Council of the
European Union

Brussels, 12 August 2016
(OR. en)

9955/1/16
REV 1 DCL 1

GENVAL 71
CYBER 66

DECLASSIFICATION

of document:	9955/1/16 REV 1
dated:	14 July 2016
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Italy

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, 14 July 2016
(OR. en)

9955/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 71
CYBER 66

REPORT

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

ANNEX

Table of Contents

1 EXECUTIVE SUMMARY

Italy approved its National Strategic Framework for Cyberspace Security in 2013. The key fields on which the Cyber Security Strategy focuses are ensuring vital services, combating cybercrime more effectively and advancing national defence capabilities. Additional supporting activities to fulfil these objectives include: establishing the Network and Information Security Authority (NIS), improving public-private partnerships, promoting international cooperation, bolstering the work of the national CERT, raising public understanding and awareness of cyber security.

There is a robust legal framework in place in Italy, with substantive criminal law covering the full range of offences related to cybercrime. The Penal Code is kept under review and amended as new trends emerge. Italy has implemented the Freezing Order Framework Decision, the Framework Decision on attacks against information systems and the Confiscation Order and the Directive on combating sexual abuse and sexual exploitation of children and child pornography. Italy is party to the Budapest Convention but has not ratified the Mutual Legal Assistance Convention 2000. Instead, it relies on the 1959 MLA Convention, Schengen Agreement, Interpol and diplomatic channels for the purpose of mutual legal assistance.

Implementation of the law enforcement aspects of the Strategy falls to the Ministry of the Interior who has responsibility for the police including the specialised police branches such as Polizia Postale e delle Comunicazioni (Postal and Communication Police). Within this branch lies the National Anti-Cybercrime Centre for the Protection of Critical Infrastructure (C.N.A.I.P.I.C.) and the National Centre for the Fight against Online Child Pornography (CNCPO).

The Postal and Communication Police has substantial powers and investigative techniques at its disposal to investigate cyber offences and deal with e-evidence and encryption. E-evidence is considered admissible if acquired according to the best practices on digital forensics, which are broadly established in accordance with the Council of Europe Convention on Cybercrime.

There is no obligation for private sector enterprises providing critical services to report cyber attacks and security incidents to the Italian authorities although the Strategy provides for the sharing of information between public and private operators and the CNAIPIC. On the prevention of child sexual exploitation, Italy blocks access to websites containing child pornography by providing black lists of sites regularly to ISPs.

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

Italy provides awareness-raising and prevention programmes to inform the public and industry about the risks of cybercrime and encourage the safe use of the internet. In particular the campaigns and road shows organised by the Postal and Communications Police are considered wide reaching and effective.

On the whole, the evaluators could conclude that Italy is committed to tackling cybercrime and has taken a series of measures to meet this objective. The team was very impressed by the number of key initiatives in place and considers that many of those could serve as models of good practice and could be used by other Member States to bolster their own efforts to tackle cybercrime. In particular, the on-line police station, the comprehensive public awareness campaigns and the blocking of illegal websites are worthy of mention.

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

2 INTRODUCTION

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

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

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

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

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

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

[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 January2003, entered into force on 1 March 2006.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. Italy was the 10th Member State to be evaluated during this round of evaluations. In accordance with Article 3 of the Joint Action, a list of experts in the evaluations to be carried out has been drawn up by the Presidency. Member States have nominated experts with substantial practical knowledge in the field pursuant to a written request on 28 January 2014 to delegations made by the Chairman of GENVAL.

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

The experts charged with undertaking the evaluation of Italy were Mr Gilles Herrmann (Luxembourg), Mr Matthew Roach (United Kingdom) and Mr Savin Svet (Slovenia). Three observers were also present: Mr Hari Tiesmaa (Eurojust), Ms Sara Marcolla (Europol/EC3) and Mr Michele Socco (European Commission), together with Ms Nicola Murphy and Mr Steven Cras from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Italy between the 26th and 28th of May 2015, and on Italy's detailed replies to the evaluation questionnaire together with their detailed answers to ensuing follow-up questions.

3 GENERAL MATTERS AND STRUCTURES

3.1 National cyber security strategy

Italy's national cyber security strategy is contained in the "National Strategic Framework for Cyber Space Security"[7] which was adopted by the Presidency of the Council of Ministers in December 2013.

The fight against cybercrime is one of the actions set out in the Plan which envisages that each government department establish structures and procedures in order to prevent and counter cyber attacks. In this context, the Ministry of the Interior is the lead Ministry in terms of overseeing the role of law enforcement and specialised police branches such as the Italian Polizia Postale e delle Comunicazioni (Postal and Communications Police Service).

The Strategy includes six strategic guidelines, which are further developed by eleven operational guidelines.

3.2 National priorities with regard to cybercrime

The National Plan foresees the establishment of an integrated information exchange system through public-private partnerships to involve technical structures (CERTs), military structures (CERT DIFESA) and law enforcement structures with regard to capacity building and training. The Italian Government has prioritised the setting up of structures that facilitate information sharing and the mutual exchange between the academic world, industry and the public administration. Overall, the national priorities are in line with the EU provisions on the fight against cybercrime.

[7] http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/piano-nazionale-cyber_0.pdf

Under section 7 bis of Act No 155 on "Urgent measures to fight against international terrorism", the Postal and Communications Police - in their capacity as a body of the Ministry of the Interior responsible for the security and regularity of telecommunications services - was given exclusive competence for the provision of critical infrastructure protection services. This is to be achieved through ICT links established in ad hoc agreements with the managers of the structures concerned.
For the purpose of implementing the provisions under the a.m. section 7 bis the Minister of the Interior issued a decree on 9 January 2008 envisaging the setting up of the National Anti-Cybercrime Centre for the Protection of Critical Infrastructure (C.N.A.I.P.I.C.). The Centre was established within the Postal and Communications Police Service by a decree issued by the Chief of Police (Director General of Public Security) on 7 August 2008[8]. It is an analysis and investigative coordination structure and cooperates with other institutions, the intelligence and military sectors and the national CERT.

3.3 Statistics on cybercrime

3.3.1 Main trends leading to cybercrime

The Criminal Analysis Service of the Criminal Police Central Directorate examines the crimes under sections 615, 617, 623bis, 635 and 640 of the Italian Criminal Code. In terms of emerging trends, Italy has found that more and more sophisticated cyber attacks are increasingly conducted against critical infrastructures, government sites, the economic and banking sectors, along with cyber terrorism attacks perpetrated, in particular, by Jihadists.

[8] The DPCM 24 January 2013 outlined the institutional architecture for the protection of cyber and national security, entrusted to the National CERT the support function to the NISP - Core Interministerial Situation and Planning, acting as a centre for the national inter-ministerial cyber coordination. www.certnazionale.ie

Statistics indicate that the number of perpetrated crimes increased by about 50% between 2012 and 2013 and in 2014 the number of cases settled amounted to just over 34,000, which was a slight decrease on previous years. Also the number of persons reported for cybercrime offences in 2013 increased by about 15% compared to the number registered in 2012, and amounted to more than 4,500 individuals.[1. The data should be completed by the data on violations of section Article 600 of the Criminal Code, section 130 of the Privacy Code, as well as violations under Legislative Decree No 64 of 11.04.2011 (identity theft), where available. 2. The percentage of cybercrimes out of the total number of perpetrated crimes should be indicated, and a distinction should be made between the reported and the arrested persons].

3.3.2 Number of registered cases of cyber criminality

The only statistics recorded relate to crimes reported to the law enforcement authorities. The Postal and Communications Police draw up statistics on the institutional activities carried out all over the national territory.

The table below contains statistics on the number of the persons reported to the judicial authorities and the crimes for which they were reported.

Description of the crime	2012		2013		2014	
	Perp. crimes	Arr. Persons	Perp. crimes	Arr. Persons	Perp. Crimes	Arr. persons
Unauthorised access to computer/ICT system	6310	1097	8051	889	9490	893
Illegal possession/circulation of access codes to ICT systems	700	253	1105	197	800	254
Circulation of programmes aimed at damaging or disrupting a computer system	59	29	63	30	80	35
Forgery/alteration or deletion of the content of communication	19	4	22	14	30	9
Illegal interception, hindering or interruption of computer/ICT communications	154	134	257	175	229	74
Installation of devises to intercept/hinder or interrupt computer/ICT	269	254	251	329	170	149
Forgery alteration or disruption of the content of electronic communications	142	18	150	22	153	30
Other communications and conversations	37	14	28	10	38	19
Damage to ICT/Computer systems	277	49	202	39	180	49
Computer fraud	17669	2088	29089	2835	22936	2936
Damage to computer or ICT systems	136	34	136	64	92	35

Damage to computer or ICT systems	128	29	146	20	132	14
Damage to computer information, data and programs used by the State	89	47	86	56	96	52

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

Dedicated budget allocations are envisaged for the fight against on line child sexual exploitation and for the protection of the critical infrastructure. The funds are allocated directly to the Postal and Communications Police.

The National Strategy sets out that adequate resources be allocated to the public administration directly responsible for fulfilling the objectives therein.

In addition several projects such as the current project to improve picture analysis for combatting online child sexual exploitation and projects designed to work with victims of these crimes are partly funded by the EU.

3.5 Conclusions

- It was obvious to the evaluators that Italy takes cyber security seriously and the team welcomed the Strategy, which sets out national priorities in this regard. The team noted, however, that the Strategy does not clearly identify particular tasks or targets for stakeholders so each stakeholders' role is not clear. This could result in a duplication of resources, which could be avoided if the functions of each stakeholder were specified within the national framework. [9]

- Similarly, there was no specific budget allocated to the implementation of the Strategy or an estimated cost of its implementation[10]. The team could see some value in the creation of an action plan which identifies specific actions for each stakeholder involved in cyber security and combatting cybercrime together with accompanying budgetary estimates. The team also considered that existing investment should be kept under review to take account of global trends in cybercrime and adjusted to respond to any increased threat.

