Council of the
European Union

Brussels, 8 June 2017
(OR. en)

10905/1/16
REV 1 DCL 1

GENVAL 83
CYBER 81

DECLASSIFICATION

of document:	10905/1/16 REV 1
dated:	24 October 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 Portugal

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, 24 October 2016
(OR. en)

10905/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 83
CYBER 81

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 Portugal

ANNEX

Table of Contents

1. EXECUTIVE SUMMARY

The mission to Portugal was organised very well and the visit took place in a pleasant and warm atmosphere. The evaluation team had the opportunity to meet representatives of different authorities involved in prevention and fight of cybercrime, including the Ministry of Justice, Ministry of Interior, the General Prosecutor's Office, the Criminal Police (National Cybercrime Investigation Unit, National Unit against Terrorism, International Cooperation Unit and Technological Support Unit), the Centre for Judicial Studies, the National Centre for Cybersecurity, the National Communications Authority and representatives of the Bank of Portugal and of the private sector.

During the visit the representatives of the Directorate General for Justice Policy within the Ministry of Justice, that coordinated the evaluation of Portugal, made everything possible to provide the evaluation team with complete information and clarifications on legal and operational aspects of detecting, preventing and combating cybercrime, international judicial cooperation in criminal matters and cooperation with EU-agencies, cyber strategy, training, etc.

During the working meetings the evaluation team had the opportunity to better understand the responses provided in the questionnaire and to fill the gaps where necessary.

It is important to state that the responsibility to secure cyberspace is shared between public and private actors within Portugal.

They all have different competences and responsibilities but the "fight against cybercrime" is a common goal observed.

There was good cooperation in general between all the actors during the visit to Portugal and they appeared well aware of the risks inherent to cyberspace.

In May 2015, Portugal adopted the National Cyberspace Security Strategy. The Strategy includes a specific intervention axis "***Fight against Cybercrime***" and the main objectives are to promote awareness, free, safe and efficient use of cyberspace, to protect fundamental rights, freedom of expression, personal data and the privacy of citizens, to strengthen and guarantee the security of cyberspace, of critical infrastructures and of vital national services and to affirm cyberspace as a place for economic growth and innovation.

There is a multidisciplinary approach which involves the National Centre for Cybersecurity (CNCS), law enforcement authorities, such as the Criminal Police (PJ), National Republican Guard (GNR) and the Public Security Police (PSP), as well as other public and private stakeholders.

The Strategy is focussed on two major options; the review and update of legislation and the streamlining of the skills of the PJ (to strengthen its structures and its technical and forensic skills to carry out investigations in the cyberspace).

It is the opinion of the evaluation team that the identification and attribution of responsibility over these interdependencies is one of the most important tasks to be achieved when implementing the National Cyberspace Security Strategy.

A more coordinated approach on statistics would also be beneficial in order to have an accurate image on the types of cyber criminality reflected in the different stages of investigation, prosecution and trial.

Regarding the national structure there are specialised units at police and prosecutor levels. The newly formed National Cybercrime Investigation Unit within the PJ coordinates and investigates cybercrime in conjunction with judicial authorities. Regional units have a capability to investigate cybercrime with central support being provided by the National Cybercrime Investigation Unit in Lisbon. These investigations include offences among others related to computer crime in general, child pornography and card fraud.

The Cybercrime Office within the General Prosecutor's Office[1] has the responsibility to coordinate the State Prosecution Service in all matters in respect to cybercrime and in the obtaining digital evidence. Their role also includes supporting in the drafting of legislation where requested by the Ministry of Justice. In addition awareness raising and the facilitation and coordination of training form part of their remit. The cybercrime office has a state-wide remit with a national network of 43 prosecutors covering 23 judicial districts.

There are no specialised judges as this would be against the constitutional rules regarding the random distribution of cases in the courts in order to ensure the impartiality of the judgement.

The national legislation complies with the Council of Europe Convention on cybercrime and its Additional Protocol and the Directive 2013/40/EU on attacks against information systems. The Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography has also been transposed by Law no 103/2015, of 24 of August.

The cooperation with the private sector is quite good, for example in the cooperation between law enforcement agencies and Interbank Cooperation Society S.A. (SIBS) on investigation and prevention of payment fraud.

There is still room for improvement at operational level due to the fact that according to the representative body for the Internet Service Providers (APRITEL) the judicial system doesn't use the software tools which would enhance more rapid access to telecommunications data.

Prevention and public awareness in respect to cybercrime is carried out by a number of authorities within Portugal. They include the National Centre for Cybersecurity (CNCS), law enforcement authorities and the private sector. These sectors play an active role in prevention and awareness campaigns throughout the state.

[1] http://cibercrime.ministeriopublico.pt

2. INTRODUCTION

Following the adoption of the Joint Action 97/827/JHA of 5 December 1997[2], 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: cyberattacks, 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[3] (transposition date 18 December 2013), and Directive 2013/40/EU[4] on attacks against information systems (transposition date 4 September 2015), are particularly relevant in this context.

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

Moreover, the Council Conclusions on the EU Cybersecurity Strategy of June 2013[5] reiterate the objective of ratification of the Council of Europe Convention on Cybercrime (the Budapest Convention)[6] 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[7].

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 cyberattacks and fraud as well as child pornography. The evaluation also covers operational practices in the Member States with regard to international cooperation and the support offered to persons who fall victims of cybercrime.

The order of visits to the Member States was adopted by GENVAL on 1 April 2014. 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.

[5] 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.

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

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

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 Portugal were Mr. Kiril Milev (Bulgaria), Mr. John Roche (Ireland) and Mr. Donatas Mazeika (Lithuania), together with Ms Carmen Necula from the General Secretariat of the Council. From Eurojust it was present Mr. Bostjan Lamesic, assistant to the National Member for Slovenia.

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 Portugal between 10 - 13 November 2015, and on Portugal 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

The National Cyberspace Security Strategy (Strategy) was adopted by means of Resolution no 36/2015 of the Council of Ministers, on 28 May 2015.

It was published in the Official Gazette, I *Series,* no 113, of 12 June 2015 (a copy of the official publication is attached to the present Questionnaire) and its description can be found at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/portuguese-national-cyber-security-strategy.

This Strategy, based on the general principle of State sovereignty, on the general ideas contained in the Cybersecurity Strategy of the European Union (EU) and on the European Convention on Human Rights, the European Charter of Fundamental Rights, the protection of the fundamental rights, freedom of expression, personal data and privacy, sets the general objectives designed to enhance the national cyberspace strategic potential, including, a specific intervention axis "***Fight against Cybercrime***".

The underlying commitment of the Strategy is to improve the security of networks and of information in order to protect and defend critical infrastructures and vital information services and to promote the free, secure and effective use of cyberspace to citizens, businesses and public and private bodies. It rests on the following five pillars:

1. Subsidiarity;
2. Complementarity;
3. Cooperation;
4. Proportionality; and
5. Awareness.

Indeed, subsidiarity is seen in terms of the security of cyberspace as being an integral part of national security and an essential factor for the functioning of the nation, for economic development and innovation, as well as for citizen confidence in the digital marketplace and in cyberspace. The State reaffirms its strong commitment to defend the cyberspace. As a large part of the technological infrastructures that make up cyberspace are owned by private operators, who are mainly responsible for their protection, this responsibility begins with the individual, and the responsible use of cyberspace, and ends with the state as guarantor of sovereignty and of constitutional principles.

As to the complementarity, the responsibility for the security of cyberspace is shared among different actors, whether public or private, military or civilian, collective or individual. A broader and more integrated approach to cyberspace security brings together a number of actors with different responsibilities and abilities, for the benefit of all.

The Strategy cooperation´s pillar derives from the fact that, in a highly interconnected and interdependent world, a secure cyberspace requires such close cooperation between national and international allies and partners, based on the development of mutual trust.

The risks inherent to cyberspace must be assessed and appropriately managed, ensuring proportionality of means and measures for their exercise, i.e., must observe the proportionality principle.

In the same token, awareness is provided for in order to guarantee the security of technological infrastructures, information systems and networks relies on end users knowing what steps to take in order to minimise the risks to which they are exposed. Raising awareness is a key aspect for maintaining a secure cyberspace.

The Strategy aims at achieving the following strategic objectives:

- To promote awareness, free, safe and efficient use of cyberspace;
- To protect fundamental rights, freedom of expression, personal data and the privacy of citizens;
- To strengthen and guarantee the security of cyberspace, of critical infrastructures and of vital national services;
- To affirm cyberspace as a place for economic growth and innovation.

The implications and requirements associated with each of these strategic objectives allow for general and specific guidelines, which are translated into six axes of intervention with actual measures and lines of action to enhance the strategic national potential in cyberspace, i.e.:

- Axis 1 - Structure of cyberspace security;
- Axis 2 – Fight against Cybercrime;
- Axis 3 - Protecting cyberspace and national infrastructures;
- Axis 4 - Education, awareness and prevention;
- Axis 5 - Research and development;
- Axis 6 - Cooperation.

The challenges posed by cybercrime entails constantly updating of the measures and means put in place in order to ensure their maximum effectiveness. In its axis 2, the Strategy provides for a review and update of legislative measures, in particular those designed to ensure the criminalisation of new types of crimes whether against or taking advantage of cyberspace, to support criminal investigations and to enhance the capacities of the PJ, as well as to improve judicial cooperation at a national and international level.

The National Cyberspace Security Strategy recognises the vulnerability of new technologies and acknowledges that they create social and material risk. In particular it recognises an exponential increase in sex crimes against minors facilitated by this technology. In addition it mentions the transnational dimension and highly sophisticated methods which demand firm, determined and effective intervention.

It acknowledges that the "networked world" engenders new and unique criminal activities such as organised cybercrime associated with bank fraud and identity theft, political sabotage and the increase in state and industrial espionage.

The strategy states that there is evidence of the ability of political and religious activists with terrorist motivations to engage nationally and internationally in activities that have an impact on the security of information infrastructures.

The PJ has intervention capacity at the levels of Interpol and Europol, being a part of the team of focal points TERMINAL (on means of payment), TWINS (on child sexual exploitation) and CYBORG (on cyberattacks). From the viewpoint of this Police, the fact that the Law explicitly confers to it the exclusive competence on cybercrime investigation is seen as good practice as the lack of jurisdictional conflicts, facilitating the joint work of all the law Enforcement Authorities (LEAs).

From the point of view of prevention, as an example GNR, as one of the law enforcement authorities with competence for the prevention of cybercrime, has carried out initiatives on crime prevention and has led special police programs on awareness raising especially addressed to the so-called risk groups (young and old) in cooperation and partnership with academia and public and private organizations. In this context, GNR is involved with a European Crime Prevention Award project consisting essentially of different forms of networking communications and joint participation initiatives (training sessions, competitions, seminars, webcasts, etc.). The output will be to build and consolidate ethical and moral values among all users of the cyberspace. This project called "Safer Internet" is particularly focussed on young people.

3.2. National priorities with regard to cybercrime

The intervention axis 2 of the Strategy recognises that the cyberspace created new legal interests that have to be protected, new types of crimes and also new ways to commit old crimes, which imply a permanent update of legislation.

On the other hand, as regards this axis, it should be highlighted, inter alia, the need for "*the institutions which deal with cybercrime investigations to be fully equipped in order to carry out their mission, while the judicial system, in general, be adapted to the new technologies*".

These are the two major options of the strategy: the review and update of legislation and to streamline the skills of the PJ (to strengthen its structures and its technical and forensic skills to carry out investigations in the cyberspace). As said before, the PJ has exclusive competence for the investigation of cybercrime, according to Law no 49/2008, of 27 August, which approved the Law for the Organisation of Criminal Investigation.

Specific legislation on attacks against information systems is in force and the rules and principles of the Convention on Cybercrime of the Council of Europe (Budapest Convention) and its Additional Protocol are foreseen in Law no109/2009, of 15 September.

Furthermore, prevention and public awareness is conducted by the National Centre for Cybersecurity (CNC), as well as by other public and private stakeholders.

Law enforcement authorities, such as the GNR and the PSP, carry out prevention and public awareness by means of implementing special community programs, some of which in conjunction with other public entities and the private sector.

It should also be highlighted that national priorities are linked to the strategic goals and operational action plans elaborated for the EU "Cybercrime" Priority.

