Council of the
European Union

Brussels, 8 February 2017
(OR. en)

14584/1/16
REV 1 DCL 1

GENVAL 119
CYBER 132

DECLASSIFICATION

of document:	14584/1/16 REV 1 RESTREINT UE/EU RESTRICTED
dated:	31 January 2017
new status:	Public
Subject:	Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Greece

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, 31 January 2017
(OR. en)

14584/1/16
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 119
CYBER 132

REPORT

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

ANNEX

Table of Contents

1. EXECUTIVE SUMMARY

- The evaluation visit to Greece took place between 29 September and 2 October 2015 and it was very well organised by the national authorities.

- The programme of the visit included meetings with a large number of representatives of the institutions involved, as police officers, prosecutors, as well as other relevant institutions and organizations, as Cyber Defence Directorate, Ministry of Culture, Education and Religious Affairs, National Telecommunications and Post Commission, Ministry of Infrastructure, Transport and Networks, Bank of Greece, Hellenic Bank Association and one representative of the civil society.

- According to the Evaluation Team, the choice of the representatives was appropriate, although if an additional presence of the magistrates could have been more beneficial for the evaluation visit.

- All the representatives that the Evaluation Team met had very detailed power point presentations on the relevant topics, helpful for the comprehension of the global system. After the evaluation visit, the national authorities provided to the team additional relevant materials.

- Greece has not yet adopted the National Cybersecurity Strategy, but the competent authorities are in drafting process.

- Concerning the legislation, Greece has signed the Convention on cybercrime of the Council of Europe, but has not ratified it yet. The Directive 2013/40/EU on attacks against information system has also still to be transposed. The Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography has been transposed into the national legislation.

- The national authorities reported difficulties in collecting statistics on cybercrime. However, additional statistics on child pornography offences had been provided after the evaluation visit.

- There are some specialised units in the Police and Prosecution Service. The Directorate of Electronic Crime Prosecutions seats in Athens and has a subordinated structure in Thessaloniki.

- The Interbanking Committee, which includes representatives of the banks, the Bank of Greece and the Hellenic Police, organise meetings in order to discuss new trends on fraud, incidents and countermeasures technologies. The Hellenic Banks Association maintains alert contact lists regarding cybercrime (skimming, e-commerce fraud, cyberattack, Internet fraud).

- Credit institutions operating in Greece are obliged to report without delay cyber-attack incidents that target the credit institutions and/or their customers.

- There is room for improvement in the matter of specialised training offered to the practitioners. However, the National School of Magistracy organize specialized training sessions for judges and prosecutors with the participation of the police officers as well.

- National authorities organize, through the Ministry of Education and police services, an impressive number of prevention and awareness campaigns for the schools' communities, addressed to the teachers as well as to the children.

2. INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

The 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 Greece were Ms Eneli Laurits (Estonia), Mr Richard Szongoth (Hungary) and Ms Ulrika Sundling (Sweden), together with Mr Gilles Duval and Ms Carmen Necula from the General Secretariat of the Council.

This report was prepared by the expert team with the assistance of the General Secretariat of the Council, based on findings arising from the evaluation visit that took place in Greece between 29 September and 2 October 2015, and on Greece' 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

Greece does not dispose a national strategy of cyber security. However, the Directorate of Cyber Defense/General Headquarters of National Defense (DCD/NDGH), with the participation of HDPS representatives, is presently elaborating a relevant text which will be soon completed and forwarded for approval to the Hierarchy.

In particular, in view of the processing of the proposal-Directive of the European Parliament and the Council regarding the measures for the safeguarding of a common high level network and information security throughout the European Union (COM(2013) 48 final), a meeting has taken place on November 8th, 2013 at the Ministry of Infrastructure, Transports and Networks. During such meeting and upon proposal by DCD/NDGH to undertake a relevant initiative, it was decided that an informal working group should be established for the preparation of National Strategy for Cyber Security. In the working group participated upon open invitation, representatives of the agencies of the public administration and the academic area, including the Communication Privacy Protection Authority (C.P.P.A.). The work progress of the working group and the interim results were presented and discussed with a wider audience which additionally included representatives of the electronic communication providers, as well as crucial infrastructures of the country.

In the end of 2014, the NDGH gave to publicity and placed under informal negotiation, the final draft paper of the National Strategy of Cyber Security. During meetings that have taken place within 2015, the NDGH, in the context of organizing the exercise PANOPTIS 2015, its representatives have informed that the draft paper was being under further processing, which is expected to have been completed by the mid July 2015, when, consequently, this will be forwarded for approval to the NDGH leadership.

The draft paper of the National Strategy for Cyber Security briefly contains "the national strategic vision for cyber security" (general principles and strategic guidelines which govern the National Strategy), the organizational structure and the governance model as well as the overall actions required to be implemented in order for the strategic goals to be achieved. The framework of the activities-actions that will have to be achieved during the implementation of the National Strategic Cyber Security is summarized to the following : Determination of the Agencies that participate in National Strategy, Monitoring of the Information Systems of Crucial Infrastructures and Assessment of Dangerousness in National Level, Monitoring of Existing Institutional Framework, National Plan of Emergency in the Cyber Space, Determination of Basic Security Requirements, Handling Security Incidents, National Alertness Exercises, Users-Citizens Sensitization, Credible Mechanisms for Information Exchange, Support of Research and Developmental Programs and Academic Programs of Education, Cooperation in National Level, and finally Assessment and Review of the National Strategy.

3.2. National priorities with regard to cybercrime

The Ministry of Interior and Administrative Reconstruction – Hellenic Police Headquarters, have processed an Anti-Crime Policy Program for the years 2015-2019 that is a central reference point for all police services. This Program is the continuation of the Anti-Crime Policy Program for the years 2010-2014.

- ✓ The Anti-Crime Policy for the years 2015-2019 is divided into four basic themes.
- ✓ In particular, the goals set for the reinforcement of security in the cyber space are as follows:
- ✓ Tracing of individuals or networks activated in trafficking child pornography
- ✓ Fighting against cyber bullying
- ✓ Fighting against the Internet fraud
- ✓ Fighting against circulation of forged travelling documents and drugs via the Internet

- ✓ Fighting against Human Trafficking Victim Solicitation via the Internet
- ✓ Fighting against intrusions-cyber attacks
- ✓ Dissuasion of suicides announced at the Internet
- ✓ In order to achieve these goals, specific actions are prescribed, as follows:
- ✓ Constant Education-Training of the Staff of the Directorate of Electronic Crime Prosecution, in Greece or abroad.
- ✓ Upgrading of the education and constant training of the officers of the Directorate of Electronic Crime Prosecution.
- ✓ Exploitation by the peripheral Services, of the guidelines for the confrontation of fraud by the Skimming method, based on a processed manual, transferred by the Directorate of Public Security/HPH to all Services of the Hellenic Police in the year 2009.
- ✓ Cooperation of the Peripheral Services with the materially competent Directorate of Electronic Crime Prosecution, in order that, in the cases where are noticed offences committed by the Use of Computer, the appropriate manner to be methodized for securing the evidence and further handling the cases.
- ✓ Strengthening of the cooperation with the Hellenic Banks Association to the effect of prevention and effective confrontation of the fraud incidents through the Internet that offend the financial system of the Country.
- ✓ Active participation in the public's briefing procedures for the safe use of the Internet and the lurking dangers involved.