- Italy records and maintains statistics on cybercrime although it was not clear how comprehensive the statistics are and how trends are monitored and mapped. Indeed the figures provided could suggest under-reporting of cybercrime which needs to be considered when targeting resources under the National Strategy. That being said, it was clear that the Italian authorities were mindful of the new emerging threats and actively respond to emerging threats through targeted action or by way of introduction of new legislation.

[9] Subsequently to the evaluation visit, Italy informed the team on the evaluation of the first schedule of the National Strategic Framework and the National Strategic Plan on cyber security (which both have a two-year's duration). The first exercise was concluded on the last December 2015, which according to the Italian authorities has led to an undeniable progress in relation to the actions performed by Italy in the overall response to the cyber threat and implementation of an effective and resilient national system. The next schedule will take into account the outcome of the planned actions, according also to the upshot of the internal audits, which already provide for specific targets and a measurement system for assessing the activities carried out by the competent Departments.

[10] Further to the evaluation visit, the Italian authorities informed the team that a new law was adopted (Legge 208 of 28 December 2015), which provides a specific budget for cyber security with a total amount of 150 million euros at national level. 10% of this amount will be allocated to the Postal and Communications Police.

- In addition, the team found that there are significant discrepancies on statistical figures when comparing between the Police with the Prosecution Office material. The team recognised that some discrepancy could be expected given the existence of different databases among several entities, managed by different criteria, namely, in terms of the fields set into use.

4 NATIONAL STRUCTURES

4.1 Judiciary (prosecution and courts)

4.1.1 Internal structure

Common cybercrime cases are dealt with by ordinary judges, i.e. prosecutors and judges. Judges may be selected from the judicial pool on account of specific experience and training to work on computer and ICT cases.

There are some prosecutors that are formally designated as specialised prosecutors in the field of cybercrime. It should be pointed out that jurisdiction in these matters is not conferred on prosecution offices attached to the courts of first instance (140), as it happens in relation to most of the offences, but to district prosecution offices (29) (see Article 51(3) quinquies of the code of criminal procedure)", it should be pointed out that jurisdiction in these matters is not conferred on prosecution offices attached to the courts of first instance (140), as it happens in relation to most of the offences, but to district prosecution offices (29) (see Article 51(3) quinquies of the code of criminal procedure). The conferral of jurisdiction regarding cybercrimes on the Offices of the Public Prosecutor attached to the Court of the district chief town and the resulting concentration of the investigations, which are assigned to a small number of prosecutors, enables the latter, as a matter of fact, to acquire a high degree of specialization.

4.1.2 Capacity and obstacles for successful prosecution

Capacity

Italy boasts a robust legislative framework on cybercrime, which is kept under review to deal with emerging trends and threats. For example, currently, a bill containing “Provisions to prevent and counter bullyism and cyber bullyism” is under consideration by Parliament.

- Additionally a recently enacted Counter-terrorism Decree Law No 7 of 2015, amended and turned into Act No 43 of 17 April 2015 (Official Journal No 91 of 20 April 2015) updated the tools to counter the use of the Internet for purposes of proselytism and aiding and abetting of terrorist groups. In particular, the following provisions are included:

  i) aggravation of the penalties established for the instigation to commit a crime and instigation to terrorism perpetrated by means of ICT tools;

  ii) the possibility for the judicial authorities to order internet providers to block access to the sites used to commit crimes for purposes of terrorism that are included in the list which is regularly updated by the Postal and Communications Police Service of the Italian National Police. In case of failure to comply with said order the judicial authorities will prohibit access to the relevant Internet sites.

- Ratification and implementation of the Protocol on Cyber Crime (bill). On 27 March 2015, the Italian Council of Ministers approved a bill for the ratification and implementation of the "Additional Protocol to the Council of Europe Convention on Cybercrime, concerning the criminalisation of racist and xenophobic acts that are committed by means of computer systems".

Obstacles

Italy considers that the main obstacle to effectively combatting cybercrime is the difficulty to obtain information quickly from foreign servers (in particular the US Google, Microsoft, Yahoo and Facebook). It finds that even when obtained, the data can be limited and, therefore, often useless for investigation purposes, as their retention period (by the mentioned providers) is a maximum of 90 days.

4.2 Law enforcement authorities

Postal and Communications Police

The Postal and Communications Police, in their capacity as a special branch of the Italian National Police in the prevention of and fight against cybercrime, ensures the constitutional values of secrecy of correspondence and freedom of any form of communication. The Postal and Communications Police is present nationwide with 20 regional districts and 81 provincial units coordinated at central level by the Communications Police Service. Therefore, the Postal and Communications Police Service is the body tasked by law with the fight against criminal phenomena, such as on-line child sexual exploitation and the protection of the critical infrastructure. The Service carries out the a.m. activities and the other investigations into cybercrimes at central level and by coordinating the Postal Police districts and units throughout the national territory.

The contact point for the technical-operational emergencies linked to transnational cybercrime as provided for under the Budapest Cybercrime Convention sits within the Postal and Communications Police Service.

The contact point works on a 24/7 basis within the High Tech Crime Network set up in the framework of the G8 and subsequently extended to the Council of Europe. It is located in the National Anti-Cybercrime Centre for the Protection of Critical Infrastructure (C.N.A.I.P.I.C.). The primary goal of the network is to respond rapidly to requests of data freezing pending the relevant formalisation through letters rogatory or MLAT.

The contact point also acts as the National Central Reference Point (NCRPs) in the framework of the Interpol channels when dealing with round-the-clock operational contact point for urgent requests.

On-Line Police Station

The on-line police station was launched in 2006 with the primary objective to provide a better service to the public. It was the first such station set up in the EU and was awarded an "E-gov" prize in 2007 as most inspiring good practice in Europe. The station operates on a 24/7 basis.

The station receives about 100-200 reports per day of which 30-35 are during the night shift. There are two ways of reporting - as a witness or as a victim. Users must register to report crime and use the service but some immediate information is available on the home page. As a consequence, reports can be made online in the first instance and followed up with a formal report at a police station up to 48 hr later. At the moment consideration is being given to using electronic signature when reporting so the follow up report will be unnecessary.

Reports of cybercrime are forwarded to the CNAIPIC and the Child Pornography unit of the Postal and Communication Police as appropriate.

4.3 Other authorities/institutions/Public Private Partnership

Coordination is organised between the National CERT, the CERT *Difesa* and the Public Administration in the context of the National Strategic Framework DCPM (Decree of the President of the Council of Ministers) of 27 January 2014.

Under the National Strategic Framework for cyberspace security, a central role for public-private partnership is defined. In particular public and private operators providing communication networks and services to the public are required to;

- communicate to the cybersecurity unit every significant security and integrity violation of their own computer systems;
- adopt all best practices and measures necessary to pursue cybersecurity;
- share information with the agencies for intelligence and security and allow access to databases that are relevant to cyber security;
- collaborate to the management of a cyber crisis by restoring the functionality of the networks and systems they operate.

The public private partnerships are therefore considered as an essential component for ensuring the success of the strategy. The cooperation has been ensured through ad hoc agreements with the aim to substantiate even further the cooperation in this context. In light of further progress, the strategy encourages that synergies with the private sector should be extended so as to include all entities that, regardless of size, are of strategic value for the scientific, technological, industrial and economic progress of the country.

One project worth mentioning is the OF2CEN project, a platform which brings together banks and police and renders anonym the data as suspicious transactions are communicated by banks to the police through a secure channel. It became fully operation in 2013 after a pilot phase with 15 banks. There are also MOUs with banks and critical infrastructures, financial services and the ABI (Association of Italian banks).

4.4.Cooperation and coordination at national level

This cooperation is outlined in the National Strategic Framework for cyber space security[11].

[11] http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf

4.4.1 Legal or policy obligations

4.4.2 Resources allocated to improve cooperation

There is no dedicated funding provided under the National Strategic Framework for Cyberspace Security but Operational Guideline no 10 'Resources' focuses on the measurement of costs associated with cyber events and the consideration of recruitment of specialised personnel. Resources to implement the Strategy are found through the normal public administration budgets.

4.5 Conclusions

- The evaluation team was happy to note that the conferral of jurisdiction regarding cybercrimes on the offices of the public prosecutor attached to the Court of the district chief town and the resulting concentration of the investigations, which are assigned to a small number of prosecutors, enables the latter, in practice, to acquire a high degree of specialization.

- Based on the Police structure and organisation, training officers for action as "first responders" when facing Cybercrime investigations, along with participation on cyber-exercises at a national level should be extended to specific officers at Police District level, thus creating one stronger centre of competencies for cybercrime investigations and extended forensic availability and support. Regional competencies empowerment would follow in good time.

- In addition, the team suggests that in future the Cybercrime Unit participates with CERT in European Cyber exercises, in order to create routines, awareness, identify weaknesses and establish good practices.

- The team was satisfied that there is a clear understanding of the role the Postal and Communication Police undertake to deal with cybercrime. Within the service there appears to be a clear distinction of the roles and responsibilities of the various units.

- The team welcomed the on-line police centre which it considered innovative, user friendly and of great assistance in the fight of on-line crime making law enforcement more effective and support more accessible to the public. The team welcomed the plans to introduce electronic signature in the future.

- The OF2CEN project was also considered useful by the team, which encourages Italy to consider its roll-out and expansion to more private sector financial institutions to improve its effectiveness and reach.

- The team was pleased to note that the Strategy makes specific provision for the promotion of public-private partnership, however, with the exception of the OF2CEN project, the team was not convinced that this partnership is operating to the extent envisaged by the Strategy and therefore encourage further work in this regard.