Conclusion

A number of sections of the strategy (Axis) highlights the national priorities with regards cybercrime, particularly in the area of prevention, legislation, capacity building, training, public awareness and international cooperation.

In particular "institutions concerned with the investigation of cybercrime must be fully equipped to carry out their mission while the judicial system in general must adapt to the new technologies".

In addition these are the two major options of the strategy: the review and update of legislation and the streamline the skills of the PJ (to strengthen its structures and its technical and forensic skills to carry out investigations in the cyberspace).

It is the view of the evaluation team that prompt and adequate resourcing of these elements of the strategy should be a priority for the Portuguese authorities.

3.3. Statistics on cybercrime

3.3.1. Main trends leading to cybercrime

Due to the diversity of this phenomenon, to the fact that it is transversal and to its insusceptibility of being re-directed to criminal typology it is difficult to provide the share of cybercrime in the total criminality picture of Portugal.

Nonetheless, according to the 2013 Report of the Cybercrime Office of the General Prosecutor's Office (PGR), it is possible to perceive this reality and some major trends from the complaints that have been received at the Public Prosecution services.

Portugal identified as an issue the creation of fake profiles on social networks (in particular Facebook), under the name of another person. There is an increasing number of complaints reporting situations in which someone creates a profile under another person's name in order to insult, discredit or disclose facts regarding the private life of another person or designed to degrade another person's image. As a rule, these situations have been considered as slander/libel or alternatively as an invasion of privacy (Article 193 of the Criminal Code) or as an unlawful disclosure of photographs (Article 199(2)(b) of the Criminal Code).

This phenomenon can be considered, in the opinion of the evaluation team, as a threat for the society but it may not be quantified as a cybercrime offence in general terms.

At the same time, complaints against authors of blogs with offensive contents have increased – to which are usually associated comments, from third parties, equally offensive. Just like it happens in the social networks, it has also been reported in the blogs the publication, not authorized, of photographs.

Another main reason of complaint has been fraud related to online shopping. Many complaints have been registered by citizens who buy online objects that are not delivered. These complaints usually appear isolated and scattered throughout several county courts, but they frequently correspond to actions performed by the same individual that uses the same method and means, over and over, towards several victims.

The same happens to fraud related to jobs (on the Internet), the not authorized use of payment cards to buy online and phishing. All these situations have been referred to as emerging. In addition, although less frequent, fraud has been reported in hotel reservations, with the creation of false web hotel pages that accept booking and payment (generally, much cheaper than in other sites). The client of the hotel is only aware of the fraud when he arrives at the hotel and realizes that the booking does not exist. This type of complaints has come up more in touristic areas (in the Algarve region, South of Portugal).

Although out of the concept of cybercrime, but requiring the resort to digital means of evidence, the complaints on the theft of mobile phones have been mentioned as very relevant. This segment of crime encompasses a great "digital" relevance, either by the contents of the phones (for instance, messages, records or personal and private photographs), or as the way to reach the author of the theft.

3.3.2. Number of registered cases of cyber criminality

The official «Statistics of Justice»[8] collects statistical data on cybercrime via two sources:

- Through the law enforcement authorities, in particular in the scope of crimes recorded by these LEAs. In this context, it is collected statistical data on crimes provided for in the Law on Cybercrime (Law no 109/2009, of 15 September) recorded by the LEAs. The body that mostly records this type of crime is the PJ, as the Law on the Organization of the Criminal Investigation allocates to this police exclusive powers for the investigation of this specific crime, as stated before.
- Through the first instance courts which convey to the «Statistics of Justice», by an automatic data transfer procedure, statistical data on criminal cases, completed at trial stage, for crimes provided for in the Law on Cybercrime as well as on defendants and convicted persons for this specific crime.

The collecting of statistical data on crimes recorded by the LEAs and the collecting of judicial statistics are different, both in terms of collection methods and of data sources; it should be highlighted that there is no correspondence between the number of crimes recorded in a year and the number of cases completed at trial stage in that same year, as these cases may relate to crimes recorded in the same year or in previous years and tried only in the upcoming years.

[8] http://www.siej.dgpj.mj.pt/webeis/index.jsp?username=Publico&pgmWindowName=pgmWindow_633918141195530467

The national authorities provided statistics on the number of registered cases, investigations, prosecutions, final convictions, as well as the number of persons investigated, prosecuted for and convicted of cybercrime acts.

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

No dedicated budget allocation for the prevention of and fight against cybercrime is foreseen by the Portuguese authorities. The prevention of and fight against cybercrime is done using the ordinary budget of the PGR and of the LEAs.

Within the PJ, two projects are being co-financed by the EU under the 7th Framework Programme (FP7), namely, CyberROAD – development of the cybercrime and cyberterrorism research roadmap in the amount of 66.018,00 €, and the ECOSSIAN – European Control System Security Incident Analysis Network, in the amount of 334.067,20 €.

The project CyberROAD is aimed at identifying current and future issues in the fight against cyber-crime and cyber-terrorism in order to draw a strategic roadmap for cyber security research. This roadmap (as it is envisaged by the project) will be built through an in-depth analysis of all the technological, social, legal, ethical, political, and economic aspects on which cybercrime and cyber-terrorism are rooted. The research roadmap will be achieved by co-ordinating the efforts of the CyberROAD consortium, which include the along three key directions including technology, society, cybercrime and cyber-terrorism.

The mission of ECOSSIAN is to improve the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures by implementing a pan-European early warning and situational awareness framework with command and control facilities. The consortium consists of international industry wide partners and the PJ.

3.5. Conclusions

Portugal has approved the National Cyberspace Security Strategy as part of a comprehensive plan to reduce weaknesses in the security and information networks and to increase the resilience of critical infrastructure. The core of the strategy is national sovereignty. Ensuring the nation's political and strategic autonomy in addition to the growing awareness of the number of malicious incidents and attacks that mean that the security of cyberspace in Portugal should be considered a national priority.

It is clear that concrete steps have been put in place to ensure the integrity of the cyber domain within Portugal. They include the establishment of the National Centre for Cyber Security. Its structure, powers and operating terms are established by Decree-Law no 3/2012, of 16 January 2015 as amended by Decree-Law no 69/2014, of 9 May 2015.

The strategy states that Portugal confirms its strong commitment to defending cyberspace. Nevertheless, a large part of the technological infrastructure that make up cyberspace is owned by private operators, who are principally responsible for their protection.

It is the opinion of the evaluators that the identification and attribution of responsibility over these interdependencies is one of the most important tasks to be done when implementing this National Cyberspace Security Strategy.

The team noted that there appeared to be no plan or draft plan for implementation of the comprehensive strategy apparent during the visits or no organisation took responsibility for its implementation. The strategy does outline this commitment at Axis 1 section (2b) that "operational coordination is an essential factor in the successful implementation of the measures outlined in this Strategy. The CNCS will oversee the coordination between the various responsible parties".

It is the clear view of the evaluation team that leadership and ownership for the implementation of the strategy needs to be given to one authority with the appropriate powers to draw up an implementation plan and ensure that all element of the plan come into effect as outlined.

An action plan should follow the strategy to clearly outline the method of interaction between national institutions.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecution and courts)

4.1.1. Internal structure

In Portugal, according to the Code of Criminal Procedure the initiative of the investigation and of the criminal action is incumbent on the Public Prosecution Service (Ministério Público), which in this activity is co-assisted by the criminal police bodies.

From among these, and as concerns cybercrime, stands out the PJ which is entrusted, by law, *with the investigation of "computer crimes committed, resorting to computer technology*", as set forth in Article 7(3)(l) of the Law on the Organization of the Criminal Investigation (Law 49/2008, of 27 August, as last amended by Law no 57/2015, of 23 June).

There are specialised structures within the Prosecution Service. At the prosecution level, both in Lisboa and Porto, there are special sections in charge of cybercrime issues. Besides, in most of the judicial districts (*comarcas)*, cybercrime issues are assigned to specialised prosecutors.

Furthermore, at the Prosecutor General's Office there is a coordination body, the Cybercrime Office, entrusted with the national coordination of the Prosecution Service in all matters respecting cybercrime and in the obtaining of digital evidence.

In Portugal, there are 23 first instance courts, located in the existing 23 judicial districts, but such courts do not have special powers related to cybercrimes.

The Cybercrime Office within the PGR has the responsibility to coordinate the State Prosecution Services in all matters in respect to cybercrime and in the obtaining of digital evidence. In addition awareness raising and the facilitation and coordination of training form part of their remit.

The Cybercrime Office has a state-wide remit with a national network of 43 prosecutors covering the 23 judicial districts. Training forms part of the strategy to familiarise prosecutors in digital evidence and cyber awareness. This training is still at a basic level with over 350 prosecutors trained since 2012 and also advanced training was delivered, even if to a smaller number of prosecutors. As part as of the training plan strategy, it was decided to provide to all the prosecutors related to criminal investigations basic training on cybercrime and digital evidence but, aside, it was also decided to provide more advanced training to a smaller number of prosecutors (namely those who are contact points of the Cybercrime Office). Moreover, this is an ongoing process; or even more than an ongoing process, this is a permanent and continuous process of training and update.

In addition there are plans to put in place (under the Cybercrime Action Plan 2015/2016 of the Cybercrime Office), a private database (with no personal data stored) on investigations conducted by prosecutors on fraud offences using communications networks. The information in this database will include data from individual cases, concerning the circumstances of the offenses, the object allegedly transacted, its value, the method of payment, the platform used for fraud, etc.

Inputting will be compulsory having the effect of allowing correlation of cases and suspects across all prosecutors.

The evaluation team is of the view that this is a good practice and will lead to more effective prosecutions and the identification of multiple crime suspects on a state-wide basis.

Prosecutors receive complaints through multiple sources including electronic means. An assessment of cases based on available information is carried out. An informed decision is then made to proceed to further investigation which is delegated in the PJ if the evidence merits it. A physical complaint to the authorities is required as part of the legislative requirement in Portugal.

4.1.2. Capacity and obstacles for successful prosecution

There are not any new measures envisaged to be taken to strengthen the capacity to investigate or prosecute cybercrime.

According to the national authorities no particular obstacles/difficulties in prosecuting and/or obtaining conviction for any specific cybercrime offences have been experienced until now.

As previously outlined it has been acknowledged that most evidence is in the possession of the private sector. There are informal protocols with some service providers which prove effective in the decision making capacity of the Prosecution Service to escalate the investigation to the PJ. Country by country statistics show the effectiveness of these protocols and can be taken as good practice in affecting a quicker response.

On the other hand this practice of cooperation with the private sector is not widespread and the policy of not including the Internet Service Providers in electronic transactions can be seen as an obstacle to successful criminal proceedings.

In particular the availability of a software tool called SAP DOC, introduced in 2008, which may speed up the process. This is acknowledged as an area to be examined in the light of the evaluation process.

4.2. Law enforcement authorities

The competence for the cybercrime investigation is entrusted and reserved to the PJ (Article 7(3)(l) of the Law no 49/2008, of 27 August, on the Organization of the Criminal Investigation).

The structure of the investigation services was recently altered with the setting up of a National Unit for Cybercrime Investigation, which is expected to include and coordinate the investigation of cybercrime, the investigation related to electronic means of payment and child pornography on the Internet, aligning these competences with the priorities established by Europol.

Though the PJ has exclusive jurisdiction to investigate computer crimes or those that are carried out using electronic means, the GNR and the PSP may also apply police measures in order to ensure the maintenance of digital evidence, if authorized to do so by the Prosecutor in charge of the criminal file. These two LEAs have competence and take initiatives on the prevention of cybercrime.

The main obstacles to successful investigation of cybercrimes are related to the obtaining of traffic data.

There is a 24/7 contact point for urgent requests. Such operational 24/7 contact point for permanent international cooperation operates within the PJ. Its main mission is to assist judicial authorities in the investigation, to develop and to promote preventive actions and to detect and investigate serious crime. During the investigations the PJ co-assists the judicial authorities (Article 21 of Law no 109/2009).

From August 2015, the newly formed National Cybercrime Investigation Unit, which has been centralised at a new headquarters of the PJ, coordinate and investigate cybercrime under the direction of the Public Prosecution Service. Regional units have a capability to investigate cybercrime with central support being provided by the National Cybercrime Investigation Unit in Lisboa. These investigations will be related to computer crime in general, child pornography and card fraud.

