECTEG</i>		the European Computer Training and Education Group
ENISA	<i>ENISA</i>		the European Network and Information Security Agency
EUCTF	<i>EUCTF</i>		the European Union Cybercrime Task Force
ICSE	<i>ICSE</i>		INTERPOL Child Sexual Exploitation Database
ISF	<i>ISF</i>		Internal Security Fund
MCA	<i>MCA</i>		The Malta Communications Authority
MFSA	<i>MFSA</i>		Malta Financial Services Authority
MGA	<i>MGA</i>		Malta Gaming Authority
MITA	<i>MITA</i>		Malta Information Technology Agency
NRA	<i>NRA</i>		National Risk Assessment