5 LEGAL ASPECTS

5.1 Substantive criminal law pertaining to cybercrime

5.1.1 Council of Europe Convention on cybercrime

Italy is party to the CoE Convention on Cybercrime, and has amended its legislation to give affect to it.

5.1.2 Description of national legislation

The Italian Criminal Code provides the following rules on cyber offences:

1. Unauthorised access to computer/ICT systems (Section 615 ter of the Criminal Code)

The code foresees a three year penalty for unauthorised entry into a computer or ICT system protected by security measures or retention of access thereto against the expressed or implied will of those who have the right to exclude him.

The imprisonment shall be from one to five years if:

1) the act is committed: *i)* by a public official or an officer of a public service through abuse of power or through violation of the duties concerning the function or the service; *ii)* by whoever practices - even without a licence - the profession of a private investigator or *iii)* with abuse of the capacity of a system operator;
2) the perpetrator uses violence against goods or persons to commit the act or if he is manifestly armed;
3) the act causes destruction of/damage to the system, total or partial discontinuation of service, or destruction of /damage to the data, information and programs contained in it;

If the acts under subsections 1 and 2 are committed against computer or ICT systems of military interest or concerning public order, public security, health, civil defence or public interest, the penalty shall be imprisonment from one to five years and from three to eight years, respectively.

If the case falls under subsection 1 the crime shall be punished upon complaint filed by the injured party; the other cases shall be prosecuted *ex officio*.

2. Damage to computer or ICT systems (Section 635 quarter of the Criminal Code)

The entry/transmission of data, information and programs destroys, damages or renders, in whole or in part, other people's computer or ICT systems useless or seriously hinders their operation shall be punished with imprisonment from one to five years.

3. Damage to computer or ICT systems or interruption (Section 635 quinquies of the Criminal Code)

If the act under section 635 quarter is aimed at destroying, damaging, rendering - in whole or in part- computer/ICT systems of public utility useless or at seriously hindering their operation, the penalty shall be imprisonment from one to four years. If the act causes destruction of/damage to the computer/ICT system of public utility or if the system is rendered, in whole or in part, useless, the penalty shall be imprisonment from three to eight years.

4. Damage to information, computer data and programs - Section 635 bis of the Criminal Code

The destruction, damages, deletion, alteration or cancelation of other people's information, computer data or programs shall be punished, upon a complaint filed by the injured party, with imprisonment from six months to three years. If the act is committed with abuse of the capacity of a system operator, the penalty shall be imprisonment from one to four years and the case shall be prosecuted *ex officio*.

5. Damage to information, computer data and programs used by the State or other public body or of public utility (Section 635 ter of the Criminal Code)

The destruction, damage, deletion, alteration or cancellation of information, computer data or programs used by the State or other public body or pertaining thereto or to a public utility shall be punished with imprisonment from three to eight years. If the act is committed with abuse of the capacity of a system operator, the penalty shall be increased.

6. Interception, hindering or unauthorised interruption of computer or ICT communications (Section 617 quater of the Criminal Code)

The fraudulent communication in a computer or ICT system or communications across multiple systems, hinders or interrupts them shall be punished with imprisonment from six months to four years. The same penalty shall apply to whoever discloses to the public, in whole or in part, through any information means the content of the communications.

The crimes under subsections 1 and 2 shall be punished upon a complaint filed by the injured party. However, the case shall be prosecuted *ex officio* and the penalty shall be imprisonment from one to five years if the act is committed:

1) against a computer or ICT system used by the State or other public body or by companies providing public services/utilities;
2) by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service or with abuse of the capacity of a system operator;
3) by anyone who practices - even without a licence - the profession of a private investigator.

7. Circulation of computer equipment, devices or programs aimed at damaging or interrupting a computer/ICT system - Section 615 quinquies of the Criminal Code

A person who obtains, produces, copies, imports, circulates, communicates, delivers or in any way makes available to others computer equipment, devices or programs in order to damage a computer/ICT system, the information, data or programs contained therein or pertinent thereto or to facilitate total or partial interruption or alteration of its operation shall be punished with imprisonment not exceeding two years and a fine not exceeding € 10,329.

8. Installation of equipment designed to intercept, hinder or interrupt computer or ICT communications (Section 617 quinquies of the Criminal Code)

The installation of equipment designed to intercept, hinder or interrupt communications concerning a computer or ICT system or communications across multiple systems shall be punished with imprisonment from one to four years. The penalty shall be imprisonment from one to five years in the cases envisaged by section 617-quater, subsection four.

9. Unauthorised possession and distribution of computer or ICT systems' access codes (Section 615 quater of the Criminal Code)

A person who, in order to obtain personal profit or profit for others or to cause damage to others, illegally obtains, reproduces, distributes, communicates or delivers codes, keywords or other methods suitable to access a computer or ICT system protected by security measures, or provides information or instructions for such purposes shall be punished with imprisonment up to one year and a fine not exceeding €5,164. The penalty shall be imprisonment from one to two years and a fine from €5,164 to €10,329 if any of the circumstances under sec. 617-quarter, subs. 4, (1) and 2) apply.

10. Virtual currency

The team was advised that no provision in Italian legislation is made for dealing with virtual currency.

The Italian authorities confirmed that domestic law does not contain specific legal provisions regarding virtual currency, but they observed that this apparent gap is filled by the possibility of extending, by way of interpretation, the operation of the measures provided for by the code of criminal procedure. They referred in this context to Article 253 of the code of criminal procedure, which provides for the possibility of carrying out the seizure of the *corpus delicti* and of the physical items related to the offence necessary for establishing the facts of the case. The second paragraph of this Article specifies that *"the* corpus delicti *consists of anything on which or through which the offence has been committed, as well as the things that constitute its product, profit or price"*. Moreover, Article 321 of the code of criminal procedure provides for the possibility of ordering the preventive seizure of those objects for which confiscation is allowed, as well as of the physical items related to the offence, if there is a danger that the free availability thereof could aggravate or extend the consequences of the offence or facilitate the commission of other offences. According to the Italian authorities, where virtual currency is the product, profit or price of an offence, or in any case is relevant thereto, there would not be any obstacle to applying restrictive measures on it, nor to admitting it in criminal proceedings.

The Italian authorities acknowledged, on the contrary, that there are no substantive rules dealing specifically with *bit coins* or similar tools, and this gap cannot be filled by applying by analogy the provisions on counterfeiting of money, spending and introducing into the State of counterfeited money, due to the explicit prohibition against application by analogy in criminal matters. In any case, the necessity to extend the operation of these provisions would be difficult to envisage, since they are clearly aimed at protecting the public faith and concern national or foreign coins having the status of legal tender.

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

The European Parliament and Council Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA was included in the Bill "Delegated Act for the Government to transpose the European directives and to implement other EU acts – European Delegation Act 2014" (A.S. 1758, p. 66, point 4).

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

Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography was transposed by Legislative Decree No 39 of 4 March 2014.

- Acts regarding the contents, in particular on line child sexual abuse and child-pornography

1. Child pornography (Section 600 ter)

Whoever,

1) using minors under 18 years of age, produces pornographic exhibitions or shows or pornographic material;
2) recruits or persuades minors under 18 years of age to participate in pornographic exhibitions or shows or otherwise makes a profit from said shows;

shall be punished with imprisonment from six to twelve years and a fine from €24,000 to €240,000. The same penalty shall apply to any person who trades in the pornographic material.

- The distribution, divulgence, circulation or publication by any means, also via ICT, the pornographic material, or distribution or divulgence of news or information aimed at enticing or sexually exploiting minors under eighteen shall be punished with imprisonment from one to five years and a fine from €24,000 to €240,000.

- The sale or transfer to others, also free of charge, of the pornographic material, shall be punished with imprisonment up to three years and a fine from €1,549 to €5,164.

- A person who attends pornographic exhibitions or shows where minors under eighteen are involved shall be punished with imprisonment not exceeding three years and a fine from €1,500 to €6,000.

For the purposes of the legislation, child pornography means a depiction, by any means, of a minor under eighteen who is involved in explicit, either real or simulated, sexual activities or any depiction for sexual purposes of the sexual organs of a minor under eighteen.

2. Possession of pornographic material (Section 600-quater of the Criminal Code)

A person who knowingly obtains or possesses pornographic material produced using minors under eighteen shall be punished with imprisonment not exceeding three years and a fine not less than €1,549. The penalty shall be increased by no more than two thirds if a considerable quantity of material in involved.

3. Virtual pornography (Section 600 quater.1)

(1) The provisions under sections 600 *ter* and 600 *quater* shall apply also when the pornographic material depicts virtual images produced using pictures of minors under eighteen or parts of said pictures. In this case the penalty shall be decreased by one third.

Virtual images are meant as pictures, produced by means of graphic processing techniques, that are not associated or are partly associated to real situations, and whose quality makes unreal situations appear as real.

C/ Online Card fraud

- **Acts in which computer/information systems are a tool or target, in particular online card frauds**

1. Computer frauds (Section 640-ter of the Criminal Code)

The alteration by any means of the operation of a computer or ICT system or unduly interfering by any means with the data, information or programs contained therein or pertinent thereto, to obtain a personal profit or profit for others or cause damage to others, shall be punished with imprisonment from six months to three years and a fine from €51 to €1,032. The penalty shall be imprisonment from one to five years and a fine from €309 to €1,549 if any of the circumstances under section 640, subs. 2, 1) apply or if the act is committed with abuse of the capacity of a system operator. The penalty shall be imprisonment from two to six years and a fine from €600 to €3,000 if the fact is committed by means of theft or undue use of digital identity to the detriment of one or more individuals.

The crime shall be punishable on complaint of the injured party, unless any of the circumstances under subsection two or any other aggravating circumstance apply.