- ✓ Implementation of informative daily conferences-seminars to parents and students for the provision of information and advice for the safe use of the Internet and the avoidance of their victimization.
- ✓ Strengthening of the cooperation with foreign competent prosecuting Authorities via the legal communication channels (INTERPOL, EUROPOL, EUROJUST, etc.) in order to make possible the tracing down and the solution of crimes with international nature that are committed at the Internet or by using the same.
- ✓ Every day "patrol" in the Internet areas for the prevention and suppression of criminal acts.
- ✓ Implementation of the memorandum of police actions for the management of suicidal intention signs.

After all these, it becomes clear that the Hellenic Police has fully adopted the strategic goals and functional action plans set for the fighting, on E.U. level, of the serious and organized crime for the period 2014-2017, as these are imprinted in the Conclusions of the Council by the no. 12095/13 document. Besides, it is noted that, according to the content of the mentioned document, the EU priorities in the issues of fighting against the electronic crime, focus on the on-line fraud by payment cards, the cyber area crimes causing serious damage to their victims, as the On-Line sexual exploitation of children, and attacks to the cyber area that affect basic infrastructure and information systems in the E.U.

Besides, the DCD/NDGH disposes an action plan for the development of cyber defense in the Armed Forces and often issues directives for the prevention and confrontation of cyber incidents while, part of the material is also available for the wide public via the website of the NDGH (http://www.geetha.mil.gr).

Additionally, the Hellenic Data Protection Authority (henceforth "HDPA"), even not formally part of any national strategy for combating cybercrime, nevertheless, as the competent national data protection authority for Greece, continuously aims at raising public awareness about cybercrime issues that are relevant to data protection. For example, on its website, there are specialised sections on topics such as identity theft, spam, as well as a special section aimed at young people and how they can safeguard their privacy online.

Finally, the Ministry of Justice Transparency and Human Rights has a key priority the transposition of legal instruments of international and European law. To this end, it has established a special legislative committee to ratify the Cybercrime Convention of the Council of Europe (Budapest Treaty), signed by Greece on 23.11.2001 but not yet ratified. Furthermore, this committee's work includes the transposition of the Directive 2013/40 / EU "on attacks against information systems". It is expected that the committee's draft will be delivered soon.

3.3. Statistics on cybercrime

Greece does not collect cybercrime statistics separately. The latest published annual report is about 2013. A total of 562 complaints were received and 214 were related to electronic communications. However, this number is not indicative. Only some of these cases were related to cybercrimes, but in report's statistics they were not marked as such, so no statistics can be provided.

However, after the evaluation visit the national authorities sent some statistics on child pornography, related to the number of cases in judicial districts (for 2012) and the number of cases in courts of first instance of Athens (2013-2015).

3.3.1. Main trends leading to cybercrime

The annual number of the cases handled by the Directorate of Electronic Crime Prosecution has significantly increased, according to the statistical data disposed by the Directorate, though a tendency of stabilization (at high rates) has been remarked.

The number of frauds committed via the Internet have been increased as well as a significant development is noticed as concerns as the complicity of methods used by the criminals. Furthermore, crimes against sexual dignity of minors and minors' pornography presents a significant increase. With regard to cyber attacks, no remarkable alterations have been noticed, their number remaining low, comparing to other Member-States of the European Union data.

On the other hand, the latest published annual report for 2013 of HDPA, from a total of 562 received complaints 214 were related to electronic communications. However, this number is not indicative. Only some of these cases were related to cyber crimes, but in its report's statistics they are not marked as such, so not statistics can be provided. This general category may include complaints about cases related to telephone call recording, unauthorised posting of personal data (e.g. video or photo) on the web, social engineering, data breaches, etc.

3.3.2. Number of registered cases of cyber criminality

Statistical data stored by the Hellenic Police concern only cases, dealt by the Directorate of Electronic Crime Prosecution.

Credit Institutions ('banks') operating in Greece send to the Bank of Greece on a regular semester basis, statistical data regarding the number, the value and the distribution of financial losses from payment card fraud. One of the main categories of fraud for which statistical information is reported, includes the one concerning transactions without the physical presence of the card (CNP / Card-Not-Present) via internet, mail, and/or phone. Furthermore, statistical data concerning cyber-attacks (e.g. phishing, malware, DDoS) are reported on a yearly basis to the Bank of Greece Supervised Institutions' Information Systems Section.

Moreover, Bank of Greece receives ad hoc and regular reporting regarding major operational disruptive events including cyber-attacks (e.g. phishing, malware, DDoS). Moreover, credit institutions are obliged to report immediately major security incidents (e.g. cyber-attacks, card fraud, e-banking, malware, DDos) to the bank of Greece.

The incidents reporting includes: incident timestamp and duration, incident description, incident causes and triggers, actions taken, incident criticality and impact).

Official Information from the website www.hellenicpolice.gr

2013: Activity of the Financial Police and Electronic Crime Prosecution Service

Financial Police and Electronic Crime Prosecution Service's contribution in confronting the financial and the electronic crime, during the year 2013 proves to be positive.

Among its significant successes, it is also included the organization and implementation of extended police operations for fighting against the illegal trafficking of pharmaceutical products, the arrest of parties involved in electronic frauds, the identification and arrest of perpetrators for criminal activities that have take place via the social media, as well as the tracing down and the further management of many criminal and anti-social behaviours that concern the tax legislation.

It is noted that, during 2013, the special phone number 11012, provided by the Financial Police to receive complaints, received 4.027 complaints in total. These complaints, grouped according to geographical criteria and kind of illegal activity, are examined by assessment committees and are forwarded to the Stations of the Financial Police and the Electronic Crime Prosecution for further police investigation. From the total number of the complaints, 1.679 complaints were made eponymously while 2.348 anonymously.