In respect to card fraud, excellent cooperation exists between the National Cybercrime Investigation Unit - Card Fraud Unit and the banking authorities, in particular with Sociedade Interbancária de Serviços), the Portuguese Interbank Cooperation Society (SIBS).

This cooperation can be seen as a positive element in the fight against card fraud and the means used by SIBS has been noted by the evaluation team as highly sophisticated and effective. 24 hour monitoring of the entire ATM network within all banks is carried out. In addition all cards used at ATMs within Portugal are monitored in addition to Portuguese cards used outside the State with a total of 19 million cards and 13,000 ATMs on the SIBS system.

The centralised approach has been noted by the evaluation team as good practice within the Portuguese banking system in addition to the excellent cooperation with the National Cybercrime Investigation Unit.

4.3. Other authorities/institutions/public-private partnership

Besides judiciary and LEAs responsible involved in the prevention of and fight against cybercrime, the CNCS and other stakeholders referred to in the Strategy, such as the critical infrastructures operators, have responsibilities in prevention of cybercrime.

The Law on the Organisation of the Criminal Investigation provides the competencies among police forces. The leadership and coordination of criminal investigation pertains to the Public Prosecution Service. From the Strategy also results further coordination between all the relevant actors.

Public Private Partnerships forms part of the National Cyberspace Security Strategy. The sharing of good practices with private critical infrastructure operators is a core goal of the strategy. In particular this role is given to the CNCS. A shared incident response reporting mechanism will be developed with the cooperation of the private operators who have the responsibility to ensure security in the critical infrastructure cyber domain.

In addition there is a mandatory reporting system in place under legislation. There is a requirement to notify the National Communications Authority (ANACOM) of any events which threaten the integrity of the designated critical infrastructure and those infrastructures designated under Directive 208/114/EC.

Apart from the legislative requirement outlined above it can be stated that police and judicial authorities cooperate on an ongoing basis with the internet service providers in accessing subscriber information pertaining to cybercrime. This requirement generates large amounts of administration for the ISPs and appears to the evaluation team to be an overly time consuming process in its present form. This may provide an obstacle to the efficient use of the facilities and expertise of the ISPs. The speed and efficiency of this process may be improved by the use of a centralised software tool presently in place but not used to any great extent by the judicial authorities

It is recommended by the evaluation team that the use of this software tool (SAP DOC Software) should be examined in order to make the processing of requests more efficient and acceptable to the ISPs.

Cooperation at a policy level with ISPs in order to leverage obvious and growing private sector expertise in the cyber domain is recommended. This is considered vital and expedient to foster cooperation between law enforcement and judicial authorities and to ensure a coordinated approach to cybercrime throughout the state and internationally. In particular the presence of ISPs outside the State could assist with the speedy resolution of requests to third countries within the parameters of existing legislation.

4.4. Cooperation and coordination at national level

Coordination is led by the Cybercrime Office of the PGR in the area of cybercrime prevention, investigation and awareness raising and training.

From a practical perspective the police (which acts under the direction of the Public Prosecution Service) interact with the national telecommunications regulator (ANACOM) and the National Cyber Security Centre (CERT.PT).

The purpose of CERT.PT is that of improving efficiency in regard to the reaction to cybersecurity incidents in Portugal, by means of facilitating the share of relevant information, coordinating mitigation and resolution actions within the involved several entities, and the remaining national and international authorities.

In the area of Emergency Planning, the Portuguese National Authority for Civil Protection deals with national policy for emergency planning.

4.4.1. Legal or policy obligations

The CNCS, on its turn, is competent in regard to all issues related to national cybersecurity. Its structure, powers and operating terms are established by Decree-Law no 3/2012, of 16 January as last amended by Decree-Law no 69/2014, of 9 May.

Its mission is to contribute to a free, reliable and secure use of the cyberspace in international cooperation, in coordination with all relevant authorities, with the implementation of measures and instruments needed to anticipate, detect, respond and recover from situations that, given the imminence or occurrence of incidents or cyberattacks, jeopardize the operation of critical infrastructures and threaten national interests. Thus, the CNC leads and promotes the:

- Development of national capabilities regarding prevention, monitoring, detection, analysis and reaction to cybersecurity incidents;
- Education and qualification of human resources in cybersecurity issues, in order to enhance the excellence of the scientific community and national awareness; and
- Collaboration among national actors regarding cybersecurity, assuring the national representation among homologous international entities.

It also collaborates in:

- Assuring security among National and Critical Infrastructure's IS and networks;
- Developing technical, scientific and industrial capabilities through R&D projects within the cybersecurity scope;
- Assuring the use of cyberspace in war and crisis scenarios, according to the crisis and emergency national directive; and
- Communicating and informing on the extent of the challenges related to the security of the information systems.

The Directives 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC and 2009/140/EC were transposed in 2011. Law 5/2004, of 10 February (Law on Electronic Communications) which encompasses the legal framework arising from those Directives imposes to the Internet Service Providers (ISPS) the duty to implement prevention and security measures (Articles 54A and 54B).

Directive 2002/58/EC was transposed by Law 41/2004, of 18 August. This Law specifically imposes to the telecommunications sector (ISPS included) the duty to inform administrative entities, such as the national telecommunications regulator (ANACOM – www.anacom.pt) and the Data Protection National Commission (www.cnpd.pt) of network security incidents, mainly, network security breaches and network personal data breaches (article 3A).

The Directive 2006/24/EC of the European Parliament and of the Council, of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, was transposed by Law no 32/2008 of 17 July.

There are no other legal obligations to report cyber-attacks. However, all the civil servants have the obligation to report all crimes, according to Article 242 of the Code of Criminal Procedure. There are some crimes that, once reported to the Public Prosecution Service or to the PJ, are immediately investigated. Regarding other crimes («public crimes») a complaint is not needed in order to be investigated.

PJ, within its prevention powers along with criminal investigation (the latter under the Public Prosecution Service direction), can interact with the national telecommunications regulator (ANACOM) and with the National Cyber Security Centre (CNCS) where the CERT.pt sits. The CNCS can request for IP addresses blockade in case of emergency and severity of attacks. In these situations the telecommunications and ISP operators are supposed to cooperate. For instance, it has been done before, in December 2011, with good results as part of mitigation actions against cyber-attacks (severe DDoS attacks).

Based on EMPACT MASP OAPs (EMPACT multi annual strategic planning operational action plans) Portugal successfully accomplished a common taxonomy proposal to enhance cooperation among main actors, namely, LEAs, EC3 in Europol, CERT community and private sector in general, within Member States.

In a detailed manner, in emergency planning matters, the Portuguese National Authority for Civil Protection pursues the following activities:

• Contributes to the definition of the national policy for emergency planning, elaborates general guidelines, promotes the elaboration of studies and emergency plans and facilitates technical support and issues opinions on its elaboration by sector-specific entities;
• Assures the articulation of the public or private services performing missions related with emergency planning, namely in the areas of transportation, energy, agriculture, fishing, food, industry and communications, so that, in the event of a serious accident or disaster, the continuity of governmental actions, protection of the population and the safeguard of the national patrimony can be guaranteed.

The Portuguese Strategy to Secure Cyberspace defines the National Cybersecurity Centre (CNCS) as the operational coordinator and national authority for CI operators and State institutions. The same strategy foresees a Cyberspace Crises Management Cabinet to be established. CNCS has also the responsibility for Civil Emergency Planning for Cyberspace and for setting up a shared situational awareness scenario with other authorities.

It should also be referred that in Portugal there is a network of CSIRT (Computer Incident Response Team) in different areas of industry (Financial, Telecommunications, Energy, etc.). The main function of this Centre takes place at the level of alert and cyber incident response and crisis management with other players at a mainly technical level. At the level of cyber operations there is the national centre of cyber-defence.

There is a close cooperation among European banking supervisors, the European Central Bank (Secure Pay Forum) and the European Banking Authority (EBA) regarding the prevention of online (card) fraud.

Regarding this matter, the cooperation between the financial industry and the LEAs is carried out together with the National Unit against Corruption of the PJ (UNCC), which also deals with economic and financial crime.

As to the security of non-cash payment and minimize the vulnerability of magnetic stripes, it is achieved through the Prevention Service of UNCC and privileged contacts with this Unit.

In what concerns the strengthening of the authorisation of online transactions and authentication of customers, such authorizations are processed by the banks and, in particular, by SIBS.

The exchange of information between SIBS and the LEAs is frequent and covers operational matters such as notifications and preventive measures so as to strengthen the authorizations, be it in the context of Card Present or Card Not Present.

ANACOM, both in the context of the legal framework of the Electronic Communications Law and in accordance with its Statute, has among its roles the promotion of technical standardization in the electronic communications sector and related areas, in particular in collaboration with other organizations.

In this context, ANACOM promotes the debate on the standardization of work in the area of security of information systems, in specific in what regards electronic communications by involving sector representatives (please see http://www.anacom.pt/render.jsp?categoryId=382834#.Vh_EvemFO71).

ANACOM's initiative to promote the discussion of legal, technological perspectives and management for the development of guidelines on investigation and interpretation methods of digital evidence should be highlighted (please see http://www.anacom.pt/render.jsp?contentId=1349045#.Vh_Fk-mFO71).

ISPs, even if they are not under a legal obligation, are members of CERT.PT (http://fe02.cert.pt/index.php/rede-nacional-csirt/directorio), a service of CNCS.

4.4.2. Resources allocated to improve cooperation

No additional resources appear to be allocated to improve cooperation but the National Cyber Security Strategy states that it is essential to invest and strengthening this area.

4.5. Conclusions

- In 2011, the Cybercrime Office was established at the PGR of Portugal. The prosecutors within the Cybercrime Office are responsible for informal cooperation with international providers (namely, via informal agreement, with the purpose of obtaining evidence within criminal investigations) and information exchange, as well as for training of other prosecutors and general monitoring activities across country. The Cybercrime Office is also responsible for an overall coordination of prosecution as such, in order to avoid different solutions in similar situations. To ensure maximum coordination, a national network of 42 prosecutors who specialise in cybercrime cases is in place.
- Nevertheless, the all process of formal international cooperation is not a responsibility of the Cybercrime Office – if a MLA request is needed in the course of an investigation, regular channels are used. The regular channel is the International Cooperation Unit), within the General Prosecutor's Office.

- One LEA deal with cybercrime issues in Portugal: (1) PJ under the Ministry of Justice, which is a part of crime investigation system. However, other law enforcement authorities (not only GNR) can deal with the so called "traditional crimes", if committed with use or by the means of a computer system (such as, for example, frauds on the Internet, or defamations in a blog, or threats via email, among others).
- National Cybercrime Investigation Unit was established recently, on 23August 2015, within the PJ. In line with the European priorities in the field of fight against cybercrime, three sub-divisions are envisaged as constituent parts of the National Cybercrime Investigation Unit:
  - Sub-division on Cyber-attacks;
  - Sub-division on Paedophilia and Crimes against Persons;
  - Sub-division on Payment Card Fraud (still belongs to the National Anti-Corruption Unit, however will be moved to National Cybercrime Investigation Unit in the near future).
- There are also capacities to investigate cybercrime within regional units. However, main competences are concentrated at National Cybercrime Investigation Unit.
- National Cybersecurity Centre was established in 2015. It functions as a national CERT, as well as provides on-site support for State organisations mitigating high-level cyber threats. The Centre has monitoring capabilities of Portuguese Internet segment, releases situation awareness reports.
- It also cooperates with law enforcement authorities. One of the outcomes of such cooperation between CERT-PT and Portuguese PJ is the Proposal for a Common Taxonomy for the National Network of CSIRTs, elaborated within the framework of EMPACT priority "Cyberattacks". However, it is not clear what are the criteria of reporting information gathered by CERT-PT to Portuguese law enforcement.

The GNR and the PSP under the Ministry of the Interior deals with cybercrime prevention (illegal use of Internet) and awareness raising issues in Portugal. GNR is involved in an initiative that aims to alert the public to the need to adopt safe behavior online. The action, called "Internet Segura" took place in 200 schools all over the country and deals with the issue of privacy, the risks associated to the use of internet, including cyberbullying, identity theft, the inaccuracies of information sources, computer viruses and dependence.