2. Computer fraud by a person who provides services of digital signature certification (Section 640-quinquies)

Any person who provides services of digital signature certification who, in order to obtain a personal profit or profit for others or cause damage to others, violates the obligations established by law for issuing a qualified certificate shall be punished with imprisonment not exceeding three years and a fine from €51 to €1,032.

With regard to instigation to, aiding and abetting and participation in cyber crime the following general rules shall apply:

- **Participation:** When more than one person participates in the same crime, the penalty established for this crime shall apply to all of them without prejudice to the provisions contained in the following sections.

- **Instigation:** If the crime is committed, instigation is equivalent to participation. Under the Italian legislation instigation without the perpetration of the crime shall not be punished.

- **Personal aiding and abetting:** Any person who, after the commission of a crime for which life sentence or imprisonment is established by law - without prejudice to the participation in said crime - aids another person to elude the authorities' investigations, including those conducted by the bodies of the International Criminal Court, or to escape their searches shall be punished with imprisonment not exceeding four years.

- When the crime committed falls under section 416 *bis*, the penalty of imprisonment of not less than two years shall apply.
- In case of crimes for which the law establishes a different penalty or in case of infringements the penalty shall be a fine not exceeding €516.
- The provisions under this section shall apply also when the person so aided cannot be charged with the crime or is found not to have committed it.

- **Aiding and abetting:** A person who aids another person to ensure the product, profit or price of a crime shall be punished with imprisonment not exceeding five years in case of a crime and with a fine from €51 to €1,032 in case of infringement.

- **Attempt:** Any person who commits acts unequivocally aimed at perpetrating an offence is responsible for attempting to commit a crime if the action is not fulfilled or the event does not occur. The perpetrator of the attempted crime shall be punished with imprisonment of not less than 12 years if the penalty established is life imprisonment and, in the other cases, with the penalty established for that crime and decreased by one to two thirds.

    - If the offender desists from the action voluntarily he shall be subject only to the penalty envisaged for the acts already committed if they constitute in themselves a different offence.
    - If they voluntarily hinder the event, the penalty established for the attempt to commit a crime shall apply, decreased by one third up to a half.

5.2 Procedural issues

- Search and seizure of information system/computer data is permissible, as provided for in sections 254 - 254bis - 352 and 354 of the Criminal Procedure Code as amended by the Council of Europe Convention on Cybercrime.

- Real-time interception/collection of traffic/content data is permissible, as provided for in section 266 bis of the Criminal Procedure Code.

- Preservation of computer data is provided for in section 132 of the privacy legislation.

- Order for stored traffic/content data and for user information is provided for in section 132 of the privacy legislation.

- Access to computer data, content data, traffic data, order for search/seizure of information system, networks managed or controlled by suspects of cybercrime is provided for in the Frattini Decree.[12]

5.2.1 Investigative Techniques

Computer equipment (hardware and software) may be seized during operations. This equipment is acquired through systems that do not alter the evidence and allow for its forensic copy. If these operations cannot be repeated for technical reasons a cross-examination of the parties involved is conducted. The subsequent analysis is aimed at searching for e-evidence that is reported and transmitted to the investigating bodies together with the relevant forensic copies.

[12] http://www.interlex.it/testi/dlg08_109.htm

Special investigative techniques such as interceptions, undercover activities and OSINT searches can be used for the purpose of cybercrime investigation. Law enforcement authorities can also make use of malware but its use has to be approved by investigative magistrate and not all allow it. The team was informed that national guidelines exist but magistrates retain ultimate discretion so the guidelines are not implemented evenly nationwide. Evidence gained from malware/legal intrusion can be used in court if there was court order to sanction its use. The team was also advised that the Postal and Communication Police sought a provision in the ability to create a police Trojan if necessary but this suggestion was not taken on board so law enforcement officers will continue to rely on more traditional investigation methods.

5.2.2 Forensic and Encryption

Italy is also able to use special tools to decrypt encrypted files (e.g., zip and office); encrypted containers (pgp, drivecrypt, truecrypt) and full disk encryption. There are no institutional forensic centres in Italy, however, there are specialised private centres that are used exclusively for data recovery on damaged supports/devices. In Italy there are no companies decrypting data on behalf of the law enforcement authorities.

The authorities involved cooperate with each other by use of agreements with EU countries, G8 countries and on bilateral agreements with non-EU countries.

5.2.3 E - e v i d e n c e

In Italy, e-evidence is considered admissible if acquired according to the best practices on digital forensics, which are broadly established in the Council of Europe Convention on Cybercrime. The same admissibility criteria apply if e-evidence is acquired outside the Italian State through cooperation with Member states or through international MLA.

5.3 Protection of Human Rights/Fundamental Freedoms

In general fundamental rights and freedoms are protected by constitutional law (articles 2, 3,13,15,19,21 and 33 of the Italian Constitution) and primary law. With reference to the protection of privacy and personal data Legislative-Decree No 196 of 30 June 2003 (The Italian Personal Data Protection Code) ensures that personal data are processed in compliance with the fundamental rights and freedoms and with the dignity of the individual concerned, with particular reference to data confidentiality, personal identity and the right to personal data protection.

The Code also contains provisions covering, in particular, data processing with the support of computer systems. These provisions envisage the adoption of specific minimum security standards to protect these systems (section 34). Moreover, the signing of codes of ethics and conduct with regard to personal data processing performed by providers of communication and information services through electronic communication networks is promoted by the Italian Data Protection Authority (section 133).

5.4 Jurisdiction

5.4.1 Principles applied to investigate cybercrime

All crimes (not only cyber crimes) also partially committed outside the Italian territory are considered as entirely committed on the Italian territory for the purposes of enforcing the Italian criminal law.

Section 6 of the Criminal Code states that any person who commits a crime within the State territory shall be punished under the Italian law. The crime shall be considered as committed on the State territory when the action or omission constituting it totally/partially occurred there, or the event that was a consequence of the action/omission took place there.

For all crimes (not only cybercrimes) committed outside the State territory the Italian law shall apply if:

a) they are crimes against the Italian State;

b) it is envisaged by the international conventions;

c) other minor cases.

Section 7 of the Criminal Code provides that an Italian or foreign national who commits any of the below listed crimes on a foreign territory shall be punished under the Italian law:

1) crimes against the personality of the Italian State;
2) forgery of the State seal and its use
3) counterfeiting of currency having legal tender on the State territory, or of other public valuables and securities;
4) crimes committed by public officials through abuse of power or through violation of the duties concerning their functions;
5) any other crime for which special law provisions or international conventions establish that the Italian criminal law shall apply.

With the exception of the a.m. cases, the punishability of crimes committed abroad shall be dependent on:

a) the severity of the crime and the relating sanction;
b) the presence of the offender in Italy;
c) the request of the Minister of Justice.

In addition, Section 8 of the Criminal Code states that an Italian or foreign national who in a foreign territory commits a political crime which is not included in those mentioned under point 1) of Section 7 shall be punished under the Italian law, on request of the Minister of Justice.

If it is a crime that is punishable upon complaint of the injured party, the complaint shall be also necessary in addition to the a.m. request.

For the purposes of the criminal law, a political crime shall be any offence against a political interest of the State or a political interest of a citizen. A common offence which is totally or partly caused by political reasons shall be also considered a political crime.

Section 9 of the Criminal Code provides that an Italian national who in a foreign territory commits a crime which the Italian law punishes with a life sentence or imprisonment not less than three years as a minimum, shall be punished under the Italian law, provided that he is on the territory of the State. If it is a crime for which restriction of personal liberty is envisaged for a lesser period, the offender shall be punished on request of the Minister of Justice or on petition or complaint of the injured party.

Section 10 of the Criminal Code provides that a foreign national who in a foreign territory commits a crime against the Italian State/Italian national that under the Italian law who is punished with a life sentence or imprisonment for not less than one year as a minimum, he shall be punished under the same law, provided that he is on the territory of the State and a request of the Minister of Justice or petition or complaint of the injured party were submitted.

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

In Italy the compulsory prosecution principle is in force as Article 112 of the Italian Constitution provides that the Public Prosecutor has the obligation to institute criminal proceedings.

For this reason, if conditions for the application of the Italian law are met, the Judicial Authority institutes criminal proceedings even if a similar investigation is under way in other States. The only exception to the exercise of the criminal action is if the case is at final sentence or acquitted for the same facts in another State adhering to the Schengen Agreements (article 54).

At the time of the evaluation visit, Italy had not yet implemented Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings. However, after the evaluation visit, Italy informed the team that Framework Decision 2009/948/JHA has now been implemented in the Italian legal order by Legislative Decree No. 29 of 15 February 2016, which entered into force on 22 March 2016. In particular, Article 10 of this Decree provides that, in case of agreement on concentration of the proceedings in another Member State, the court shall make a declaration that proceedings may no longer be pursued. According to Italy, this provision resolves the problem owing to the principle of mandatory prosecution and to the absence of a specific provision enabling to resolve cases of conflicts of jurisdictions.

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

No judgment of the Court of Cessation is known on the issue, however, by virtue of the Italian law on jurisdiction (section 6 of the Criminal Code) if illicit electronic files in the cloud (for instance, a child-pornography image) are visible from a computer in Italy, Italian jurisdiction shall apply with the possibility to intervene by means of letters rogatory, it may also request the deletion of the illicit file when it is physically allocated in servers in foreign territories.

5.5 Conclusions

- The substantive criminal law is comprehensive and flexible. Italy provides for a range of offences and covers attempt, participation, aiding and abetting, negligence and legal liability.

- The Postal and Communication Police has substantial powers of investigation and tools at its disposal. The team was satisfied that fundamental rights are respected in Italy and appropriate judicial oversight is applied to any surveillance or special investigation technique. The team noted, however, that the use of some specialised surveillance is limited due to the discretion of magistrates despite the national guidelines in this regard.