COMPLAINTS RECEIVED BY THE FINANCIAL POLICE – CYBER CRIME PROSECUTION

2.157 by phone (54%)

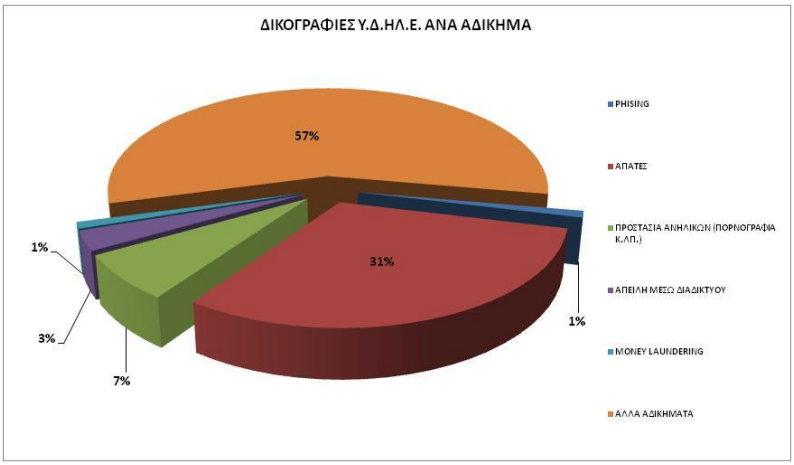
1.117 by email (28%)

583 via post (14%)

92 via fax (2%)

78 in person (2%)

In the sector of the electronic-internet form of criminal behaviors, the Electronic Crime Prosecution handled 1.189 legal briefs for piles of internet or electronic crimes of which briefs, 292 were created ex officio while 897 were created upon district attorney's order, following a citizen's complaint.



57% OTHER CRIMES

31% FRAUDS

7% MINORS' PROTECTION (Child Pornography etc.)

3% CYBER THREAT

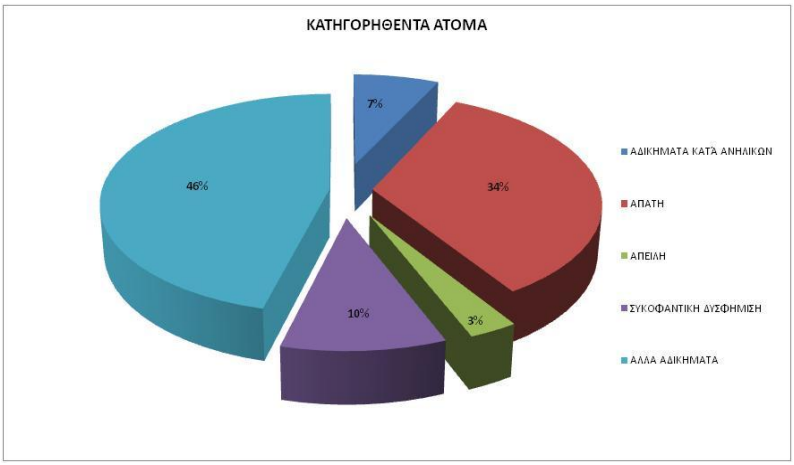
1% PHISHING

1% MONEY LAUNDERING

Among the above cases, 104 of them were investigated by the police, and a legal procedure took place investigation followed and a legal brief was created by echelons of the Electronic Crime Prosecution, upon complaints by citizens, Agencies of Consumer Protection, Organizations, Financial Institutes, Telecommunication Companies etc.

Additionally, in the context of the international Police cooperation (Interpol and Europol), the Sub-Directorate of Electronic Crime Prosecution handled 414 requests of cooperation. The requests concerned cases of interstate police investigations that had felony cybercrimes as object and concerned electronic trade, Internet frauds, embezzlements of data and passwords to electronic databases, platforms and websites of electronic economic activities.

Totally, charges have been addressed against 1.030 persons totally for various offences.



ACCUSED PERSONS :

46% Other Offences

34% Fraud

10% Slanderous Defamation

7% Offences against Minors

3% Threat

2014 : Activity of the Directorate of Electronic Crime Prosecution

The Directorate of the Electronic Crime Prosecution, in the year 2014, developed many actions concerning prosecution of crimes committed via Internet as well as prevention, by informing citizens about safe Internet surfing.

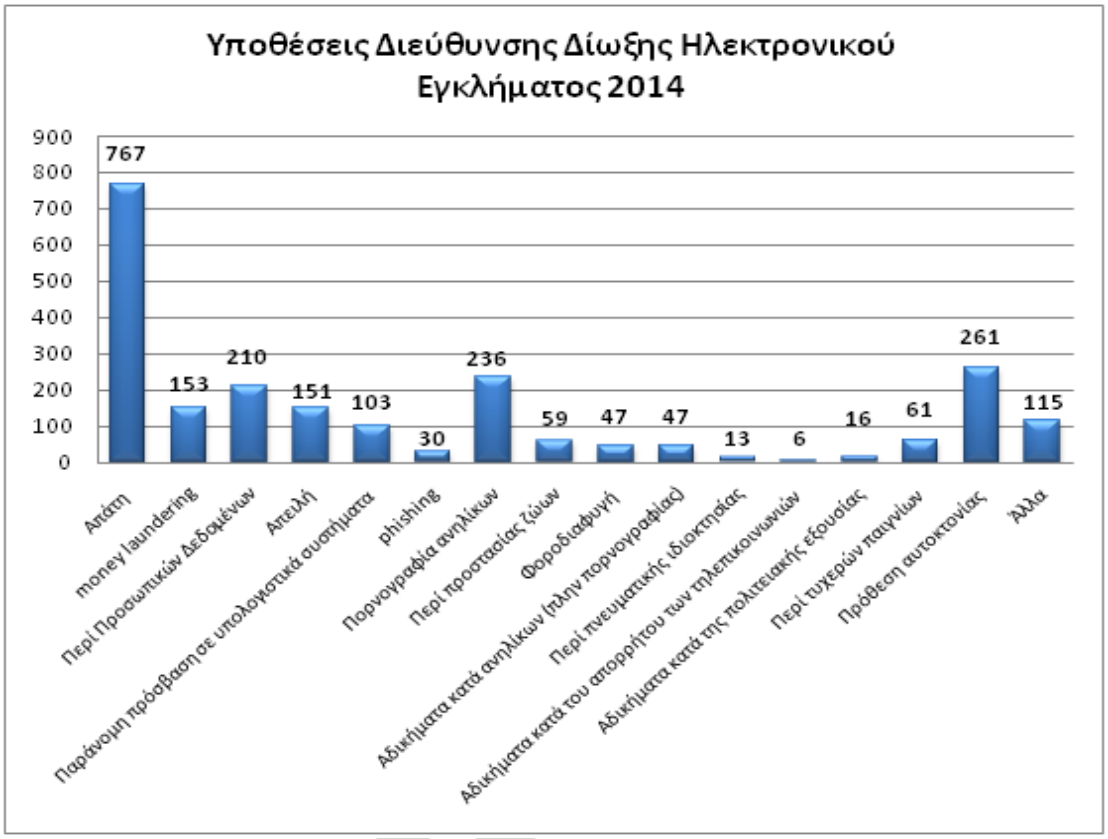
For fulfilling its mission, the Directorate cooperated with other competent central and regional competent Services of the Hellenic Police, while a great number of information has been transferred from and to the Directorate of International Police Cooperation and especially the National Europol Unit and the Department of International Organizations –Interpol.