These police forces can deal also with the so called "traditional crimes", if committed with use or by the means of a computer system (such as, for example, frauds on the Internet, or defamations in a blog, or threats via email, among other). In fact, if cybercrime is considered *lato sensu*, all police corporations have to deal with it.

- The Interbank Cooperation Society (SIBS) is responsible for processing the transactions made using payment cards, as well as ATMs and cooperates closely with Portuguese law enforcement agencies in order to prevent and investigate payment-related fraud. Cooperation between SIBS and law enforcement agencies is ensured not only at national, but at international level as well. SIBS contributed greatly to the elaboration of the ATM Malware prevention guide, which was created by Europol in cooperation with private industry.
- APRITEL – Association of Electronic Telecommunications Sector in Portugal. This Association represents member businesses and enterprise from Internet and Telecommunication sectors. During the meeting with the evaluation team representatives from the telecommunication sector stressed that cooperation between the private sector and the law enforcement could be improved.
- In particular, regarding usage of electronic request system for IP data that was created in 2009. It has been stated by ISP representatives that this system has not been used to date. Representatives of APRITEL and national ISPs also presented current initiatives on crime prevention on the Internet, in particular blocking of websites related to piracy of intellectual property (complaint-based DNS blocking), blocking of known child sexual abuse material using "NetClean Cloud" solution, as well as participation in cybercrime prevention programmes for children at schools (in cooperation with law enforcement agencies).
- Representatives of Portuguese authorities mentioned that the national coordination body exists and is lead by General Prosecutor's Office.

- The national strategy document acknowledges that a large part of the technological infrastructure that make up cyberspace are owned by private operators. Whether this is telecommunications, banking, social media multinationals or other internationally owned business infrastructure.
- The inclusion of industry wide forums to test the willingness of the private sector to play the good citizen in providing resources, technological knowhow and innovative techniques to the judicial authorities and law enforcement authorities could be taken into consideration by the Portuguese Authorities in developing future strategies.
- The evaluation team were privy to this willingness in their meeting with representative of the ISP's. In particular the ISP community and banking areas who have resources that may be provided in order to assist in dealing with cyber related crime and awareness raising. There was evidence of a willingness to cooperate in this area.
- The use of this software tool (SAP DOC) should be considered in order to make the processing of request to the ISP's more efficient.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to Cybercrime

5.1.1. Council of Europe Convention on Cybercrime

Portugal is Party to the CoE Convention on Cybercrime since 2009 and it's additional Protocol since 2010.

The Convention was internally approved by the Resolution of Assembly of the Republic no 88/2009 and ratified by the Decree of the President of the Republic 91/2009, both published in the Official Journal, *I Series*, of 15 September 2009.

The mentioned Law no109/2009, of 15 September, was adopted in order to fully comply with the obligation arising from CoE Convention on Cybercrime.

5.1.2. Description of national legislation

Legal persons and other legal entities are criminally liable for the crimes provided for in Law 109/2009 (Article 9).

On its turn, Article 11 of the Criminal Code (liability of legal persons) establishes that legal persons and analogous entities (except for the State, other legal persons exercising public powers and public international law organizations) are liable for crimes, when committed on their behalf and in their collective interest by persons who have a leading position therein or by whoever acts under the authority of the persons previously referred to, by virtue of a breach of the supervision or control duties incumbent upon them.

The Portuguese legislation provides for specific criteria. For instance, Article 5 of Law 109/2009 describes aggravating circumstances to the crime of computer sabotage (or system interference):

4 - The penalty will be imprisonment of 1 to 5 years if the damage arising from disturbance is of high value.

5 - The penalty will be imprisonment of 1 to 10 years if:

a) damage arising from disturbance is of a considerably high value;

b) the disturbance reaches seriously a computer system that supports an activity designed to provide critical social functions, including supplying chains, health, safety and economic well-being of persons, or the regular functioning of public services.

- There are no particular provisions on minor cases related to cybercrime. The Portuguese Public Prosecution Service is bound by principle of legality but in minor cases related to cybercrime, prosecutions can be stopped / postponed.

Regarding the Directive 2013/40/EU on attacks against information systems the national authorities specified that when the aforementioned Directive was issued, the Law 109/2009 was already in force. The provisions of this Law fulfil the obligations of result of the Directive. Therefore, Portugal fully complies with the Directive and duly notified that to the European Commission. No special difficulties in implementation were verified.

The Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography was transposed by Law no103/2015, of 24 of August.

5.2. Procedural issues

5.2.1. Investigative Techniques

All the mentioned investigative techniques are allowed under Portuguese law, being explicitly established as follows:

Investigative techniques	Portuguese law provisions
Search and seizure of information system/computer data	Article 15, 16 and 17 of Law no109/2009
real-time interception/collection of traffic/content data	Article 18 of Law no109/2009 (which refers to the legal regime on telephone interceptions on the Code of Criminal Procedure)
preservation of computer data	Article 12 of Law no 109/2009, to be read in conjunction with the provisions set forth in Law no 32/2008, of 17 July, related to data retention, generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and the provisions of Law no 46/2012, of 29 of August, Law on Data Protection and on the Privacy in Telecommunications.
order for stored traffic/content data;	Article 13 of Law no 109/2009, Code of Criminal Procedure, Law no 32/2008, of 17 July, Law no 46/2012, of 29 of August.
order for user information.	Article 14 of Law no 109/2009 and the Code of Criminal Procedure.

The most commonly used special investigative techniques are interception of communications and covert actions are foreseen in Law no 109/2009, in Law no 101/2001and in the Code of Criminal Procedure.

The methodology of investigation, namely in the framework of intrusion attacks and defacement of sites, faced a great evolution in the approach to the investigation in the more recent years.
This methodology has been frequently used and, with the collaboration with the private sector operators, lead to several detentions in the framework of ongoing criminal procedures.

5.2.2. Forensics and Encryption

Article 15(5) of the Cybercrime Law (Law no 109/2009, from 15 September), foresees, among other, the possibility of extending computer searches to remote systems – this includes remote examinations of a computer system. On the other side, Article 19(2) of the Cybercrime Law allows the use of specific software to obtain evidence, in the context of an under covered operation in the networks.

5.2.3. e-Evidence

Article 2 of the Law no 109/2009 contains a list of definitions for following notions: computer data, content data, traffic data, order for search/seizure of information system, networks managed or controlled by suspects of cybercrime.

There are no specific rules regarding the admissibility of e-evidence. General rules on the admissibility of evidence are stipulated in the Code of Criminal Procedure. In specific cases related to the obtaining of evidence outside the European Union (EU), Portuguese law provides for legal international cooperation mechanisms in criminal matters (Article 25 of Law no 109/2009). Once the evidence is obtained, it is up to the court to decide upon its admissibility in accordance with the mentioned rules of the Code of Criminal Procedure.

5.3. Protection of Human Rights/Fundamental Freedoms

The Constitution of the Portuguese Republic (CRP) explicitly establishes a protection regime on fundamental rights, freedoms and guarantees, which constitute the cornerstones of the overall of the Portuguese legal system. Such principles, fundamental rights, freedoms and guarantees are also foreseen at the ordinary law level, in particular in what concerns cybercrime, in the Criminal Code, the Code of Criminal Procedure and in the Law 67/98, of 26 October, on Personal Data Protection.

Criminal investigation connected to cybercrime faces the difficulties inherent to the protection of the citizens´ privacy, who have the right of having their rights, freedoms and guarantees protected. The Constitution of the Portuguese Republic, in its Article 29, enshrines the main criminal law principles.

In what specifically concerns cybercrimes, Article 18 of Law no 109/2008 contains provisions allowing for certain restrictions to privacy and, thus, in such a measure, to rights, freedoms and guarantees.

Also, whenever such cybercrimes are carried out in an organized manner and/or connected to terrorist offences, Articles 143(4), 174(5) (a) and 177(2) (a) of the Code of Criminal Procedure foresee restrictions of certain of such rights, freedoms and guarantees.

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of Cybercrime

Article 27 of Law no 109/2009 provides for particular rules on jurisdiction in addition to the general provisions of the Criminal Code regarding jurisdiction, i.e., unless there is a contrary disposition on a treaty or international agreement, the Portuguese criminal law is applicable to the facts:

- Committed by Portuguese nationals, if, to the case, is not applicable the criminal law of any other State;

- Committed in the benefit of legal persons established in Portuguese territory;
- Physically committed within Portuguese territory, even if they aimed to reach computer systems located outside that territory, or
- That aimed computer systems located within Portuguese territory, regardless of where those facts were physically committed.

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

Still according to Article 27 of Law no 109/2009, if due to the applicability of Portuguese criminal law, it is established simultaneous jurisdiction by the courts of Portugal and the courts of any other Member State of the EU, being legally admissible in both of them the prosecution of the same facts, the competent judicial authority requests the bodies and mechanisms established within the EU (vg. Eurojust) to facilitate cooperation between judicial authorities of the Member States to coordinate their actions in order to decide which of the two States initiates or continues the prosecution regarding the perpetrator of the offense in order to concentrate it in one of them.

Besides, the decision to accept or to transmit a procedure is taken by the competent judicial authority, taking into account successively the following: a) the location where the crime occurred; b) the nationality of the perpetrator, and c) the location where the perpetrator was found.

Until now there was no need to resort to the provisions related to the Council Framework Decision 2009/948/JHA of 30 November 2009.

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

Until now no specific problems have been detected.

5.4.4. Perception of Portugal with regard to legal framework to combat Cybercrime

The existing legal framework for investigation and prosecution of cybercrime is sufficient. Nevertheless, there is always room to improvement and, as mentioned, the novelties implied in this field led to recognize in the Strategy those specificity and need. Moreover, whenever a cybercrime is committed outside national territory, the difficulties that may arise are those experienced by all law enforcement and prosecution authorities.

5.5. Conclusions

- In Law no 109/2009, Portugal implemented legislation on attacks against information systems and the rules and principles of the Convention on Cybercrime of the Council of Europe (Budapest Convention). Legal persons and other legal entities are criminally liable for the cybercrimes committed under their supervision.
- For the purpose of cybercrime investigation Portuguese competent authorities can also use special investigative techniques such as interception of communications and covert actions foreseen in Law 109/2009, in Law no 101/2001, of 25 August, and in Code of Criminal Procedure. These techniques must be ordered by competent judge (Juíz de Instrução Criminal). This ensures that fundamental rights are well protected when tackling cybercrime.
- According to national legislation, "the policeware" software tool could not be used for cybercrime investigations, while it is stated that it can be used for other serious crimes, such as drugs trafficking, etc.
- The Portuguese Public Prosecution Service is bound by principle of legality but in minor cases related to cybercrime, prosecutions can be stopped / postponed.

- In Article 16 of Law no 109/2009 is stated that e-evidence must be collected, stored and transferred to the Public Prosecutor or the court to be used in a trial. There are no specific provisions in Portuguese law regarding the admissibility of e-evidence. General rules on the admissibility of evidence are stated in the Code of Criminal Procedure. With respect to the admissibility of evidence gathered outside the territory of Portugal, the Public Prosecution Service currently sees no problem with regard to this.
- In respect to the admissibility of evidence gathered in Portugal or in other EU member States or third States, it was stated that the admissibility in court has not been challenged to date.
- Nowadays data traffic retention is an important issue because Portugal transposed the Directive 2006/24/CE, which was invalidated by the ECJ Decision of 8 April 2014 (case C-293/12).

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1. Nature of cyber attacks

Since 2011 a significant number of cyber-attacks occurred in Portugal. They were mainly "DDoS attacks", "defacing attacks" and data exfiltration by the method of "SQL injection".

These activities are usually linked to "hacktivism" and have additional echoes on social network platforms.

As lessons learned, national authorities still notice the critical dependency of data traffic, all from third parties and rarely from MS. Data traffic preservation is a serious issue for LEAs criminal prevention and investigation entities.