- The team recognised that Italian law on jurisdiction (section 6 of the Criminal Code) makes it easier for Italy to deal with data held in the cloud although it also noted that the rules on jurisdiction could lead to complications with dealing with cybercrime given its likelihood to contain cross-border elements.

- During the visit, the impression was given that the Italian judicial authorities do not consider virtual currencies as "money", and that therefore several elements of its legal order would not apply to virtual money. The team was informed for instance, that there would be no power to act as regards confiscation of virtual money. This seems to go against the reality of the "cyber world", where many forms of virtual money exist, which are used extensively by criminals, and in respect of which it should be possible to take legal action. It seems appropriate therefore that Italy adapts its legislation and practice in this regard.[13]

[13] Subsequently to the evaluation visit, the Italian authorities informed the team that it is in the course of implementation of a cyber-study centre, in cooperation with the Academia (University of Modena- Reggio Emilia and University of Rome "La Sapienza"), whose purpose is to investigate and analyse the arising phenomena concerning the use (and misuse) of Bit Coin and its "close relatives", like Ripple, Lite Coin etc. In this centre the several de-anonymization techniques will be studied in order to move up the block-chain and obtain high impact in facing the new investigative challenges.

6 OPERATIONAL ASPECTS

6.1 Cyber attacks

6.1.1 Nature of cyber attacks

6.1.2 Mechanism to respond to cyber attacks

As mentioned in the first Chapter, the Minister of the Interior issued a decree on 9 January 2008 envisaging the setting up of the National Anti-Cybercrime Centre for the Protection of Critical Infrastructure (C.N.A.I.P.I.C). The Centre was established within the Postal and Communications Police Service by a decree issued by the Chief of Police (Director General of Public Security) on 7 August 2008.

It is an analysis and investigative coordination structure and cooperates with other institutions, the intelligence and military sectors and the CERT.

6.2 Actions against child pornography and sexual abuse online

Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography was transposed by Legislative Decree No 39 of 4 March 2014. Moreover, the rule includes specific aggravating circumstances when anonymization systems are used in the types of crimes linked to circulation and production of paedo-pornographic material.

The National Centre for the Fight against Online Child Pornography of the Postal and Communications Police (CNCPO) keeps up to date lists of websites which contain illicit material involving minors and mandate ISPs to remove and block such content on services located inside Italy. In cases where the server is located outside Italy, the Notice & Takedown procedure is started, where and when possible, through the National Centre for Missing and Exploited Children (NCMEC) because it guarantees the freezing and transmission of investigative data to the territorially competent investigation agencies.

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

Italy does not have any national database to identify victims, however, it makes use of the Interpol ICSE database. ICSE can be directly accessed by Italian law enforcement through the National Centre for the Fight against Online Child Pornography of the Postal and Communications Police (CNCPO).

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

When information is supplied by NGOs or citizens that a website contains illicit content, the CNCPO makes the necessary checks. If confirmed, it includes the website on the black-list and orders its removal.

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

Italian legislation contains specific provisions to criminalise sex tourism. Act No 269/1998 includes a section (Tourist initiatives aimed at exploiting child prostitution) which criminalises the organisation or advertisement of travel aimed at exploiting prostitution to the detriment of minors or, in any case, at including these activities shall be punished with imprisonment from 6 to 12 years and a fine from €30 to €300 million.

Italy makes use of online undercover investigation to counter real time web-based child sexual exploitation. It finds this to be an effective tool, in particular in the framework of international police cooperation.

6.2.4 Actors and measures counterfeiting websites containing or disseminating child pornography

Failure to delete images/videos occurs either when they have circulated on the internet and it is not possible to remove them, or when they are on foreign servers and it is not possible to obtain their deletion.

In this connection, Italy participates in the global initiative named Global Alliance, aimed at removing this material from the original source.

6.3 Online card fraud

6.3.1 Online reporting

The local units of the Postal and Communications Police regularly receive reports by both citizens holding payment cards and private agencies (issuer/acquirer).

6.3.2 Role of private sector

Child Pornography

The CNCPO operates on its own initiative drawing up reports on the operations carried out and/or conducted by ISPs (or content providers) upon its request. It also informs the judicial authority if the case pertains to the national territory.

As mentioned in Para 6.2, the Internet Service Providers have an obligation to and are responsible for the filtering of the contents indicated by the judicial authority and the CNCPO.

If the material is on Italian web sites the judicial authority orders the seizure of the site. For foreign sites, the filtering procedures (Black Lists) fall within the competence of the CNCPO in agreement with the judicial authority, which may request their restoration and therefore make them visible again.

In case of social networks or widespread services, platforms dedicated to law enforcement agencies are used, which often require the authorisation by the national judicial authority.

In cases where the server is located outside Italy, the Notice & Takedown procedure is started, where and when possible, through the National Centre for Missing and Exploited Children (NCMEC) because it guarantees the freezing and transmission of investigative data to the territorially competent investigation agencies. Police requests can be transformed into letters rogatory or other channels established through the Budapest Convention on Cybercrime can be used.

Credit Card fraud

Cooperation is ensured through the exchange of information and experiences between industry, private sector and law enforcement agencies in relation to criminal attacks against electronic payment instruments.

Italy uses a range of software and hardware for the analysis of data obtained during investigations on card present/not present fraudulent transactions.

The daily examination of the criminal techniques in the sector of card fraud enables a constant exchange of information between the bodies involved, and, as such, the physical and virtual defense systems are enhanced in order to combat the fraudulent access to sensitive data and adjust the investigative responses by means of an adequate information-based prevention activity.

The close and intense cooperation with Europol and the EMPACT project "Cybercrime Card Fraud", in which Italy is represented by the Postal and Communications Police, enables a good exchange between the law enforcement agencies engaged in the sector through regular meetings. During these meetings joint operations are planned, proposals for the solution of legislative, logistic or instrumental problems are examined, and, where necessary, operational meetings are organised for a direct sharing of views between and among the investigators involved in the investigations. Eurojust also takes part in this working group acting as a link between Member States' law enforcement and judicial authorities.

6.5 Conclusions

- The team welcomes the establishment of the National Anti-Cybercrime Centre for the Protection of Critical Infrastructure (C.N.A.I.P.I.C) and encourages it's further coordination and cooperation with the National CERT.

- The team was impressed with the work of the CNCPO and the regular monitoring of websites leading to creation of black lists to be filtered and blocked.

- The team was also pleased to learn that the take down and blocking of sites was mandatory for ISPs under the domestic legislation and, in addition, steps were taken to notify foreign authorities of websites containing child abuse material located outside Italy.

- The team also welcomed Italy's specific legislation on sex tourism and its notification to the ICSE of images found to reduce repeat victimisation.

7 INTERNATIONAL COOPERATION

7.1 Cooperation with EU agencies

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

Italy enjoys good cooperation with Europol/EC3 at various levels.

At an EU level via the European Cybercrime Centre (EC3)

- Italy is involved in the EMPACT[14] priority on cybercrime[15] as defined within the EU policy cycle 2014-2017[16]. In accordance with this latter framework, strategic objectives are defined in MASP[17] and operational goals implemented via OAPs[18].

- Italy is associated to all Focal Points (FPs) dedicated to cybercrime which are operational projects developed by Europol/EC3 to support EU MS and third parties' investigations.

14 European Multidisciplinary Platform against Criminal Threats

15 Cybercrime – aiming to: combat cybercrimes committed by OCGs and generating large criminal profits such as online and payment card fraud, cybercrimes which cause serious harm to their victims such as Child Sexual Exploitation, and cyber-attacks which affect critical infrastructure and information systems in the EU.

16 Council Conclusions on the creation and implementation of an EU policy cycle for organised and serious international crime, doc. 15358/10.

17 Multi-annual Strategic Plans

18 Operational Action Plans

- Italy participates in the Joint Cybercrime Action Taskforce (J-CAT) launched on 01 September 2013, which aims to further strengthen the fight against cybercrime in the EU and beyond. An Italian cyber officer from the Postal and Communication Police has participated in J-CAT since the beginning of this initiative.
- Currently 3 out of 68 officials at EC3 are Italian nationals, 1 is a temporary agent (FP Terminal). Two are contract agents (1 in the Outreach team and one in the Strategy team).
- Since 2013, Italy has been a Board member of European Union Cybercrime Task Force (EUCTF) composed of the Heads of the designated National Cybercrime Units throughout the EU MS and Europol. The EUCTF is an inter-agency group formed to allow the heads of Cybercrime Units with the participation of Europol, the European Commission, CEPOL and EUROJUST INTERPOL, Norway, Switzerland and Iceland as observers, to discuss the strategic and operational issues related to cybercrime investigations and prosecutions within the EU and beyond.
- Italy is participating to the European Financial Cybercrime Coalition (EFC) which has been established to foster relations between law enforcement and the financial sector against commercial sexual exploitation of children online.
- EU OF2CEN- Between 2010 and 2013 the (Postal and Communication Police) completed a successful EU funded project (OF2CEN) for creating an information sharing platform for banks and law enforcement agencies (LEAs) to combat cybercrimes and online frauds. Starting from that successful case, there is an new project in place to expand the scope of the previous OF2CEN to a European level, with the aim of enhancing the cooperation between all European Banks and LEAs.