At the same time, actions have been undertaken (150 cases have been reported) for implementing the National Business Program of Fighting against Tax Evasion.

Total Cases

The total number of new cases handled by the Directorate of Electronic Crime Prosecution in the year 2014 is 2.275. Specifically, per case:

Cases of the Directorate of Electronic Crime Prosecution, 2014



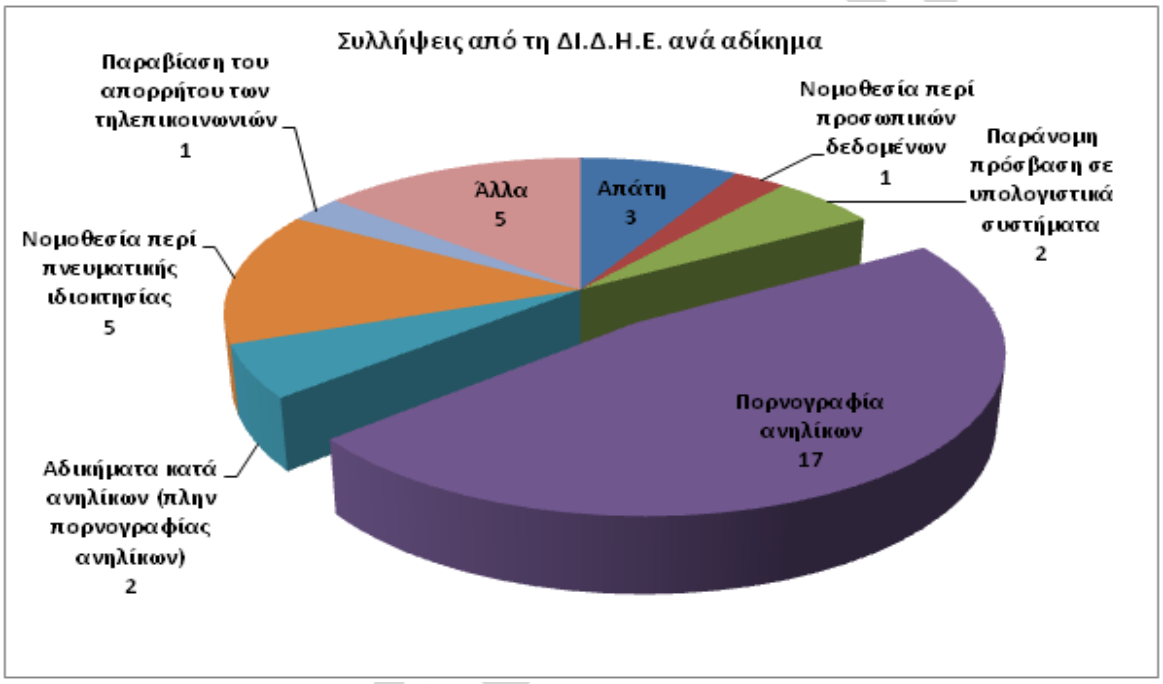
[767 Fraud, 153 money laundering, 210 personal data, 151 threats, 103 illegal access to computer systems, 30 phishing, 236 minors pornography, 59 animal protection, 47 tax evasion, 47 offences against minors (other than pornography), 13 Intellectual property, 6 Offences against privacy of telecommunications, 16 Offences against the State Order, 61 Lucky Games, 261 Suicidal Intention, 115 Others]

Among those, 102 legal procedures came after complaints by Agencies for the Protection of Consumers, Organizations, Financial Institutes, Telecommunication Companies, as well as e-shops.

Also, in the context of the international police cooperation (Interpol and Europol), the Directorate of Electronic Crime Prosecution dealt with 573 requests of cooperation. The requests concerned cases of interstate police investigations that had as object of felony nature, electronic crimes and concerned minors' pornography, electronic trade, the Internet frauds, embezzlements of data and passwords to electronic databases, platforms and websites of electronic economic activities.

Arrests – Accusations Imputed

36 persons in total were arrested for the following offences:



ARRESTS BY THE DI.E.C.P. PER OFFENCE

Violation of telecommunications privacy : 1

Legislation regarding intellectual property : 5

Offences against minors (other than minors' pornography) : 2

Legislation regarding personal data : 1

Illegal access to computer systems : 2

Other : 5

Fraud : 3

Minors' Pornography : 17

Charges have been addressed to 1.032 persons, in the context of penal procedure.

District Attorney's Orders

During 2014, in 1.244 cases, District Attorney ordered a Preliminary Examination or Pre-Interrogation.

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

Prevention and fight against cybercrime is a part of the wider context of operation of Hellenic Police and the co-competent agencies. There is no specific provision in the budget of the Hellenic Police concerning prevention and fight against cybercrime, apart the standard amount referring to operational expenses of the Service (consumable materials, travelling expenses in case of staff trips etc.).

Indirectly, participation of Greek police forces to the Cybercrime Priority of the EMPACT Program of the European Union's Policy Cycle and specifically, in the sub-priorities of Payment Card Fraud, Child Sexual Exploitation & Cyber Attacks, proves to be quite useful. Also, the e-crime project that is co-funded by the National Strategic Reference Framework (NSRF) resources, with a budget of almost 2,5 million euro is running. This program includes the creation of a computerized operational center, supplied with computer equipment, appropriate software, specialized in automatic internet research and data storing. The project is gradually implemented with the supervision of the Society of Information S.A. and, it is scheduled to be in full operation before the end of October 2015.

Additionally, the European and Developmental programs management Service, the competent Service of the Hellenic Police regarding the preparation and submission of the Multi-Year Program Plan 2014-2020 for the Internal Security Fund (ISF), is negotiating with the European Commission so that the final plan of the above program is approved.

With regard to prevention and fight against cyber crime by the mentioned Service, an Action, initiated by the Directorate of Electronic Crime Prosecution, has been integrated for funding, entitled: "Creation of Hellenic Center for the Electronic Crime", upon a budget of 900.000,00 € that is planned to include the following authorities, in summary:

- Planning and implementation of national strategy concerning prevention of cyber crime;
- Recognition and Monitoring of informational infrastructures of the country and implementation of a continuous operational plan;
- Education of Police Staff;
- Creation of a Portal concerning public awareness;
- Motivating citizen's sensitivity;
- Supporting Hellenic authorities' active participation in programs and actions of the EC / Europol;
- Ensuring the optimum cooperation and coordination of all agencies involved, in national level, including the academic and private sector;
- Creation of a national contact point with the international excellence centers for cyber crime.