The data on abuse of information and incidents regarding Portuguese Cyberspace are as follows:

Abuse information regarding Portuguese Cyberspace (May to September 2015)	
Abusive Content	145
Fraud	6371
Information Gathering	19
Intrusions Attempts	2753
Intrusions	34908
Malicious Code	598679
Other	5311

Source: CNCS

Incidents for Portuguese Cyberspace (May to September 2015)	
Abusive Content	1
Availability	11
Fraud	17
Information Security	1
Information Gathering	51
Intrusion Attempt	4
Intrusion	6
Malicious Code	42

Source: CNC

6.1.2. Mechanism to respond to cyber attacks

There is a coordinated multidisciplinary mechanism to respond to a serious cyber attack in the national context. The PJ in cooperation and direction of the Public Prosecution Service interact at a national level with the national telecommunications regulator and with the National Cyber Security Centre and CERT.pt. The Cyber Security Centre has the authority to block IP addresses in cases where an emergency response is required based on a severe national incident. The cooperation of the ISP operators is expected. There is precedence for such action in that in December 2011, action against cyber-attacks (severe DDoS attacks) was accomplished.

Inside the EU territory, the cooperation mechanisms (police and/or judicial) are becoming stronger and easier to use on a daily basis.

MLA instruments are often used in critical aspects of cooperation, in particular, for obtaining information regarding personal data, financial data and other private information. Since data traffic is mandatory to the investigation of this specific crime, the length of time taken to respond to MLA requests is one major obstacle.

In practice, the absence of due response from the USA towards certain crimes and the absence of legal efficient contacts in China and Russia created difficulties to the criminal investigation.

6.2 Actions against childpornography and sexual abuse online

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

Portugal has not any software databases specifically designed to identify victims.

The only measure adopted until now for this effect is the placing in the ICSE database so as to include them as already known images and make it easier for another Member State to get to the origin/production, in case such is unknown.

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

Alerts on the PJ official webpage and press releases in order to promote safe behaviours online have been put in place.

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

The PJ is training on how to fight against this kind of conduct. An international prevention action, in 2014, against child sex tourism, was attended.

There is an open hotline (member of *inhope*) and a telephone help line 24/7.

Furthermore, prevention activities in schools, participation in public debates as well as awareness raising during the "Safer Internet Day" and alerts on the PJ official webpage have been carried out.

6.2.4 Actors and measures countering websites containing or disseminating child pornography

It is stated that all the webpages containing or disseminating child pornography are blocked, removed and taken down, in accordance with the law. ANACOM, in its "quality central supervising authority", has the power of to order the blockage of access and/or removal of webpages, as foreseen in Law 46/2012, of 29 August (Law on Electronic Commerce).

Some ISPs are members of *Internet Watch Foundation* (IWF) and use the list of that entity to block the sites identified as having child pornographic contents. The ISPs also disseminate recommendations on security and prevention regarding the: (i) use of equipment for Internet access; (2) the use of the Internet by minors; and (iii) the type of contents addressed to minors (such as social networks, inappropriate or offensive language/images); which are published in their Websites

The blocking of access or removal of content is authorised by Criminal Instruction Judges (Juiz de Instrução Criminal), or by the Public Prosecutor in charge of the case and the LEAs, with the subsequent validation of the said Judge.

The urgent situations communicated to the PJ impose, in the scope of injunctions and of police measures, the collection and preservation of all data, at request of third parties (in the case of a telecommunications operator, through the Criminal Instruction Judge), the blockage and the subsequent validation of such blockage by the competent authority (the said Judge).

In addition, the competent authorities above mentioned issue an order on the blockage of access and/or removal of contents and the taken down of webpages, notifying the ISPs to fulfil with this order.

International cooperation is used, by activating the prevention 24/7 contact point or the Interpol service or yet through an international letter of request.

6.3 Online card fraud

6.3.1.Online reporting

Although Banco de Portugal does not have any data about the number of citizens and private companies who usually report online card fraud offences to LEAs, it should be highlighted that, in complaints analysed by this Central Bank, bank customers usually mention the report of fraud situation to LEAs.

The Interbank Cooperation Society (SIBS) works in close cooperation with the PJ and the report of any relevant online card fraud offence is immediately exchanged between them.

6.3.2 Role of the private sector

There is a close cooperation among European banking supervisors, the European Central Bank (Secure Pay Forum) and the European Banking Authority (EBA) regarding the prevention of online (card) fraud.

In this context, it should be noted that the EBA issued Guidelines on the security of internet payments in the end of 2014 (please see EBA/GL/2014/12_Rev1, available in https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29.pdf/f27bf266-580a-4ad0-aaec-59ce52286af0).

These Guidelines aim to improve the security of online payments (including through a payment card) and mitigate the risk of fraud in this field.

In particular, the EBA Guidelines provide that payment service providers should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, and establish a procedure for reporting incidents to management and, in the event of major payment security incidents, the competent authorities.

Regarding the authorisation of online transactions and the authentication of customers, they embrace the 'strong customer authentication' procedure. According to the Guidelines, it is "a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e., the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet". Thus, the EBA Guidelines establish that the initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication.

Finally, it should be mentioned the development of self-regulatory initiatives by the industry to mitigate security risks associated with card transactions, such as the EMV (technical standard) and the 3D-Secure (protocol).

The Guidelines entered into force in August of 2015 and the Banco de Portugal, as Central Bank, is the competent authority to ensure its enforcement in the Portuguese jurisdiction (Circular Letter. 55/2015/DSP).

Regarding this matter, the cooperation between the financial industry and the LEAs is carried out together with the National Unit against Corruption of the PJ (UNCC), which also deals with economic and financial crime in general.

As to the security of non-cash payment and minimize the vulnerability of magnetic stripes, it is achieved through the Prevention Service of UNCC and privileged contacts with the Unit.

In what concerns the strengthen of the authorisation of online transactions and authentication of customers, such authorizations are processed by the banks and, in particular, by SIBS.

The exchange of information between SIBS and the LEAs is frequent and covers operational matters such as notifications and preventive measures so as to strengthen the authorizations, be it in the context of Card Present or Card Not Present.

6.4 Other cybercrime phenomena

Examinations are carried out by the Technological Support Unit within PJ and sometimes by SIBS; at the IT Unit, direct examinations and reading of card bands are made, being considered sufficient the equipment in place.

The training is carried out mainly at the IT Unit, where the equipment that is being seized is shown and where those that are identified and which come through Europol/EAST and others are disclosed.

The concrete measures to avoid access of organized criminal groups to financial data and credentials are taken by the services responsible for the detection of bank fraud SIBS/FPS, by banks and through formal or informal training given to the intervening parties on the detection and investigation of card fraud, in which the PJ is actively collaborates.

As regards the skimming devises and software that are planted in the ATMs or POS, these are mostly signalled by SIBS that contacts the PJ and in particular the SCIMF/2nd Unit which, on the site, verifies whether these devises are planted, resorting to the experience that the Unit already has in this matter.

In what respects the know-how, numerous initiatives are being undertaken, aligned with the various PCI standards, such as the International Payment Scheme requirements or regulations from the European Banking Authority or stemming from the Payment Services Directive. SIBS is mandatorily audited annually by several entities.

The Central Bank, the ISPs, *etc*., all review and certify the measures and actions to guarantee full compliance with the norms that are applicable and with effective measures to combat cybercrime.

The PJ know-how, as aforesaid, is obtained through training carried out by CEPOL, EUROPOL, EPE, SIBS and in particular by the IT Unit, where all information that is possible to get from the various partners is stored. SIBS is present in several European Forums, such as the EPC fraud prevention and security committees and the European ATM Security Team. These groups share online card fraud intelligence on a regular basis.

The obstacles found are overcome by the PJ through the use of Interpol National Cabinet and the National Europol Unit channels, the participation in JITs coordinated by Europol and by the involvement in Eurojust. Sometimes, there are privileged contacts in several Member States and direct contacts with some private entities frequently occurs.

6.5. Conclusions

- The PJ is responsible for investigations related to cybercrime and child sexual abuse on the Internet. Additionally, regional units responsible for these investigations operate at 4 central departments and 8 regional units.
- PJ officers may carry out undercover operations on the Internet with the authorization of a court order issued by a Judge (Juiz de Instrução Criminal). These operations are conducted extensively on TOR and P2P networks in order to collect evidence on child sexual abuse.
- Portuguese law enforcement authorities actively took part in international operation "Haven", organised within the framework of the EMPACT project. During the action days, a number of checks have been carried out at the airports.
- According to the statistics on child pornography investigations that has been presented during the visit, over 250 investigations were started in 2014. However approximately one fifth of them lead to prosecutions.
- There is no national database on child sexual abuse material in Portugal. However, the National Cybercrime Investigation Unit within the PJ has direct access to Interpol ICSE data base. Police investigators can upload child sexual abuse material to the ICSE data base and no prosecutor's permission is needed in order to do this.
- The General Prosecutor's Office receives reports of eventual criminal facts from NCMEC - National Centre for Missing and Exploited Children - via the local office of Department of Homeland Security.

-
- The Unit responsible for payment card fraud is currently located at National Anti-Corruption Unit. However, it should be moved to the National Cybercrime Investigation Unit shortly. Units responsible for these investigations exist also at 4 central departments and 8 regional units of the PJ.
- This Unit is dealing with the following wide spread offences: card skimming, shimming, ATM infection using malware and jackpotting, card-not-present fraud, carding sites, various money mule activities.

  At the moment, each complaint filed to the law enforcement electronically still has to be signed physically. There is no system in place that would allow signing complaints with digital signature.

- It appears that there is a lack of cooperation between law enforcement authorities and the private sector in terms of obtaining traffic data in a timely manner. Representatives of Portuguese law enforcement (PJ) indicated that standard period for obtaining IP data from local ISPs is two to three weeks, which is not efficient enough considering the sensitive and fragile nature of electronic evidence.
- On the other hand, great cooperation between law enforcement authorities (PJ)and SIBS takes place with regard to investigation and prevention of payment fraud.

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

There are no formal requirements or specific procedures foreseen by national law in respect of the cooperation between Portuguese national authorities and Europol/EC3, Eurojust, ENISA, in relation to cybercrime cases.

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

Portugal has not had yet experience of cooperation in a concrete case with Europol/EC3, Eurojust, ENISA but national authorities participated in joint action days within the EMPACT framework on in the development of best practices with Europol.

All Portuguese authorities are aware of the existence of Europol/EC3, Eurojust and ENISA and of their added value.

As to the PJ, the creation of JITs as well as the so-called J-CAT hosted by Europol are particularly important. The same reasoning is made in regard to the EMPACT projects, which cover child sexual exploitation, cyber attacks and payment card fraud.

The national authorities are of the opinion that JITs should be incentivized and procedures to make part of them should be simplified.

7.1.3. Operational performance of JITS and cyber patrols

Portugal has no experience in JITS and cyber patrols until now.

7.2. Cooperation between the Portuguese authorities and Interpol

PJ has experience in using the International Child Sexual Exploitation Data Base at Interpol. Also the PJ participates regularly in Interpol working groups on cybercrime since 1999.

7.3. Cooperation with third states

Portugal has no experience in cooperation with third countries but General Prosecutor' Office cooperates directly with the ISPs located in third countries.

7.4. Cooperation with the private sector

ANACOM has hosted a workshop on "Cybersecurity: economic aspects", organized in partnership with Directorate General for Economic Activities, which took place on September 30, 2013 (please see http://www.anacom.pt/render.jsp?contentId=1169370&languageId=1#.Vh_GR-mFO70) and which involved representatives from the private sector.

The Law no 7/2004, of 7 January, on the electronic commerce legislation, similarly to what is provided for in the Directive 2000/31/EC, establishes a liability framework for the Web service providers, according to each of the activities that they pursue: simple transportation, intermediary or main storage (Articles 14 to 16).

Moreover, the Web service providers must promptly comply with decisions on prevention or termination of illicit actions, such as those to remove or hinder the access to a given information.

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

Portugal has a general basis for international judicial cooperation in criminal matters, the Law nr 144/99 of 31 August. Articles 20 to 26 and 145 *et seq* of the said Law set forth specific rules for international cooperation applicable to the cybercrime investigations but also to other types of investigations.

Moreover, Articles 20 to 26 of Law no 109/2009, of 15, September address specifically requisites for international cooperation related to investigations on cybercrime.

Requests for MLA are directly received or sent by the national judiciary competent authorities. Whenever direct cooperation is not accepted, the General Prosecutors' Office (International Cooperation Unit), as central authority for the international judicial cooperation in criminal matters, receives and /or transmits such requests. Decisions are taken by the competent authority (Article 146 of Law no 144/99). Additional information may be requested or provided in the same manner and by using the same channels of communication.