Cyber-attacks

Italy's participation in the EMPACT sub-priority on cyber-attacks

Italy is participating in Crime Priority G3 Cyber Attacks in the following OAs:

- Drafting of the Internet Organised Crime Threat Assessment (iOCTA 2015).
- To identify current and emerging major cyber threats impacting against two or more Member States (MS).
- To develop a common tool kit to target and disrupt prevalent malware distributors, systems and services affecting two or more MS.
- To identify high value targets appropriate for a collaborative response involving two or more MS.
- Consolidation of the 2014 established European Union internet operational research coordination group.
- To collect malware contributions on current attacks from the banking industry at EC3 and contribute them to the EUROPOL Malware Analysis System (EMAS). Collect the contributions through the J-CAT and other EUROPOL channels
- To identify targets and coordinate arrests of lower level cybercrime groups or individuals (that use services of cyber OCGs).
- To support the Member States and operational partners to integrate money laundering and asset recovery techniques as an inherent part of operational actions in this OAP and exploit financial investigations avenues to the fullest extent against targets identified in OAs of this OAP.
- To exchange best practices and experiences in the co-operation with third states, indirectly via EUCTF (OA 3.1).
- To create a common taxonomy for cybercrime among MS law enforcement agencies and CERTs (Computer Emergency Response Team).
- To create and or adopt a common format to report cybercrime events to EUROPOL EC3, law enforcement agencies and CERTs.
- To create an automatic statistics analysis software of reported cybercrime incidents, indirectly via EUCTF.
- Develop and implement a solution for the pseudonomised cross-matching and de-confliction of data.

Italian participation in the FP CYBORG[19]

Italy participates in FP Cyborg. In most of the recent operations concerning malware attacks and botnet takedowns, Italy played a significant role either as affected country or because part of the criminal infrastructure was being hosted there. Europol received accurate operational support in all operations and when necessary the Polizia di Stato provided on site officers. Excellent cooperation with Carabinieri is ensured by the presence of a representative on the EUCTF Board.

Payment Fraud

Italian participation in the EMPACT sub-priority on Payment Card Fraud (PCF)

Italy participates in the following OAs:

- To increase participation and contributions in the Europol Platform for Experts (EPE SPACE).
- To conduct training activities and exchange of best practices on credit card fraud.
- To increase the awareness of the impact of the credit card fraud at European and national level.
- To include non-cash payment fraud on the agenda of awareness-raising events addressed to the citizens.
- To increase interaction with the private sector at national level in order to assist national/international investigations.
- To increase the level of exchanging the information between Europol and MS.
- To facilitate the exchange of information within European Union countries including non-EU countries.

[19] Preventing or combating the forms of criminality within Europol's mandate associated with internet and ICT (Information and Communication Technology) related Organised Crime. More specifically the focus will be on the crimes defined in Articles 2-8 of the Cybercrime Convention.

- To organise and coordinated action at the airports to target on-line fraudsters purchasing and facilitating purchase of airline tickets.

Italian participation in the FP TERMINAL[20]

Italy participates in FP Terminal, with a role in many international operations, including Airport Action Day.

Child Sexual Exploitation:

Italian participation in the FP TWINS[21]

Italy participates in FP Twins. There is a good level of cooperation and participation in operational activities. The main cooperation takes place with the Postal Police. [22]

20 Targeting networks consisting of individuals involved in fraudulent activities related to payment card fraud.

21 Child pornography networks on the internet: Targeting criminal networks involved in the production, sale or distribution of child abuse material.

22 Subsequently to the evaluation visit, the Italian authorities provided the following information: Regarding Law Enforcement activities aimed at disrupting- Online Child Sexual Offending with a view to enhance "Global Alliance" objectives, as already being referred to in the Assessment Document, we deem it would be useful to consider thoroughly the issue of the investigations on Darknets, which are well known as allowing the user to keep anonymous while browsing the Internet. Such investigative activities, in which the National Centre for the fight against online Child Pornography (CNCPO) is deeply involved, represent the current challenge and priority for investigations in such criminal area, and to this purpose have been carried out jointly and within the framework of international cooperation with LE agencies, such as Europol's FP Twins - Cybercrime Centre EC3.
Different projects have been developed, aimed at searching investigative and forensic solutions allowing to improve investigative techniques, required in order to counteract increasingly widespread anonymization systems, as well as those channels being used for virtual currency 'bitcoin', already being targeted by the National Centre for the 'Fight against Online Child pornography' (CNCPO), with a huge number of seizures of virtual portfolios. Findings of such research activities may soon be available and to be shared within the framework of the EMPACT projects as well as a subject of training activities for investigators at European level.

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

Italy has a positive view of this cooperation. The team was informed that Italy is also exploring ways of further enhancing this cooperation for example when dealing with third states.[23]

7.1.3 Operational performance of JITs and cyber patrols

An investigation is currently underway in cooperation with Europol which will provide other Police agencies of EU countries with information about criminal cases.

7.2 Cooperation between the Italian authorities and Interpol

Division III (Interpol) of the Service for International Police Cooperation is part of an effective system for combating the so-called "Cybercrime".

The INTERPOL National Central Bureau (NCB) for Italy is part of the International Police Cooperation Service (SCIP). SCIP is part of the DPS Central Directorate of Criminal Police, International Police Cooperation Service (Servizio per la Cooperazione Internazionale di Polizia) and coordinates investigations and operations requiring international outreach. It is headed, on a rotation basis, by a high ranking official of the Polizia di Stato, Carabinieri or Guardia di Finanza.

Italy also supports the liaison officers' network, which:

- allows for the acquisition of knowledge of the criminal phenomenon by comparing the different laws of other countries;
- provides regular updates on the "modus operandi" and techniques employed abroad to combat the phenomenon;
- rapidly identifies foreign points of reference with a view to promoting more direct forms of cooperation also outside ordinary police channels.

[23] Further to the evaluation visit, Italy informed the team that the Postal and Communications Police is now the single point of contact for Europol IRU.

Other initiatives

- The International Police Cooperation Service is an interagency service for international operational police cooperation. It also comprises the National Central Bureau-Interpol, the Italian Europol National Unit and the S.I.R.E.N.E. Division.
- Italy also participates in the G8 High Tech Crime (Group Rome-Lyon).

7.3 Cooperation with third states

Italy like many other Member States finds cooperation with third countries variable and has experienced some difficulties with receiving information required for the purposes of investigation in a timely manner from some third states such as the United States. The team was informed that Italy is considering the possibility of making better use Europol/EC3 to deal with third states in joint operations or with a view to approaching new partner countries that can contribute to widening the scope of operational activities in the field of cybercrime.

7.4 Cooperation with private sector

As to the provisions contained in the Code of Criminal Procedure, the private sector is not involved. Technical consultants, often from the private sector, may be appointed within the framework of particularly complex criminal proceedings in relation to investigations into cybercrime (for example, to analyse the content of a Hard Drive that has been seized).

Working groups set up at the Postal and Communications Police often involve the private sector. Participation in these groups, however, depends on the will of the single service providers (Internet providers, telephone companies, banks. etc.).

Sections 14-16 of Legislative Decree No. 70/2003 (implementing the European Directive on electronic commerce) regulate the liability of the so-called intermediary service providers by making a distinction between the following:

- data carrier activities (mere conduit);
- intermediate and temporary storage of information designed to facilitate its forwarding to other recipients who have requested it (caching);
- storage of information provided by recipients of the service, including making available a storage space on a server for Web sites or pages (hosting).

These rules, however, mainly apply in a civil law context. In a criminal law context, liability of Internet providers can be derived from the general principles concerning aiding and abetting (Section 110 of the Criminal Code), or failure to prevent an act (where the law expressly imposes to take action to prevent the said act, Section 40, subsection 2 of the Criminal Code). Requests for blocking access to websites or removing contents from websites are submitted to the G.I.P. is provided under Italian legislation by specific decree (seizure for preventative purposes under Section 321 of the Code of Criminal Procedure).In the field of terrorism prevention, Act No. 43 of 17 April 2015 (turning into law the Decree-Law on terrorism) has provided for a more rapid mechanism for inhibiting/removing contents. More specifically:

- The Interior Ministry provides an up-to-date blacklist of websites used for the activities and conducts referred to under Sections 270-*bis* and 270-*sexies* of the Criminal Code based on the reports from the judicial police offices.
- Connection providers, at the request of the competent Judicial Authority, must prevent access to the websites included in the list within the time limits established and according to the methods and technical solutions identified and defined by law.
- When dealing with the crimes that have been committed for terrorist purposes and where there are strong grounds for believing that these activities may be carried out via ICT, the Prosecutor may order, the removal of this content. In the case of contents generated by users and hosted on platforms related to a third party, only the removal of illicit contents is specifically provided for.

- Recipients must comply with the order without delay and, in any case, within 48 hours after they have been notified. In case of failure to comply with the order, access to the Internet dominion is prevented according to the procedures and methods established by Section 321 of the Code of Criminal Procedure.

7.5 Tools of international cooperation

7.5.1 Mutual Legal Assistance

There are no special MLA rules for dealing with cybercrime. International, bilateral or multilateral conventions of a general nature apply, or, if the necessary prerequisites are satisfied, conventions relating to specific crimes (i.e., the 2000 UN Convention against Transnational Organised Crime).

Italy has not ratified the 2000 MLA Convention. Italy pointed out, however, that a draft enabling law concerning the implementation of MLA Convention has now been approved by the Chamber of Deputies and is currently being examined by the Senate; in order to accelerate implementation, the Minister of Justice has formalised the appointment of a technical commission, with the task of working out rules for its transposition. The same commission has also been entrusted with the task of drawing up a set of rules aimed at implementing the Directive regarding the European Investigation Order in criminal matters, for the implementation of which powers have already been conferred on the Government. Therefore, it is very likely that in the course of this year the Directive regarding the European Investigation Order will be implemented and the MLA 2000 Convention ratified.

In the meantime, (other) general rules apply, including relevant international conventions (since no specific legislation exists in relation to cybercrime). For example, the 1959 European Convention on Mutual Assistance in criminal matters lays down that during investigations, or in cases of urgency, a request may be directly forwarded by the Italian Judicial Authority (active MLA) or to the Italian Judicial Authority (passive MLA), who is also competent for making decisions on such requests.