3.5. Conclusions

- The relevant authorities in Greece consider cybercrime as a serious threat to the state and to society, therefore there is a wide range of authorities involved in combating cybercrime. Law enforcement organization and the cooperation with the private sector during prevention's activities seem to be effective and proactive.
- There is no comprehensive National Cyber Security Strategy in place in Greece. However, the national authorities have established a working group for the drafting of National Strategy for Cyber Security. During the evaluation visit the draft paper was being under further process. In the opinion of the Evaluation Team the strategy, along with the defined priorities and an action plan, would be a solid basis on which to fight effectively against cybercrime.

- Greece has clearly defined its national priorities with regard to handling cybercrime. The Ministry of Interior and Administrative Reconstruction – Hellenic Police Headquarters have processed an Anti-Crime Policy Program for the years 2015-2019 that is a central reference point for all police services. This Program is the continuation of the Anti-Crime Policy Program for the years 2010-2014 which sets out objectives for the coming years. In particular, the goals set for the reinforcement of security in the cyber space are tracing of individuals or networks activated in trafficking child pornography; fighting against cyber bullying; fighting against the Internet fraud; fighting against circulation of forged travelling documents and drugs via the Internet; fighting against Human Trafficking Victim Solicitation via the Internet; fighting against intrusions-cyber attacks and dissuasion of suicides announced at the Internet.
- Close cooperation between the private sector and public organisations creates a unique opportunity to involve a wide range of entities working together. This should be regarded as best practice.
- The Evaluation Team realised that there are no detailed, standardised and comprehensive statistics at the national level showing all the threats and incidents that have occurred with regard to cyber attacks on a yearly basis. Also, there is no figure available for cybercrime as a percentage of overall criminality. However, after the evaluation visit the national authorities sent some statistics related to child pornography, but it is still room to improve the data's collection on cybercrime in a systematic manner.
- In the evaluators' view, the incomprehensive statistics make it difficult to get a clear view of the progress of cyber criminality on the one hand, and on the other of the effectiveness of combating this phenomenon. Some of the incidents registered may seem small at first glance but turn out to be bigger after a more in-depth evaluation. Therefore, the Evaluation Team considers that collecting overall statistics could make detailed analysis possible and so help building a clearer picture of the effectiveness of the legal system in protecting the private interests of citizens victimised by cybercrime.

- There is no specific domestic budget allocated to combating cybercrimes, but some programs funded within EMPACT Program of the European Union's Policy Cycle are developed and the national authorities made applications in order to obtain funds from the European Commission.

4. NATIONAL STRUCTURES

4.1. Judiciary (prosecutions and courts)

4.1.1. Internal structure

Greek Law does not provide for a special court, competent to deal with cybercrime acts. Nevertheless, in the "Public Prosecutor's Office of District Court Judges of Athens", two specialized prosecutors have been appointed to deal with cybercrime cases.

4.1.2. Capacity and obstacles for successful prosecution

A serious obstacle to the successful prosecution of the crime in the Cyber space is the fact that usually this requires the sending and fulfillment by another country, of a Request of Judicial Assistance. The procedure for the provision of Judicial Assistance requires time for the translation and shipment of the Requests of Judicial Assistance while the successful or non-successful outcome of it is related to the legal order of the country of execution.

In specific, if in the country of Execution, the investigated act does not fulfill the condition of the dual criminality because, for example, this is not a criminal act for that country, or it has been barred, then the prosecution cannot proceed.

An indicative example is also the shipment of such Requests of Judicial Assistance to the U.S.A. Greece has sent and continues sending piles of Requests of Judicial Assistance to the U.S.A. based on the bilateral agreement for Mutual Judicial Assistance signed in Washington on 26.05.1999 and

ratified by Greece by the L. 2804/2000 (Gov. Gaz. 49/3-3-2000, Issue A'), in combination with the Protocol to the Convention of mutual judicial assistance in criminal matters between the Government of the Hellenic Republic and the Government of the United States of America, signed on 26.50.1999 as prescribed in the Article 3(2) of the Agreement between the European Union and the United States of America regarding the mutual judicial assistance, signed on 25.06.2003 and the Verbal Notes with numbers AS 199 of the Ministry of Foreign Affairs of the Hellenic Republic and 116/POL/09 of the Embassy of the United States of America and ratified by Greece, by the L. 3771/2009 (Gov. Gaz. 111/9-7-2009, Issue A'). The problem that arose was the lack of the dual criminality and the consequential non fulfillment of the Requests of Judicial Assistance of the Hellenic Judicial Authorities, for offences such as vilification or slanderous defamation which, in the legal order of the United States of America, fall under the protection of the freedom of speech.

Another issue Greece occasionally encounters, concerns the finite period of time for the retention of the electronic traces (IP) which might be short and thus, the Request of the Hellenic Judicial Authorities, might not be able to be fulfilled due to lapse of the time for the retention thereof.

4.2. Law enforcement authorities

A) Directorate of Electronic Crime Prosecution

By the Presidential Decree 178/2014, it has been prescribed the establishment and the structure of the Directorate of Electronic Crime Prosecution with seat in Athens and the establishment and the structure of the Sub-Directorate of Electronic Crime Prosecution with seat in Thessaloniki. The mission of the Directorate of Electronic Crime Prosecution includes prevention, research and suppression of crimes or antisocial behaviors that are committed via the Internet or other means of electronic communication. The Directorate of Electronic Crime Prosecution is an autonomous Central Service and is directly subjected to the Chief of the Hellenic Police.

The Directorate of Electronic Crime Prosecution, in its internal structure, comprises five departments that constitute the total spectrum of the user's protection and the security of the Cyber space. Thus, in its new upgraded structure, it consists of:

a. Department of Administrative Support and information Management,
b. Department of Innovative Actions and Strategy,
c. Department of Electronic and Telephone Communication Security and Protection of Software and Intellectual Property Rights.
d. Department of Minors Internet Protection and Digital Investigation and
e. Department of Special Cases and Internet Economic Crimes Prosecution

Department of Administrative Support and Information Management

The authorities of the Department of Administrative Support and Information Management are the following:

a. the handling of staff issues, economic issues and materials, the secretarial, administrative and technical support and generally, the service of the functional needs of the Service.
b. the collection, survey, analysis, assessment, possible correlation and processing of information, evidence and data related to the mission of the Service and the forwarding of the processed data to the competent Departments of the Directorate for business exploitation, as per ratio of competence,
c. the case for the permanent specialized education and further education of the staff of the Directorate in matters of fighting against the electronic crime, via the preparation and implementation of educational programs, according to the relevant needs of the Business Departments and in cooperation with the Directorate of Education and Development of Human Resources of the Headquarters as well as with all competent services or agencies of the Country and other countries, through the Directorate of the International Police Cooperation of the Headquarters.

d. In the Department of Administrative Support and Information Management, there is an Operation center in place which ensures the coordination and the communication of the staff of the Service during its operational action. In the Operation center, operate, round-the clock, a call center with a special complaints line, as well as e-mail Service for the communication of the citizens with the Service.