There are no available statistics on requests sent or received concerning investigations on cybercrime.

MLA requests related to cybercrime follow the same legal conditions as all the other requests. The Law states that these requests must be dealt with urgency, but no data on the average time of execution is available.

The most common reason for MLA requests is to obtain information on IP users.

Portugal has developed several protocols to obtain cooperation from the providers that somehow alleviate the burden of traditional MLA; however, in case there is the need of an interlocutor, the European Judicial Network contact points or EUROJUST may facilitate the contacts.

Until the moment no specific problems in providing/requesting MLA assistance have been encountered.

MLA (and international judicial cooperation in general) shall be carried out in accordance with the provisions of the international treaties, conventions and agreements that bind the Portuguese State and, where such provisions are non-existent or do not suffice the provisions of mentioned Law nr 144/99. According to Article 4 of the same Law international cooperation could be provided based on reciprocity.

Inside the EU territory, the cooperation mechanisms (police and/or judicial) are becoming stronger and easier to use on a daily basis.

MLA instruments are often used in critical aspects of cooperation, in particular, for obtaining information regarding personal data, financial data and other private information. Since data traffic is mandatory to the investigation of this specific crime, the length of time taken to respond to MLA requests is one major obstacle.

In practice, the absence of due response from the USA towards certain crimes and the absence of legal efficient contacts in China and Russia created difficulties to the criminal investigation.

7.5.2. Mutual recognition instruments

Portugal has not used any of the EU mutual recognition instruments in relation to prevention, investigation and prosecution of cybercrimes.

7.5.3. Surrender/Extradition

All cybercrime acts are both extraditable or give rise to surrender since they are all punishable with at least 12 months of imprisonment. The offence cybercrime is included in the list of Article 2 of Law no 65/2003, of 23 August 23 on the EAW.

In cases of EAW, competent issuing authorities are the local Courts/Prosecutors; foreign EAWs will be executed by the existing five Courts of Appeal. Direct communication between competent authorities, by several channels (SIRENE, Interpol, directly through fax or email) is accepted.

For traditional extradition, requests will be received or sent by the Central Authority (PGR). As requested State, the final decision on extradition is preceded by an administrative decision on the admissibility of the request taken by the Minister of Justice, being subsequently taken by a judicial authority, in case one of the Courts of Appeal, that can be appealed to the Supreme Court and the Constitutional Court. As requesting State, the Prosecutor General of the Republic requests the extradition, in the use of a competence that is generally delegated to him/her by the Minister of Justice.

From 2012 onwards, Portugal did not send nor received requests for extradition or surrender based on cyber criminality.

All requests for extradition/surrender are by Law classified as urgent and when a person is provisionally arrested – which can be considered as the rule – procedures are very limited in time.

On traditional extradition, where appeals to the Supreme Court of Justice and the Constitutional Court have been presented, the whole procedure takes no longer than 11 months; in the case of the EAW, the average surrender time, in case of no consent from the suspect, is 40 days. When he/she consents, this delay comes down to 15 days.

Portugal sent a couple of requests to third countries (Nigeria, Burkina Faso), but due to the existence of the international Law that allows for cooperation based on mere reciprocity no international instrument has been involved. These requests were never responded. Portugal did not receive requests related with cybercrime from third countries.

7.6. Conclusions

- PJ cooperates actively with Europol EC3 and are members of FP CYBORG, TWINS and TERMINAL. Cooperation within the framework of EMPACT priorities on cybercrime also takes place. PJ also actively participates in actions within the framework of EMPACT Cyberattacks OAP for 2015/2016.
- When a prosecutor, from any court in the country, needs to ask information to ISPs based in third countries, namely fro the United States - Facebook Inc., Google Inc. and Microsoft Corporation - the request will be directly sent from the prosecutor to the ISP.
- There is a bilingual standardized request form elaborated in order to avoid translation issues. Only basic subscriber information and traffic data can be obtained directly from ISPs of third countries.
- No important obstacles were highlighted and in Portugal there are special provisions that regulate international cooperation on cybercrime as stated in Articles 20 to 26 and 145 *et seq* of Law no 144/99. International cooperation goes through MLA requests and is facilitated by 24/7 contact points.

- For EU Member States Europol, Eurojust and EJN are the channels used in order to obtain fast responses and there are no specific requirements or specific procedures foreseen by Portuguese national law in respect of the cooperation between their authorities and Eurojust, Europol, ENISA, in relation to cybercrime cases. Eurojust is involved in relation to most serious crime.
- The competent national authorities are encouraged to send MLA requests directly to another EU Member State. When direct cooperation is not accepted or if there are any difficulties then the Prosecutor General's Office (International Cooperation Unit), as the central authority for international cooperation, facilitates the execution of such requests.
- Interpol channels and databases are also used by the PJ.
- Difficulties regarding cooperation was reported in relation to Russia and China because of the absence of legal efficient contacts. In regard with cooperation with USA difficult cooperation was reported because of the absence of due response towards certain crimes. Regarding the requests that Portugal send to third countries (Nigeria, Burkina Faso) these requests were never responded.
- Portugal did not receive requests related with cybercrime from third countries.
- Law enforcement authorities and prosecutors are well aware of Eurojust and Europol. Portuguese representatives at Eurojust are participating in training of prosecutors. Law enforcement authorities participate in the activities carried out by all 3 Focal Points at Europol dealing with cybercrime issues.
- During the visit the national authorities stated to the evaluation team that so far one JIT was signed and facilitated with support from Europol. This JIT was considered by the prosecution service and by the PJ as a very useful tool in the fight against cybercrime. The facilitation of Eurojust and Europol (EC3) in the fight against cybercrime is considered beneficial and helpful.
- Europol has been involved in concrete cases and information is exchanged via the corresponding channels (SIENA). Portugal is not a member of J-CAT.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

General education and training programs on cybercrime are given to the staff of the LEAs and to magistrates (Judges and Public Prosecutors).

It is important to refer that, within the Prosecutor General Office, an action plan on cybercrime was adopted to be executed from October 2015 to July 2016. This plan includes, *inter alia*, training of prosecutors, envisaging those prosecutors all over the country that are in charge of criminal investigations.

In this context, whenever possible, specific training is equally targeted to the special units of LEAs dedicated to cybercrime investigations, especially in the area of e-evidence.

The Criminal Police School has training modules on cybercrime investigation and on collection and preservation of e-evidence.

At international level, the Portuguese LEAs receive training provided by the quoted bodies/entities, particularly from CEPOL.

In general, cybercrime is not the object *per se* of the Universities curricula, the matter is studied within other disciplines, mainly in what concerns Faculties of Law, within criminal law.

Most of the Portuguese Universities have already some masters and doctorates related to cybersecurity but there are not direct links to LEAs.

At national level, a project called "*Multinational Cyber-defence Education and training*" is taking place within the creation of the future NATO school in Portugal, which will encompass several education and training courses on cybersecurity and cyber-defence (masters and doctorates).

Training forms part of all institutions encountered during the evaluation. Specific training in the Cybercrime area takes place within the Police, Judiciary, Banks and private organisation touched by cybercrime.

During the visit the evaluation team found that the Centre for Judicial Studies (CEJ) organises cybercrime training for judges and prosecutors on an annual basis. E-training and podcasts will form part of that training in the future with an emphases on classroom training at present. This e-training and podcast concept was seen as good practice and an effective training method. This type of training can ensure that those judges and prosecutors involved in the awareness of cybercrime can be kept up to date quickly in this fast moving realm.

However, there appears to be no curriculum on cybercrime investigation at this institution and therefore training appears to be fragmented. If this is the case further more elaborate and detailed training is recommended at this level.

Training at the Criminal Police School in cyber forensics and the awareness of cybercrime is ongoing. This is largely carried out by the National Cybercrime Investigation Unit.

The PJ provides different types of training courses, for example:

- Information Security Course – training takes place at the Police School, provided by trainers-practitioners from Sub-division of Cyber-Attacks;
- Police School Training and Special Courses;
- Cooperation with the universities of technical background and other educational organizations;

- CEPOL Webinars;
- ECTEG Courses (European Cybercrime and Education Group);
- OLAF (European Anti-Fraud Office)-funded courses;
- Exchange of knowledge at Europol EPE SPACE platform.

In addition the National Counter Terrorism Unit receives training on the current threats in respect or radicalisation and Islamic terrorist activities on the Internet.

There is a requirement to keep up-to-date with the evolution and proliferation of activities in this area as an ever changing landscape. The evaluation team noted a willingness to increase training and it was stated that there was a lack of resources in this area. This was noted by the team at the time of the visit.

It has been acknowledged that the ISP's have in their possession large amounts of valuable data and expertise. It was noted by the evaluation team that there is a willingness by these companies to be more involved in providing this expertise to the public bodies in the form of training and assistance.

It is recommended that more involvement by the private sector in training and supply of expertise is considered. There is compelling arguments that the private sector are in a better position to identify new trends in technology and its use. This should be capitalised on by State institutions. This is particularly important for online terrorist and cyber-criminal activities.

The General Prosecutor' Office has established a training plan in Digital Evidence at a basic level. At the time of the visit 350 prosecutors had been trained in this area. This training is a long term objective and will continue.

The ultimate goal of the PGR is to provide at least initial training on cybercrime and digital evidence to every prosecutor with investigative tasks. The usual duration of this training is up to one day.

The CNCS promotes events and initiatives forwarding open discussions on subjects concerning security and citizenship on cyberspace and cybersecurity. In every last week of each month, between 15:00 and 18h, CNCS promotes the "Afternoon Talks". CNCS organized the C-Days 2015 in 7-8 October. C-Days 2015 was organized in partnership with ISCTE-IUL.

It was an event focused on information sharing with interventions from academia, industry and public sector in order to show the current view of the state of the art in Cybersecurity.

Awareness, strategy, risk management, information security, were among the topics required concerning Cybersecurity and this event assumed a reference position for all those looking for a forum to discuss these issues (https://c-days2015.topi.com/, https://www.youtube.com/watch?v=oEkbqiuIoQ8, https://www.youtube.com/channel/UCxWGbCv8YC8a0ImlYebUblg)

8.2. Awareness-raising

The Central Bank aims to enhance bank customers' awareness and financial literacy on innovative payments and prevention of fraud. In particular online and mobile fraud. In order to achieve this goal, Banco de Portugal participates in awareness campaigns on the correct use of innovative payment services and its advantages and risks. Moreover, the Bank Customer Website provides information about the risks associated with online and mobile payment services and identifies security measures that bank customers should observe in order to prevent fraud.

Various cybercrime prevention activities take place in Portugal. The GNR as one of the law enforcement authorities, runs the following cybercrime prevention activities:

- "Safer Internet Day";
- Cybercrime awareness programme on Social Media;

- A competition for children called "Charter of Cybersecurity Principles" – This charter has been drafted by Children for Children. In that way they are involved in awareness-raising and is stated to be very effective;
- A competition for children called "Digital Citizenship" – Cyber Challenge 2015. This is a national competition aiming to promote digital security among young people;
- A Brochure "You and the Internet" published in 2013 for children in order to raise awareness about threats on the Internet.

The evaluation team noted the presence of the GNR's "Cyber Security Task Force" and their focus on cybercrime awareness for young people. In particular, the awareness of the threat that exists from social media activity and the work carried out in this area by the task force.

Participation by children themselves in the initiative was seen as an excellent approach in awareness raising. The introduction of a pilot imitative in cyber awareness which is expected to build to a national awareness programme was seen as an effective way of preventing cybercrime before it begins.

As stated before, CNCS provides as well awareness raising activities through open discussions on subjects concerning security and citizenship on cyberspace and cybersecurity.

8.3. Prevention

The general principles on prevention are provided for in the National Security Law and in the LEAs organic laws.

Prevention activities and cooperation between the several entities in the cybercrime domain derive from Law no 53/2008, of 29 August (the National Security Law) and from the National Strategy on Cybersecurity.

As mentioned, prevention is seen as a responsibility of everyone. Several entities (institutions and non-governmental organisations, including schools and academia), that are responsible in this area also develop, more and more and on their own, prevention programs.

LEAs (GNR and PSP) developed, within community policing, special police programs specifically targeted to the prevention of cybercrime.