For States that, like Italy, adhere to the Schengen agreements, there is also the possibility of requests being sent directly to Judicial Authorities who are also competent for making decisions on requests for MLA.

In other cases, an MLA may be sent through the Central Authority for International Judicial Cooperation (Justice Ministry). In cases not specifically provided for in agreements, or if so indicated in these agreements, the communication channel used, if not direct or through Central Authorities, is the diplomatic one.

Italy also makes informal direct contact with police forces or the Judicial Authorities in other jurisdictions where possible. A number of different channels may be used (phone, email, call conferences, personal visits, etc.).

Many requests for MLA are sent to the United States (for example, to know the contents of a Facebook account). In this case, the bilateral treaty in force between Italy and the US is used, as supplemented by the US-European Union Treaty. Sometimes the US rejects a request for MLA on the grounds that it lacks the so-called “probable cause” or when the case is considered de minimis.

7.5.2 Mutual recognition instruments

Italy has implemented the Framework Decision on the European arrest warrant (FD 2002/584) and that on the execution of custodial sentences (FD 2008/909). This has made it possible to implement mutual recognition of sentences and measures involving deprivation of liberty with a view to directly executing a sentence or the surrender of the person sought.

7.5.3 Surrender/Extradition

With regard to passive European arrest warrant procedures, all cybercrime qualifies for surrender under an EAW, without verification of double criminality. The relevant Italian legislation provides that all cybercrimes carrying a maximum penalty of over three years' imprisonment may give rise to surrender.

An EAW may lead to surrender, provided a penalty of no less than four months' imprisonment has been actually imposed (European arrest warrant issued for the purpose of executing a sentence), or the crime carries, in the abstract, a maximum penalty of over one year's imprisonment (European arrest warrant issued for the purpose of prosecution) (Section 7, subsections 3 and 4 of Act 69/2005).

As to active EAW procedures, in order to comply with the principle of proportionality, it is necessary that the cybercrime concerned carries a penalty of over one year's imprisonment to be actually imposed (European arrest warrant issued for the purpose of executing a sentence) or that an arrest warrant be issued for a cybercrime carrying, in the abstract, a maximum penalty of over five years' imprisonment (European arrest warrant issued for the purpose of prosecution).

With regard to passive extradition, international conventions in force apply. In the case of active extradition, the Justice Minister, according to the principle of proportionality and with the exception of specific cases, submits a request for extradition only for sentences exceeding four years' imprisonment (extradition for the purpose of executing a sentence) or if an arrest warrant has been issued for a cybercrime carrying, in the abstract, a maximum penalty of over five years' imprisonment (extradition for the purpose of prosecution).

Please refer to the following table:

1)Computer frauds;				
Offence	Penalty		Surrender	Extrad.
	Min.	Max.		
Section 640-ter ("Computer fraud") Phishing or Dialer				
Common	6 months' imprisonment	3 years' imprisonment	Only by Exec. Ord.	YES
Aggravated	1 year	5 years	YES	YES
Section 640 ("Fraud")	1 year	5 years	YES	YES

2)Forgery;				
Offence	Penalty		Surrender	Extrad.
	Min.	Max.		
Section 491-bis (“Computer documents”)				
Committed by a private individual	8 months	4 years	Only by Exec. Ord.	YES
Committed by a public official	1 year	6 years	YES	YES
	1 year	5 years	YES	YES

3)Data and computer systems integrity;				
Offence	Penalty		Surrender	Extrad.
	Min	Max		
Section 635-bis (“Causing damage to computer and ICT systems”)	6 months	3 years	Only by Exec. Ord.	YES
Section 420 (“Attack on systems of public utility”)	1 year	4 years	Only by Exec. Ord.	YES
Section 392 (“Arbitrary exercise of one’s rights involving violence against property”) In relation to information systems, it includes altering, modifying or erasing a program, entirely or in part, with a view to preventing its regular functioning.	Penalty Fine		NO	NO
Section 615-Quinquies (“Circulation of programs intended to cause damage to or interrupt a computer system”):	up to 2 years		Only by Exec. Ord.	YES

4)Confidentiality of data and computer communications.				
Offence	Penalty		Surrender	Extrad.
	Min	Max		
Section 615-ter (“Unauthorised access to a computer or ICT system”):				
Common	Up to 3 years		Only by Exec. Ord.	YES
Specific cases provided for in this section	1 year	5 years	YES	YES

If the facts referred to under sections 1 and 2 concern computer or ICT systems of military interest or systems related to public order and security, or to health and civil defence, or , in any case, of a public interest. General cases Specific cases	1 year 3 years	5years 8 years	YES	YES
Section 615-quater ("Unauthorised possession and distribution of computer or ICT systems'access codes"):	Up to 1 year		Only by Exec. Ord.	YES
Section 621 ("Disclosure of the contents of secret documents")	Up to 3 years		Only by Exec. Ord.	YES
Section 617-quater ("Interception, hindering or unauthorised interruption of computer or ICT communications"):				
Common	6 months	4 years	Only by Exec. Ord.	YES
Specific cases provided for under this section	1 year	5 years	YES	YES
art. 617-quinquies ("Installation of equipment designed to intercept, hinder or interrupt computer and ICT communications")	1 year	4 years	Only by Exec. Ord.	YES
art. 617-sexies ("Falsifying, altering or erasing the contents of computer or ICT communications"):	1 year	4 years	Only by Exec. Ord.	YES

There are no specific rules for cybercrime. Hence, general rules apply.

In active extradition cases, the Justice Minister directly submits the request, also at the request of the Judicial Authority. It may be directly transmitted to the foreign Central Authority or through the Ministry of Foreign Affairs and international cooperation (according to existing international conventions).

In passive extradition cases, the request is submitted, either directly or through diplomatic channels, to the Italian Justice Minister. Responsibility for deciding on passive extradition lies with the Justice Minister, after the competent judge has ruled in favor of extradition. If the competent judge believes that it is not possible to grant extradition, the Justice Minister cannot grant it. If the judge believes that it can be granted, the Minister may have discretion to grant or deny it.

Surrender by means of the so-called passive European Arrest Warrant - EAW

An EAW issued by a foreign Judicial Authority is sent, through the Justice Ministry, to the Court of Appeal that has territorial jurisdiction (according to the place where the person whose surrender is requested is).

Responsibility for issuing an EAW lies with the G.I.P. [Judge in charge of pre-trial investigations] who has issued a pre-trial warrant, or with the Prosecutor who has issued the order to impose the sentence or the final security measure provided for in the sentence. The sending of the request to the foreign Sate comes within the competence of the Justice Ministry.

The communication channels used are SIRENE and SIS II for the European Arrest Warrant, and INTERPOL (I 24/7). The ASF database may also be consulted.

The EAW, be it passive or active, always entails temporary arrest and is generally executed, once the person sought has been located, within the time limits established by the Framework Decision (for a maximum of 90 days). The average execution time, however, is shorter.
Extradition requests, both passive and active, are generally accompanied by a provisional arrest request. Extradition procedures, both passive and active, usually take a longer time.

Whenever a European Arrest Warrant is issued, the procedure followed is the standard one for countries not adhering to the Schengen agreement – the so-called associated countries (including Norway and Iceland). The extradition procedure is employed in this case.

7.6 Conclusions

- Italy has not ratified the MLA Convention 2000 and as a result relies on the earlier mutual legal instruments such as the 1959 Convention and the Schengen Agreement to facilitate mutual legal assistance. As the MLA Convention 2000 has streamlined MLA procedures, the team considers it would be of tremendous benefit to Italy to ratify this convention.

- Italy does not participate in the 2015 EMPACT sub-priority on Child Sexual Exploitation (CSE) and should be encouraged to do so. [24]

[24] Further to the evaluation visit, Italy informed the team that it now participates in the CSE.

8 TRAINING, AWARENESS RAISING AND PREVENTION

8.1 Specific training

Training for the Judiciary: The School for Advanced Studies for the Judiciary organises courses on cybercrime, both in the form of initial training – for members of the Judiciary on probation – and permanent training – for members of the Judiciary in regular active service. Part of the training includes a module dedicated to Investigative and Analysis Protocols concerning the main aspects of cybercrimes and crimes via ICT, and the permanent training course P15089 – Criminal law and the Web, an e-learning module for 2014. In addition, specific training is provided to officers employed in operational activities at their respective Units.

Training for Police: The training for the Postal and Communication police is composed of basic training, alongside the regular university -level studies for middle and upper management and part of the standard education for police officers. There are also refresher courses for all cyber-units. The duration of training courses depends on the officers' years of service in the specialty, i.e. six weeks if the officer has been serving for less than three years, and one week if the officer has been serving for more than three years. The training is provided using internal trainers.

In addition a 3 day train-the-trainer course in the Cesena police academy has been developed with the support of the FBI and US Secret Service. In between the basic and the refresher course the Police Academy of Rome has started to deliver training for top level management which includes a module on cybercrime.

8.2 Awareness raising and prevention

Over the last few years, the Postal and Communication Police Service has been carrying out projects designed to provide information about how to prevent Internet risks for minors and care givers in cooperation with public and private entities engaged in child protection.

The campaign, which is in its fifth year, targets children aged 7-18. Last year alone it visited 400,000 students so has a far reach. It involves dedicated sessions with teachers and parents to highlight the risks and benefits of using the internet.

The Postal and Communication Police have also been running a information roadshow since 2013. Presentations are given by Police, Ministry of Education, psychologists and the Private Sector. The event is also attended by celebrities and sports stars to make it more attractive to the target audience and also involves real victim stories. The school campaign also included a theatre show depicting a real case of cyberbullying which led to the suicide of a 17 year old.