Department of Innovative Actions and Strategy

The authorities of the Department of Innovative Actions and Strategy are the following :

a. The preparation of programs for the information of the citizens and the agencies on issues of internet and electronic crime, through the implementation of various actions, such as congresses, daily conferences, and teleconferences, as well as the organization of other innovative actions in the sector of fighting against the electronic crime,
b. the framing of strategic planning issues, related to the cyber crime,
c. the promotion and the disclosure of the social work of the Service, via the creation and management of profiles in social media (Twitter, Facebook etc.) to the effect, exclusively of the communication, information and sensitization of the citizens on matters of electronic threats and dangers.
d. the follow up on the developments in electronic crime issues, in both domestic and international level, the preparation of a relevant annual survey with conclusions' extraction for the delinquency on these offences in the Country and the submission of specific reasoned proposals for confronting the same and
e. the monitoring of actions and statistical information regarding the electronic crime and the observance thereof.

Department of Electronic and Telephone Communication Security and Protection of Software and Intellectual Property Rights.

The Department of Electronic and Telephone Communication Security and Protection of Software and Intellectual Property Rights operates according to the provisions of the no. 7001/2/1261-(21) dated 28.08.2009 common Ministerial decision of the Ministers of Interior, Economy and Finance and Justice (B'1879). Also, this Department is competent for :

a. handling cases of illegal penetration in computer systems and theft, destruction or illegal circulation of software material, digital data and audiovisual works, committed throughout the country,
b. assisting other competent services that investigate such cases, according to the applicable legislation and
a. providing the necessary technical assistance to the other Departments of the Service, the performance of digital and internet research by using modern technological equipment and the digital and internet analysis of digital data, files and other means and findings in cases of investigation of serious matters falling under their authority.

Department of Minors' Internet Protection and Digital Investigation

The authorities of the Department of Minors Internet Protection and Digital Investigation are the following :

a. The solution and prosecution of the crimes committed against the minors by the use of the Internet and other means of electronic or digital communication and storage,
b. the investigation of internet or electronic harassment cases (cyber bullying) and racism or xenophobic content in the internet, as well as cases of participation in suicide and cases of expression of suicidal intentions or disappearance, via the Internet and
c. the provision of assistance to the competent State Services for the dissuasion of suicides that are announced via the internet, as well as the Services that investigate cases for crimes committed at the Internet according to the applicable legislation.

Department of Special Cases and Internet Economic Crimes Prosecution

The powers of the Department of Special Cases and Internet Economic Crimes Prosecution are the following :

a. Fighting, in cooperation with the Financial Police Directorate and the other competent national, European and foreign services and authorities, of financial crimes and especially crimes that have been committed in the cyberspace by the use of electronic means and new technologies, against the financial interests of the State and the national economy in general or present the features of the organized financial crime and their investigation requires specialized know-how.

b. The constant research in the internet and the other means of electronic communication and digital storage for the revelation, solution and prosecution of the criminal acts that fall under its authority, that are committed in them or via them throughout the Country, provide a specialized technical or digital research is required for their investigation.

A respective structure and powers are prescribed also for the Sub-Directorate of Electronic Crime Prosecution.

B. National CERT – National Information Agency

Electronic attacks to infrastructures of the State – National Information Agency (N.I.A.)

The confrontation of the offences committed via the Internet and concerning the performance of Cyber Attacks to Ministries and Services of the State either within or outside Greece, is subjected to the competence of the National Information Agency (N.I.A.) while the Directorate of Electronic Crime Prosecution assists whenever there is need to. In particular :

- ✓ By the article 2 of the P.D. 360/92, it has been prescribed that the NIA/Directorate E is competent for the collection of information from and by electronic means for the security of the National Communications.

- ✓ By the article 2 of the P.D. 325/2003, N.I.A. has been nominated as the National Security Organization while the E' Directorate thereof as the Information Security Authority (INFOSEC) which, among others, proceeds also to the assessment and certification of the devices and systems of Communication and Information Security.
- ✓ By the Ministerial Decision F. 120/6/200994/S.1691/08-06-2004 of the Minister of National Defense, the NIA/Directorate E' is nominated as the National Authority of Communication-Information Security (INFOSEC)
- ✓ By the article 4 of the L. 3649/2008, NIA was nominated as the National Authority for the Confrontation of Cyber Attacks.

C. Department of Digital Evidence Examination, Directorate of Criminal Investigations

As far as the Department of Digital Evidence Examination is concerned, of the Directorate of Criminal Investigations (see Question 1.3), as its general powers are described in the above question, the following are particularly noted :

a. The Laboratory for the Computer System Evidence Examination, which:

aa. carries the reading, recovery-reset, examination, decryption, analysis, comparison, processing, data monitoring, found in storage digital places of local computer networks or other special fixed or portable means for the data digital storage.

bb. decides about the mode for the operation of the software or the digital material, verifies the sequence of the actions of software use or material and performs examinations for the verification of the creator or the application user or data on digital evidence, that are suitable for reading.

cc. makes examinations on electronic devices or other special electronic structures, which are possible to store digital data

dd. performs examinations in mobile phones and position location devices,

ee. makes specialized examinations, readings, recoveries and resets of digital data on banking or other cards, as well as examinations on relevant special electronic means (electronic passports), since these examinations are not possible to be made at the Laboratory of Forgery-Counterfeiting Investigation and Forgery of Documents and Values of the Directorate of Criminal Researches.

ff. makes examinations in telecommunication systems, in devices for receiving satellite TV or other signal which contains digital data suitable for reading,

gg. cooperates with the responsible Agencies for ensuring the confiscation, correct handling and faster shipment of the evidence to be examined, by providing to those agencies, instructions for the safe transfer and safeguarding while, in exceptionally crucial cases, it offers technical assistance to the confiscation, via the shipment of specialized echelons.

b. Secretarial Support Office which is competent for :

aa. the receipt, circulation, delivery, charge-discharge and generally management of the evidence, the documents, the reports and the overall correspondence of the Department according to the applicable provisions,

bb. the technical support of the functionality of the Department's Laboratories and especially for the support of the networks and the creation of security copies on the discs of the official computers,

cc. the supply of equipment, materials and means for the assistance of the requested laboratory examinations, upon motion made by the Managers of the Laboratories,

dd. the organization of internal educational programmes for the specialization-further training of the staff serving at some Sector or is going to be transferred to it, upon relevant motion by the managers of the Laboratories.

ee. The finding, organization and classification of the relevant bibliography that concerns the object of the Department, upon relevant motion made by the Managers of the Laboratories,

ff. the monitoring, maintenance, upgrading and charging of the possessed special official software, material and the overall equipment of the Department,

gg. all other special tasks, related to its competence, as assigned according to the each time applicable provisions and orders,

hh. the keeping of the electronic or physical files and official books, where the relevant registrations are made for the most effective organization of the task of every Laboratory and

ii. the receipt, general signaling and safe circulation of the evidence sent to be examined.