The PSP, during the school years of 2013-2014 and of 2014-2015, has carried out 7882 awareness raising actions, of which 429 were specifically related to Internet threats/dangers, and 7469 awareness raising actions, of which 506 on the Internet use, respectively.
Furthermore, from 5 to 10 February 2015, PSP also organized a police operation called «safe-click» at national level. This action aimed at the celebration of the Safer Internet European Day, was targeted to the youngsters with the purpose of raising awareness on specific matters, such as identity theft, phishing, cyber bulling, sexting, spam, *etc*.

In this same period of time 560 awareness raising actions were carried out, covering 347 schools and 19388 students.
As stated in previous paragraphs, the GNR and the CNCS runs some cybercrime prevention activities.

ISP representatives indicated their willingness to become involved in the preventive aspects of cybercrime. This was observed by the team as a worthwhile initiative during the visit.

8.4. Conclusions

Training

- General education and training programs on cybercrime are given to the staff of the LEAs and to magistrates (Judges and Public Prosecutors).
- The Criminal Police School has training modules on cybercrime investigation and on collection and preservation of e-evidence.
- PJ also organize and participate at a number of training initiatives in the area of cybercrime.
- During the visit the evaluation team found that the Centre for Judicial Studies (CEJ) organises cybercrime training for judges and prosecutors on an annual basis.
- E-training and podcasts will form part of that training in the future with an emphases on classroom training at present. This e-training and podcast concept was seen as good practice and an effective training method.
- There appears to be no curriculum on cybercrime investigation at this institution and therefore training appears to be fragmented. If this is the case further more elaborate and detailed training is recommended at this level.
- Most of the Portuguese Universities have already some masters and doctorates related to cybersecurity but there are not direct links to LEAs.
- At national level, a project called "*Multinational Cyber-defence Education and training*" is taking place within the creation of the future NATO school in Portugal, which will encompass several education and training courses on cybersecurity and cyber-defence (masters and doctorates).

Prevention and Awareness

- Awareness raising is high on the agenda of state institutions including the CNCS, PSP, GNR, PJ, Judicial Authorities and the Private Sector. It was noted that best practices exists within the GNR in their efforts to focus on awareness, education and training in the area of cyber and malicious on-line activities.
- The PSP carry out extensive awareness raising activities. This is seen as good practice within the State.
- CNCS provides awareness raising activities through open discussions on subjects concerning security and citizenship on cyberspace and cybersecurity.
- ISP representatives indicated their willingness to become involved in the preventive aspects of cybercrime. This was observed by the team as a worthwhile initiative during the visit.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Portugal

Generally speaking, national authorities consider that Portugal has the capability to successfully prevent and fight cybercrime.

The PJ has intervention capacity at the levels of Interpol and Europol, being a part of the team of focal points TERMINAL (on means of payment), TWINS (on child sexual exploitation) and CYBORG (on cyberattacks).

From the viewpoint of the authorities in Portugal (the PJ), the fact that the Law explicitly confers the exclusive competence on cybercrime investigations to it can be identified as good practice. In this particular field the evaluation team agrees with this assertion.

GNR has carried out initiatives on crime prevention and has led special police programs on awareness raising specifically addressed to the risk groups (young and old) with the assistance of partners, such as academia and public and private organizations. In addition GNR is involved in a European Crime Prevention Award project consisting mainly of different forms of networking communications and joint participation initiatives (training sessions, competitions, seminars, webcasts, etc.), in order to build and consolidate ethical and moral values among all the users of the cyberspace. This initiative involves young people and the project is called “Safer Internet”. The evaluation team is of the view that this is an excellent initiative by GNR.

In the context of the development of a cyber space strategy these initiatives should be resourced properly and adequately funded to make these state wide initiatives.

In respect to computer piracy**,** the Portuguese association of ISPs, APRITEL, are of the view that cooperation and sharing of information/knowledge between the judicial authorities, the LEAs and the private sector operators should be stronger. They are of the view that this will create more efficiency in dealing with computer piracy. The evaluation team is in agreement that better cooperation and sharing of information with the private sector will lead to more efficient investigation of cybercrime.

In respect to the visit by the evaluation team with the GNR and the responses to the questionnaire a number of issues was highlighted by the GNR:

- Enhanced interaction between LEAs and the private sector, in particular e-evidence collecting and exchange of information;
- An common education and awareness training programme and better international cooperation for all LEAs on a global scale with appropriate financing structures.

The evaluation team agree in principle with the above suggestions. There is merit in better international cooperation and cybercrime awareness.

9.2. Recommendations

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

Portugal 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 Portuguese 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 Portugal

1. Portugal should develop a coordinated approach for collecting standardised statistics on investigations, prosecutions and convictions relating to all cybercrime areas.

2. Portugal should elaborate and adopt a National Plan in order to implement the National Cyber Security Strategy, recently adopted.

3. The national authorities should evaluate the possibility for the citizens to address complaints related to cyber offences in electronic form.

4. Portugal should be encouraged to use the Europol channel even more in providing information to the focal points/EC3/Europol for analysis and cross-check.

5. The national authorities should take into consideration the strengthening of cooperation with private sector. The evaluation team recommends cooperation at a policy level with ISPs in order to leverage obvious and growing private sector expertise in the cyber domain This is considered vital and expedient at this time in Portugal to foster cooperation between Law Enforcement and Judicial Authorities and to ensure a coordinated approach to cybercrime throughout the State and internationally. In particular the presence of ISPs outside the State could assist with the speedy resolution of requests to third countries within the parameters of existing legislation.

6. Portugal should take into account the possibility of accessing more European and international funds.

7. Portugal should be encouraged to develop more training activities involving police, prosecutors and judges and to include in these training activities information on the support which may be offered by Eurojust, Europol and ENISA. In addition joint training with the private sector should be provided to all the relevant authorities.

8. In general there are many individual mechanisms which respond to cyber attacks within the Portuguese system both in the public and private sectors. There is a need for a coordinated approach and the allocation of a lead agency to guide and project manage the response to cybercrime.

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

1. Member States should consider involvement in awareness campaigns both at an institutional and private level. In Portugal awareness campaigns are organised by the PJ, GNR, PSP, National Centre for Cybersecurity and Bank of Portugal.

2. Member States should consider the use of the Common Taxonomy for the National Networks of CSIRTs developed by the Portuguese authorities.

3. Member States should consider enhanced cooperation with the private sector (financial organizations) in the fight against payment fraud.

4. Member States should consider to use blocking procedures on cases of Intellectual Property Rights (IPR) infringement.

9.2.3. Recommendations to European Union, the Eurojust/Europol/ENISA

1. Following the annulment of Directive 2006/24/EC, of 15 March 2006, the European Union Institutions should reflect on the most appropriate way to remedy the lack of harmonisation of national laws regarding the electronic traffic data retention, while fully considering the protection of fundamental rights.

2. Europol should continue its efforts to provide training on practical aspects of countering cybercrime, for practitioners from different fields of expertise.

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT

Monday 9-11-2015

- PM arrival GENVAL experts in Lisbon
- between 20.00 - 21.30 Informal meeting and introductions of experts team

Tuesday 10-11-2015

10.00 - 10.20 Welcome meeting with the Deputy Director General for Justice Policy

11.00 - 12.40 Meeting with PJ - National Cybercrime Investigation Unit

13.00 - 14.30 Lunch break

15.00 - 16.00 Meeting with PJ - National Cybercrime Investigation Unit

16.15 - 17.00 Meeting with PJ - Technological Support Unit; National Counter Terrorism Unit; International Cooperation Unit.

17.30 - 18.30 Meeting with Bank of Portugal

Wednesday 11-11-2015

10.00 - 12.30 Meeting at Prosecutor General's Office - with International Cooperation Unit and with the Coordinator of the Cybercrime Office

12.30 - 14.00 Lunch break

14.30 - 15.45 Meeting with the National Centre for Cybersecurity

16.15 - 17.00 Meeting with the National Republican Guard

Thursday 12-11-2015

9.30 - 10.20 meeting with the Centre for Judicial Studies

10.40 - 11.20 Meeting with a Judicial Magistrate of the Criminal Instruction Court of Lisbon

12.00 - 13.00 Meeting with Interbank Cooperation Society S.A. (SIBS)

13.00 - 14.30 Lunch break

15.00 - 16.00 Meeting with representatives of Association of the Electronic Communication's Sector (APRITEL)

16.30 - 17.30 Meeting with representatives of National Communications Authority (ANACOM)

20. 00 - dinner organized by the Ministry of Justice

Friday 13-11-2015

10.00 - 12.00 Final round for debriefing

12.30 - Departure

ANNEX B: PERSONS INTERVIEWED/MET

Persons/services interviewed/met

Procuradoria-Geral da República	
Dra. Joana Ferreira	Procuradora da República
Dr. Pedro Verdelho	Procurador da República
Dra. Ana Paula Rodrigues	Procuradora Adjunta
Dra. Marta Viegas	Procuradora Adjunta

Conselho Superior de Magistratura	
Dra. Maria Antónia Andrade	Juiz de Instrução Criminal

Polícia Judiciária	
Dra. Ana Moniz	Unidade de Cooperação Internacional Coordenadora Superior de Investigação Criminal
Dr. Sotero Freitas	Diretor da Unidade de Telecomunicações
Dr. Carlos Cabreiro	Coordenador de Investigação Criminal
Dr. Rogério Bravo	Inspetor-Chefe
Dra. Silvia Costa Ramos	Inspetora
Dr. Jorge Duque	Inspetor-Chefe
Dr. Álvaro Tomé	Inspetor
Centro de Estudos Judiciários	
Dr. Luís Manuel de Cunha Silva Pereira	Diretor Adjunto
Dr. Francisco Mota Ribeiro	Juiz de Direito, Coordenador da área penal

Guarda Nacional Republicana	
Paulo Jorge Soares dos Santos	Tenente-Coronel

Banco de Portugal	
Dr. Carlos Lopes	Departamento de Supervisão Bancária
Dr. Manuel Luz	Coordenador de Área

ANACOM	
Eng.º Manuel Barros	
Dra. Isabel Clarisse Rodrigues	
Dr. Filipe Prista Lucas	

APRITEL	
Dra. Daniela Antão	Secretária-Geral
Dra. Maria João Duarte	Representantes de operadores de

Dra. Rita Santos	telecomunicações
Dr. António Gonçalves	
Dra. Susana Gaio	
Dr. Sérgio Silva	

SIBS – Sociedade Interbancária de Serviços	
Eng.º Rui Carvalho	
Eng.º Valentim Oliveira	

Direção-Geral da Política de Justiça		
Dra. Patrícia Ferreira	Subdiretora-Geral	
Dr. João Arsénio Oliveira	Diretor de Serviços	
Dr. António Folgado	Chefe de Divisão Unidade para a Justiça Penal	
Dra. Fátima Russo	Jurista Unidade para a Justiça Penal	
Dra. Sílvia Boto	Jurista Unidade para a Justiça Penal	

ANNEX C: NATIONAL LEGISLATION

Regarding the provisions of the Budapest Convention, these are the references:

Budapest Convention **Art. 2 Illegal access to a computer system**	*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*
Corresponding domestic provision:	**Law no 109/2009** **Article 6 Illegal access** 1 - Any person who, without legal permission or without being authorized to do so by the owner, in any manner accedes to a computer system, shall be punished with imprisonment up to 1 year or with a fine of up to 120 days. 2 - The same penalty will be applied to whoever illegally produces, sells, distributes or otherwise disseminates within one or more computer systems devices, programs, a set of executable instructions, code or other computer data intended to produce the unauthorized actions described under the preceding paragraph. 3 - The penalty will be imprisonment up to 3 years or a fine if access is achieved through violation of safety rules. 4 - The penalty will be imprisonment of 1 to 5 years if: a) by means of this access, the agent becomes aware of commercial or industrial secrets or confidential information protected by law, or b) The benefit or pecuniary advantage obtained are of considerably high value. 5 - The attempt is punishable, except regarding paragraph 2. 6 - In the cases referred to in paragraphs 1, 3 and 5 the prosecution depends on of the complaint

Intent, negligence/recklessness	General rules of the Criminal Code apply.
Aggravating circumstances	**Article 6(3)(4)** 3 - The penalty will be imprisonment up to 3 years or a fine if access is achieved through violation of safety rules. 4 - The penalty will be imprisonment of 1 to 5 years if: a) by means of this access, the agent becomes aware of commercial or industrial secrets or confidential information protected by law, or b) The benefit or pecuniary advantage obtained are of a considerably high value.
Minimum, maximum penalty	30 days of imprisonment up to 5 years.
Attempt	The general rule of the Criminal Code applies, even if it is not punished, to the cases provided under nr 2.