The data protection authority the *Garante*, has also been running awareness campaigns in schools since 2005 to make children aware of the risks of sharing data on the internet.

8.2.1 National legislation/policy and other measures

8.2.2 Public Private Partnership (PPP)

The Italian authorities receive good support from the private sector to assist the public awareness campaigns, for example through financial contributions to fund the media centre at the roadshow and also the attendance of celebrities and sport stars to the events.

8.3 Conclusions

- The team was impressed by the level of training provided to practitioners, in particular the police dealing with cyber crime, however it considers that more training could be provided to magistrates, in parallel with (at least) specific District level officers, thus creating positive synergies between legal practitioners and Police practitioners, creating effective networking. The use of a common taxonomy, as in use by European CERTS and EC3 (in attachment to this Report) would also be a good and positive contribute to approximate magistrates, CERT and Police.

- It would be useful if Italy made better use of the opportunities provided for by Europol for that purpose, so that a certain number of (at least at) District level Officers could participate on Europol's EC3 space platform, and apply to ECTEC and CEPOL courses. Consideration could also be given to providing access to external training courses i.e. third level courses for practitioners dealing with cybercrime.

- The team was impressed by the public awareness campaigns undertaken by the Postal and Communication Police and Il Garante. It noted, however, that there may be some duplication of efforts and would suggest better coordination between the two authorities, for example, in the framework of the National Strategy."

9 FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Italy

The Italian authorities consider that common legislation on data storage should be finalised with a view to directly acquiring data from partner countries within the framework of investigations into cybercrime and introducing tougher security measures for private institutions (former Policy Documents).

9.2 Recommendations

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

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

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

9.2.1 Recommendations to Italy

1) The team was pleased to note that Italy has a National Cybercrime Strategy, "National Framework for Cyber Space Security" and accompanying operational guidelines but it considers that it needs to be more targeted and contain specific, measurable objectives so the role of each stakeholder under the Strategy is clear. This would also ensure a better coordination of the roles of the stakeholders to avoid duplication of efforts. It would also be useful to provide an estimated cost of each action.

2) In terms of sanctioning of special investigation techniques, whilst noting that regional guidelines exist on the use of these measures, the team was advised that there was variance in these guidelines. The team recommends that Italy considers addressing this inconsistency in order to improve the capacity of the police to investigate cybercrime.

3) Italy seems to have a robust legislative framework but the team was advised that no provision is made for dealing with virtual currency. Italy is invited to consider if its legislation or legal procedures could and should be adapted in order to better deal with the issue of virtual currency.

4) Developing public-private cooperation was a key priority of the strategy. The team recommends that Italy takes further steps to foster this cooperation by (i) making use of the experience and expertise of service providers/industry experts, (ii) improving cooperation with the financial sector by expanding the OF2CEN project[25], and (iii) considering whether the mandatory reporting for of cyber attacks for private sector could be of benefit.

5) It is highly recommended that Italy terminates the ratification of the 2000 MLA Convention to enhance mutual legal assistance between Member States. This would greatly aid its ability to tackle cybercrime more effectively and improve cooperation with other Member States. This would also benefit all criminal investigations with a cross-border element.

[25] Subsequently to the evaluation visit, the Italian authorities observed that, as regards the Financial Cyber-crime sector, in the period 2016-2017 Italy will focus on strengthening of Public Private Partnerships in relation to the EU OF2CEN project. The Italian Postal and Communications Police is leader of the EU OF2CEN project, which involves the Law Enforcement Authorities of Hungary, France and Spain and foresees the active participation of the European Banking Federation, which will provide support and disseminate the initiative among its associate banks. At the same time, European Cybercrime Center of Europol (EC3), as a focal point in the EU's fight against cybercrime, will help engagement in the project of Member States throughout EU and will benefit by an enhanced ability to identify new crime trends. In relation to the participation to the current policy cycle (2014-2017), POLCOM joined both the priorities related to "Cyber attacks" and "Card frauds": in particular, for the first time, in the Operational Action Plan 2016 (priority Cyber Attacks) Italy is the Action Leader of O.A. 1.3, related to 'Money Mules', that consists of a PPP operational plan, in order to collect and share information about financial cyber-crimes.

6) It is also recommended that Italy increase awareness amongst practitioners on mutual legal assistance generally, particular to inform them which channels are most appropriate in terms of issuing letters rogatory and seeking information from foreign law enforcement and judicial authorities regarding cybercrime. There was a clear lack of understanding amongst practitioners on where cases should be sent and who should be contacted. In this regard, it is recommended that Italy reinforce its cooperation with Europol and Eurojust.

7) Italy is recommended to complement its in-house training programmes on cybercrime by making use of training opportunities provided both by EU bodies such as EC3, ECTEG and CEPOL and those offered by academic institutions and private companies.[26] In particular, the team considered that training for the judiciary could be enhanced.

8) The team recommends that the gathering and collation of statistics should be improved, both at law enforcement and prosecution level. This would assist inter alia in resource allocation, case comparisons and crime classification based on categories such as Modi Operandi and criminal activities.

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

1) The team considers that the Italian model of recording personal identification information at the point of sale of SIM cards is a practice, which should be adopted by other Member States, where feasible. This practice would provide law enforcement authorities with valuable information, which can assist in investigation of a range of criminal activity such as cybercrime, organised crime and terrorism.

[26] Subsequently to the evaluation visit, the Italian authorities informed the team that Italy is complementing the in house training, also using opportunities provided by EU Agencies such as Cepol. For 2016 Italy will participate in the Cepol Exchange Programme, with particular focus to area related to cyber attacks and card fraud. The Italian authorities have also requested Cepol to be included in several courses.

2) The team recommends that a converted European effort needs to be made to tackle cybercrime. Issues such as how to collect e-evidence, deal with jurisdiction, improve mutual legal assistance and access data stored in the 'cloud' need further consideration at an EU level.

3) The team recommends that consideration should be given to developing EU legislation to mandate ISP to block/remove websites containing malicious content. This is already in practice and used to good effect in the Italian system and could be replicated across the EU.

9.2.3 Recommendations to Eurojust/Europol/ENISA

1) The team recommends that Eurojust provides information by way of user manual/directory of services to Member States on how to contact other authorities for the various MLA activities in each Member State (e.g. by using certain tools or procedures).

2) Eurojust and Europol should promote the services and resources they provide to Member States which can improve national capacity to deal with mutual legal assistance.

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

Agenda dei lavori

Monday, 25 May 2015

Time to be defined	arrival at the Rome – Fiumicino Airport transfer to the Hotel

Tuesday, 26 May 2015

09:00	arrival at Polo Tuscolano
09:15	welcome to the SGAE by Dr. Roberto Sgalla Central Director of Highway, Railway, Postal and Communication and Special Units of State Police

10:00 to 12:30: Postal and Communication Police Service

- introduction by Mr. Antonio Apruzzese Director of Postal and Communication Police Service
- general presentation of the Italian contrast and prevention strategies against cybercrime

12:30 to 13:45: lunch

14:00 to 15:30: visit to CNAIPC, CNCPO, COMMISSARIATO di P.S. on line

- CNAIPC: overview of the operational procedures in relation to the protection of critical infrastructures
- CNCPO: introduction to infrastructures tools in preventing and combating on line pedophilia. Multidisciplinary approach, International Cooperation
- COMMISSARIATO DI P.S. ON LINE: presentation of the on line Police Office

17:00 National Security Agencies DIS, AISI e AISE

- New National cyber security system
- D.P.C.M. 24 gennaio 2013

20:00 dinner

Wednesday, 27 May 2015

09:00 visit to data protection Authority

- introduction to the Autority's tasks
- cybercrime contrast vs rights of privacy (Decreto Legislativo n. 196/2003)
- cooperation at governamental level

12:30 to 13:45: lunch

14:15 transfer to Procura della Repubblica di Roma

15:00

- meeting with the cybercrime task force set up by the Prosecution Office: strategies, operational procedures
- ratification law of Budapest Convention n. 48/2008
- International cooperation

17:00 arrival in Hotel

Thursday, 28 May 2015

09:00 departure to Milan

- security protocols implemented by CNAIPC for Expo

Time to be defined departure to Rome

Friday, 29 May 2015

09:30 arrival at Polo Tuscolano

- wrap up meeting - closing remarks

10:45 transfer to the Ministry of the Interior

12:00 welcome to the SGAE by the Chief of Police, General Director of Public Security

Time to be defined: transfer to the Rome Fiumicino Airport

ANNEX B: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	ITALY OR ACRONYM IN ORIGINAL LANGUAGE	ITALIAN OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
CERT	-	-	Computer Emergency Response Team
CSE	-	-	Child Sexual Exploitation
NIS		-	Network and Information Security Authority
CNCPO	-	-	National Centre for the Fight against Online Child Pornography
EC3	-	-	European Cybercrime Center at Europol
CNAIPIC		-	National Anti-Cybercrime Centre for the Protection of Critical Infrastructure
EMPACT	-	-	European Multidisciplinary Platform against Criminal Threats
ENISA	-	-	European Network and Information Security Agency
EUROJUST	-	-	The European Union's Judicial Cooperation Unit
EUROPOL		-	The European Police Office

GENVAL	GENVAL	*Groupe de travail "Questions Générales y compris l'Evaluation"*	Working Party "General Questions including Evaluation"
NCRPs			National Centre Reference Point
JIT	-	-	Joint Investigation Team
ABI			Association of Italian Banks
MLA	-	-	Mutual Legal Assistance
EUCTF	-	-	European Union Cybercrime Task Force
EFC	-	-	European Financial Cybercrime Coalition
LEAs	-	-	Law Enforcement Authorities
PCF	-	-	Payment Card Fraud
FP TWINS	-	-	Child pornography networks on the internet
EAW	-	-	European Arrest Warrants