It is also noted that, similar powers are also exercised by the Department of Laboratories of the Sub-Directorate of Criminal Investigations of Northern Greece to the authorities of which are subjected as mentioned also in the question 1.3, the powers of the Department of Examination of the D.C.I. digital evidence.

Also, to the Directorate of Criminal Investigations are also subjected as to their special mission, the education and the material-technical equipment, the following :

a. The Criminal Investigation Stations (C.I.S.), which operate at the Headquarters of the General Regional Police Directorates, with the exception of the General Regional Police Directorate of Central Macedonia (totally 11 throughout the state) and
b. the Criminal Investigations Offices (C.I.O.) which operate at the Headquarters of the prefectural Police Directorates as well as in Services out of the Police Directorates seats, provided there is a seat of First Instance Court there (totally 53 throughout the State).

Additionally, with regard to the specialized positions for special examiners in the sector of Information Technology, it is noted that, in the Electronic Crime Prosecution Directorate as well as the Department of Digital Evidence Examination of the Directorate of Criminal Investigations, general and special duty police officers are serving, who possess titles of studies of undergraduate, postgraduate and certain of them, even doctorate level, in computer-science related objects.

4.3. Other authorities/institutions/public-private partnership

The Supervised Institutions Inspection Department of the Bank of Greece and in particular the Supervised Institutions' Information Systems Section play an active role including that of the prevention of cybercrime.

Furthermore, highly important in the field of cyber risk mitigation is the role of the European Central Bank regarding the 4 systematically important Greek banks that have been, since November 2014, under the micro-prudential supervision of Single Supervisory Mechanism (SSM). Very recently Greek banks received and replied to an extensive SSM questionnaire concerning cyber-crime risk mitigation.

Additionally, at a proactive level, there is constant cooperation and exchange of information among the stakeholders (banks – Hellenic Police and Bank of Greece) in the framework of regular meetings of the HBA interbank committee regarding prevention and combating of fraud in payment systems and means of payment. As part of this committee international, European and national respective initiatives are being thoroughly discussed.

The National Authority for the Confrontation of Cyber Attacks – National CERT is the National Authority, competent for the confrontation-protection from electronic threats-attacks, according to the L. 3649/2008 and the P.D. 126/2009. In particular:

It is the competent National Authority for the confrontation-protection from cyber threats-attacks to the Public Agency and the crucial infrastructures of the country.

It collects electronic attacks-threats information from public and private agencies,

It analyzes the information, it monitors-categorizes the kind of the attacks-threats (dangerous code, intrusion, software inabilities etc.) and it handles the attacks-threats depending on their kind.

It provides information and advice for the protection of the computer systems of the Public and the private sector, with regard to security from the mentioned attacks-threats.

It proceeds to announcements related to imminent threats or cyber attacks made and it proposes preventive or suppressive protective measures.

It circulates information and proposals related to the protection- results, consequences and conclusions from threats-attacks.

It gets updated on the evolution of the information technology, it participates in conferences, seminars and relevant educations.

It cooperates with other National or not CERTS as well as Agencies of the Public Sector on relevant issues.

It gives advice and assistance at the premises of the agency that suffered the attack, for the restoration- limitation of the impact from the attacks, provided this is asked by the agency.

It coordinates the response actions between the parties involved in attacks.

It disposes the required equipment for the handling, the development of strategy and the confrontation of threats-attacks as well as the collection, processing and circulation of the relevant information.

The HDPA is an independent administrative authority, it reports only to the Parliament and is not subject to any administrative control but its decisions may be appealed to the Council of State. Its independence is both derived and guaranteed by the Hellenic Constitution (art. 9A) and Law 2472/1997. It is composed of a judge of one of the three national high courts as President and six members i.e. a University professor specialized in law, a University professor specialized in information technology, a University professor of any discipline and three persons of high standing and experience in the field of the protection of personal data. The President, the members of the Board and their substitutes are elected by the Parliament, following a proposal by the President of the Parliament. They hold their offices for four years, their appointment is renewable only once, and, in the course of their duties, they enjoy full personal and functional independence.

As explained briefly in certain previous answers, the HDPA has the power to order the rectification and/ or deletion of any incorrect data, conduct audits of the IT infrastructure used with respect to the fulfillment of the security principle, address recommendations/opinions regarding the appropriateness of data processing (according to art. 19 of Law 2472/1997) and has also the power to impose administrative sanctions such as pecuniary penalties and notes of serious warnings (according to art. 21 of Law 2472/1997).

The Hellenic Authority for Communication Security and Privacy (ADAE) was established in 2003 as prescribed by article 19 par.2 of the Hellenic Constitution, which calls for the establishment of an independent authority with the mission to ensure the confidentiality of mail and all other forms of free correspondence and communication. ADAE monitors the implementation of all legislation relevant to the lawful interception of communications and, for this purpose, it is authorized to receive all lawful interception mandates issued by the judicial authorities. Moreover, Law 3115/2003 attributes ADAE, inter alia, the power a) to issue regulations regarding the assurance of the confidentiality of communications, b) to perform audits on communications network/service providers, public entities as well the Hellenic National Intelligence Service, c) to hold hearings of the aforementioned entities, d) to investigate relevant complaints from members of the public and e) to collect relevant information using special investigative powers.

Working in the communication security area for over 10 years, ADAE has obtained sufficient experience in managing the risks and vulnerabilities posed to the security of the networks and services of communications providers. In practice, ADAE investigates and audits the communications providers' systems and services, it identifies and discusses their security weaknesses and breaches in detail with their administrators and it proposes technical and procedural measures in order to safeguard the confidentiality and the integrity of users' communication data.

As it is prescribed by its founding law, ADAE performs onsite audits, both scheduled (periodical) and ad hoc. A valuable tool during the audits is the provider's security policy, which must be previously approved by ADAE and must comply with the terms set out in ADAE'S Regulations. In scheduled audits, all systems and services of the provider are usually audited, while in ad hoc audits, specific functions, systems and services of the provider are audited. Ad hoc audits are mainly triggered by user complaints or when a security incident/breach becomes known. After the audit, ADAE submits an audit report to the providers. This report usually includes the identified security weaknesses and eventual technical, procedural or legal findings and deviations from the approved provider's security policy. The report proposes appropriate technical and organizational measures to the provider. ADAE, may also impose administrative sanctions on providers, taking into account the severity of the security deviations and weaknesses found as well as the principle of proportionality.

In central headquarters level the Directorate of Public Security operates at the Hellenic Police Headquarters, in the structure of which the Department of Organized Financial and Electronic Crime (P.D. 178/2014) is established and operates, to the competence of which is integrated among others, the study of measures for the confrontation of the crimes by the use of computers as well as the guidance of the regional Services in the prosecution of such crimes.