Budapest Convention **Art. 3 Illegal interception**	*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*
Corresponding domestic provision:	**Law no 109/2009** **Article 7 - Unlawful interception** 1 - Any person who, without legal permission or without being authorized to do so by the owner, other right holder of the system or part of it, through technical means intercepts transmissions of computer data processed within a computer system, to there directed or from there proceeding, will be punished with imprisonment up to 3 years or a fine. 2 - The attempt is punishable.

	3 - The same penalty provided for in paragraph 1 will be applied to those who illegally produce, sell, distribute or otherwise disseminate within one or more computer systems devices, software or other computer data intended to produce the unauthorized actions described under that paragraph.
Intent, negligence/recklessness	The general rule of the Criminal Code applies.
Aggravating circumstances	The general rule of the Criminal Code applies.
Minimum/maximum penalty	30 days of imprisonment up to 3 years.
Attempt	The general rule of the Criminal Code applies, according to Article 7 (2).

Budapest Convention Art. 4 Data interference	1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
Corresponding domestic provision:	**Law no 109/2009** **<u>Article 4</u> - Computer damage** 1 - Any person who without legal permission or without being authorized to do so by the owner, other right holder of the system or part of it, deletes, alters, destroys, in whole or in part, damages, removes or renders unusable or inaccessible programs or other computer data of others or in any way affects their ability to use, shall be punished with imprisonment up to 3 years or a fine. 2 - The attempt is punishable. 3 - The same penalty of paragraph 1 will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computers or other systems devices, software or other computer data intended to produce the unauthorized actions

	described in that paragraph. 4 - If the damage is of high value, the penalty is imprisonment up to 5 years or a fine of up to 600 days. 5 - If the damage is pretty high value, the penalty is imprisonment of 1 to 10 years. 6 - In the cases provided for in paragraphs 1, 2 and 4 the prosecution depends on the complaint.
Intent, negligence/recklessness	The general rules of the Criminal Code apply.
Aggravating circumstances	**Law no 109/2009** **<u>Article 4 (4)(5)</u>** 4 - If the damage is of high value, the penalty is imprisonment up to 5 years or a fine of up to 600 days. 5 - If the damage is of a pretty high value, the penalty is imprisonment of 1 to 10 years.
Minimum/maximum penalty	30 days of imprisonment up to 10 years.
Attempt	The general rule of the Criminal Code applies, according to nr 2.

Budapest Convention **Art. 5 System interference**	*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.*

Corresponding domestic provision:	**Law no 109/2009** **<u>Article 5</u> - Computer sabotage** 1 - Any person who, without legal permission or without being authorized to do so by the owner, other right holder of the system or part thereof, prevent, stop, or severely disrupt the operation of a computer system through the introduction, transmission, damage, alteration, deletion, preventing access or removal of programs or other computer data or any other form of interference in the computer system is punished with imprisonment of up to 5 years or a fine of up to 600 days. 2 - The same penalty will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computer systems devices, software or other computer data intended to produce the unauthorized actions described in the preceding paragraph. 3 - In the case of the preceding paragraph, the attempt is not punishable. 4 - The penalty will be imprisonment of 1 to 5 years if the damage arising from disturbance is of high value. 5 - The penalty will be imprisonment of 1 to 10 years if: a) damage arising from disturbance is of a considerably high value; b) the disturbance reaches seriously a computer system that supports an activity designed to provide critical social functions, including supplying chains, health, safety and economic well-being of persons, or the regular functioning of public services.
Intent, negligence/recklessness	The general rule of the Criminal Code applies.

Aggravating circumstances	**Law no 109/2009** **Article 5(4)(5)** 4 - The penalty will be imprisonment of 1 to 5 years if the damage arising from disturbance is of high value. 5 - The penalty will be imprisonment of 1 to 10 years if: a) damage arising from disturbance is of a considerably high value; b) the disturbance reaches seriously a computer system that supports an activity designed to provide critical social functions, including supplying chains, health, safety and economic well-being of persons, or the regular functioning of public services.
Minimum/maximum penalty	30 days of imprisonment up to 10 years.
Attempt	The general rule applies.

Budapest Convention **Art. 6 Misuse of Devices**	
Corresponding domestic provision:	**Law no 109/2009** **Article 3 (4), Article 4 (3), Article 5 (2), Article 6(2) and Article 7(3)** **Article 3 - Computer forgery** 4 - Whoever imports, distributes, sells or holds for commercial purposes any device that allows the access to a computer system, to a payment system, to a communications system or to a conditioned access service, on which was committed any of the actions referred to in paragraph 2 is punished with imprisonment of 1 to 5 years. **Article 4 - Computer damage** 3 - The same penalty of paragraph 1 will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computers or other systems devices, software or other computer data intended to produce the unauthorized actions described in that paragraph.

	Article 5 - Computer sabotage 2 - The same penalty will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computer systems devices, software or other computer data intended to produce the unauthorized actions described in the preceding paragraph. **Article 6 - Illegal access** 2 - The same penalty will be applied to whoever illegally produces, sells, distributes or otherwise disseminates within one or more computer systems devices, programs, a set of executable instructions, code or other computer data intended to produce the unauthorized actions described under the preceding paragraph. **Article 7 - Unlawful interception** 3 - The same penalty provided for in paragraph 1 will be applied to those who illegally produce, sell, distribute or otherwise disseminate within one or more computer systems devices, software or other computer data intended to produce the unauthorized actions described under that paragraph.
Intent, negligence/recklessness	The general rule of the Criminal Code applies.
Aggravating circumstances	
Minimum/maximum penalty	30 days of imprisonment up to 5 years.
Attempt	The general rules of the Criminal Code apply.

Budapest Convention **Art. 7 Computer-related forgery**	*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.*
Corresponding domestic provision:	**Law no 109/2009** **Article 3 - Computer forgery** 1 - Whoever, with intent to cause deception in legal relations, enters, modifies, deletes or suppresses computer data or otherwise interferes with computer data to produce information or documents that are not genuine, with the intention that they be considered or used for legally relevant purposes as if they were, is punished with imprisonment up to 5 years or a fine of 120 to 600 days. 2 - When the actions described in the previous paragraph relate to the data registered or incorporated in a banking card or any other device that allows the access to a payment system or to a communications system or to a conditioned access service, the penalty is 1 to 5 years in prison. 3 - Whoever, acting with intent to cause injury to others or to obtain an unlawful gain for him or her or for others, makes use of a document made of computer data that were the subject of the acts referred to in paragraph 1 or a card or other kind of device in which it were registered or incorporated the data of the acts referred to in the preceding paragraph, shall be punished with the penalties provided for in either number, respectively. 4 - Whoever imports, distributes, sells or holds for commercial purposes any device that allows the access to a computer system, to a payment system, to a communications system or to a conditioned

	access service, on which was committed any of the actions referred to in paragraph 2 is punished with imprisonment of 1 to 5 years. 5 - If the facts referred to in the preceding paragraphs are committed by an official employee in the performance of their duties, the penalty is imprisonment of 2 to 5 years.
Intent, negligence/recklessness	The general rule of the Criminal Code applies.
Aggravating circumstances	**Law no 109/2009** **Article 3 (2)(4) (5) - Computer forgery** 2 - When the actions described in the previous paragraph relate to the data registered or incorporated in a banking card or any other device that allows the access to a payment system or to a communications system or to a conditioned access service, the penalty is 1 to 5 years in prison. 4 - Whoever imports, distributes, sells or holds for commercial purposes any device that allows the access to a computer system, to a payment system, to a communications system or to a conditioned access service, on which was committed any of the actions referred to in paragraph 2 is punished with imprisonment of 1 to 5 years. 5 - If the facts referred to in the preceding paragraphs are committed by an official in the performance of his duties, the penalty is imprisonment of 2 to 5 years.
Minimum/maximum penalty	30 days of imprisonment up to 5 years.
Attempt	The general rule of the Criminal Code applies.

Budapest Convention **Art. 8 Computer-related fraud**	*Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:* *a any input, alteration, deletion or suppression of computer data;* *b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.*
Corresponding domestic provision:	**Criminal Code** **<u>Article 221</u> - Computer and communications fraud** 1 - Whoever, with intent to obtain for himself or for someone unlawful enrichment, causes loss of another person property, interfering in the result of treatment of computer data or by incorrect structuring of a computer program, incorrect or incomplete use of computer data or by some other unauthorized processing of data or intervention in data, will be punished with imprisonment up to three years or a fine. 2 - The same penalty applies to those who, with intent to obtain for themselves or for others an unlawful gain, cause financial loss to another, using programs, electronic devices or other means which, separately or together, are intended to reduce, amend or prevent, in whole or in part, the normal functioning or operation of telecommunications services. 3 - The attempt is punishable. 4 - The prosecution relies on the complaint. 5 - If the injury is: a) of a high value, the perpetrator is punished with imprisonment up to five years or a fine of up to 600 days; b) of a considerably high value, the agent is punished with imprisonment from two to eight years. 6 - It is also applicable to the provisions of Article 206.

Intent, negligence/recklessness	The general rules of the Criminal Code apply.
Aggravating circumstances	**Criminal Code** **Article 221(5)** 5 - If the injury is: a) of a high value, the perpetrator is punished with imprisonment up to five years or a fine of up to 600 days; b) of a considerably high value, the agent is punished with imprisonment from two to eight years.
Minimum/maximum penalty	30 days of imprisonment up to 8 years.
Attempt	The general rules of the Criminal Code apply.

Budapest Convention **Art. 9 Child pornography**	
Corresponding domestic provision:	**Criminal Code** **Article 176 - Child pornography** 1 - Whoever: a) Uses a minor in a pornographic show or entices that minor for said purpose; b) Uses a minor in photography, film or other pornographic record, in whatever form, or entices that minor for said purpose; c) Produces, distributes, imports, exports, distributes, displays or assigns, in any way or by any means, the materials mentioned in the preceding paragraph; d) Acquires or possesses materials mentioned in b) with the intent to distribute, import, export, advertise, display or transfer; will be punished with imprisonment of one to five years. 2 - Whoever commits the acts described in the preceding number professionally or with profit purposes, will be punished with imprisonment of one to eight years. 3 – Whoever commits the acts described in c) and d) of number 1 using pornographic material with realistic representation of a minor will be punished with imprisonment up to two years.

	4 - Whoever acquires or possesses materials provided in b) of number 1 shall be punished with imprisonment up to one years or a fine. 5 - The attempt is punishable.
Intent, negligence/recklessness	The general rules of the Criminal Code apply.
Aggravating circumstances	**Criminal Code** **Article 176(2)** 2 - Whoever commits the acts described in the preceding number professionally or with profit purposes, will be punished with imprisonment of one to eight years.
Minimum/maximum penalty	30 days of imprisonment up to 8 years.
Attempt	General rules of the Criminal Code apply.

ANNEX D: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

List of acronyms, abbreviations and terms	Acronym in original language	Full name in original language	English
ANACOM			National Communications Authority
APRITEL			Association of the Electronic Communication's Sector in Portugal
CAPSEND			Central Aggregation Point for Sexual Exploitation Network Data
CEJ			Centre for Judicial Studies
ECTEG			European Cybercrime Training and Education Group
EMPACT			European Multidisciplinary Platform against Crime Threats
ENISA			European Union Agency for Network and Information Security
EPE			Europol Platform
ERA			Academy for European Law
GENVAL			Working Party on General Matters including Evaluations
GNR			National Republican Guard
IP			Internet Protocol
MLA			Mutual Legal Assistance
MoI			Ministry of Interior
MoJ			Ministry of Justice
SIBS			Interbank Cooperation Society S.A.
PSP			Public Security Police
PJ			Criminal Police

List of acronyms, abbreviations and terms	Acronym in original language	Full name in original language	English
CNCS			National Centre for Cybersecurity
PGR			General Prosecutor's Office