Additionally, according to the provisions of the par. 7 of the article 31 of the P.D. 178/2014, for the fulfillment of its mission, the Di.E.C.P. cooperates with other locally and materially competent central and regional Services of the Hellenic Police and especially the Directorate of Computer Science of the Headquarters, the Directorate of Information Management and Analysis, the Directorate of Financial Police and the Directorates of Security of Attica and Thessaloniki. Also, in this context, it cooperates with other competent services, principles and agencies of the Country, as well as with respective services, organizations and agencies of European and other countries, according to the applicable provisions and the relevant international agreements and conventions.

Finally, in the paragraph 3 of the article 65 of the P.D. 178/2014, it is mentioned that the Directorates of the Branches and the regional Services of the Hellenic Police cooperate responsibly and effectively with the autonomous central Services in the context of their powers by providing to those all necessary assistance in fulfilling their mission. To this effect, all Services of the Hellenic Police transfer or notify the Directorate of Information Management and Analysis, the informative material that they collect in the context of their official activity and they inform the Directorates of Financial Police and Electronic Crime Prosecution as well as the Directorate for the Confrontation of Special Violence Crimes, for every case of common competence which they deal with.

Furthermore, the Department of Examination of Digital Evidence, of the Directorate of Criminal Investigations, cooperates with the responsible Services for ensuring the confiscation, correct handling and faster shipment of the evidence to be examined, by providing to those agencies, instructions for the safe transfer and safeguarding while, in exceptionally crucial cases, it offers technical assistance to the confiscation, via the shipment of specialized echelons.

The National CERT informs on regular basis, the public agencies for the newly appeared cyber threats and it distributes IoCs to them for the prevention or/and confrontation of cyber attacks. In case a cyber attack is made to a public agency, then the agency being attacked is obliged to report the incident to the National CET and provide it all necessary information for analyzing the attack. The National CERT proceeds to analysis of the aggressive activity and then notifies the conclusions to the public agency, to which it proposes advisory measures of electronic security which are advisable to be applied in order to avoid similar incidents in the future. Then, it is up to the agency's discretion whether it wishes to proceed to the legal prosecution of the attackers. In such case, the conclusions of the National CERT analysis are forwarded to the competent service for the law enforcement, which usually is the Electronic Crime Prosecution.

In the context of the national exercises of cyber war "Panoptis" wide participation exists from academic institutes, agencies of the public as well as the private sector. The cooperation between all involved agencies requires better coordination.

4.4. Cooperation and coordination at national level

4.4.1. Legal or policy obligations

The private sector may notify, without however being obliged to, electronic attacks incidents to the cyber space, on the National Authority for the Confrontation of Cyber Attacks and get advice of handling as well as business-technical assistance from it, for the confrontation of the incidents if requested.

Credit institutions operating in Greece are obliged to report without causal delay cyber-attack incidents that target both the credit institutions and/or their customers. The report is addressed to the Cyber Crime Division of the Hellenic Police, Bank of Greece as well as to the SSM of the ECB. The HBA created and maintains two alert contact lists with contact details of the competent representatives of credit institutions, Cyber Crime Division of the Hellenic Police and Bank of Greece.

The 1st alert contact list is concerning any kind of payment card fraud incidents (e.g. ATM & POS skimming, e-commerce fraud, etc.) whereas the 2nd alert contact list is concerning any kind of internet fraud (e.g. sophisticated phishing techniques, identity theft, sharing of customer secret credentials with third parties and man-in-the-middle/browser attacks which intercept/modify/divert customer data, malware, social engineering, DDoS and breaching the perimeter zone, etc.).

Law 3471/2006 (GG A' 133), which transposes Directive 2002/58/EC into the national legal order, designates ADAE, together with the national Data Protection Authority, as the competent national authority to receive data breach notifications. Moreover, ADAE has issued Regulation 165/2011 "for the Assurance of confidentiality in Electronic Communications" (GG B' 2715). Both ADAE's Regulation 165/2011, as well as article 8 of Law 3674/2008 (GG A' 136) include provisions for the immediate notification of communication confidentiality breaches or risk of such breaches to ADAE and to the subscribers concerned.

The National Authority for the Confrontation of Cyber Attacks is the competent governmental authority that coordinates the confrontation of the cyber attacks between the parties involved, as far as this concerns the public sector or crucial infrastructures. Also, in cases of quite extended cyber attack, it will notify the security services.

Yes there is sufficient/effective cooperation between banks and LEAs to prevent and fight online card fraud.

In the HBA, a dedicated Interbanking Committee has been created for encountering fraud in the payment systems. Members of this Committee are representatives of the Banks, the Bank of Greece and the Hellenic Police. In the Committee, the new trends of fraud, incidents and countermeasures/ technologies are discussed in order to take appropriate measures. Inside this Committee, an alert contact list operates with contact details of the competent representatives. The contact list is concerning any kind of payment card fraud incidents (e.g. ATM & POS skimming, e-commerce fraud, etc.)

- **notify police/LEA if they become aware of any abuse of new payment tools developed by industry?**

The law enforcement authorities are in cooperation with the private sector of the country. Especially, as to the credit institutes of the country, in the context of the interbanking committee for the prevention and confrontation of fraud in the means and he payment systems as well as the ad hoc interbanking task group that receives updating with confidential content, transferred by Europol, there is made an exchange of confidential information via the European Central Bank and EC3 which concern new methods or new tools of payment. Respectively, the exchange of confidential information in national level between the credit institutes and the law enforcement principles, is made via the work group for fighting against internet fraud).

- **increase the security of non-cash payment and minimize the vulnerability of magnetic stripes?**

For the most effective cooperation between the private sector and the law enforcement authorities, Di.E.C.P., in the context of its authorities, make sensitization updates to the private sector with regard to new tendencies in the topic of the online frauds as well as provision of advice for taking appropriate prevention measures.

The adoption of the new EMV technology in the total of the portfolio cards from the credit institutes of the country, results now to the reinforcement, to the maximum extent, of the security in the payments by the presence of card, thus minimizing the vulnerability of the magnetic tapes.

Greek payment cards industry is EMV/chip and PIN oriented. Anti-fraud monitoring systems for payment card transactions have been implemented by all issuing banks. Special security routines are taking place when a Greek payment card is used abroad and more specifically on a non-EMV country (e.g. USA).

- **strengthen the authorisation of online transactions and authentication of customers?**

For fighting against the frauds through the Internet, every company has adopted its own system of protection from frauds. The systems for the protection from frauds, perform controls in real time, for the detection of cases of fraud in the online internet transactions by the use of payment cards.

As to the credit institutes of the country, there is a channel of communication and direct cooperation between them for the reinforcement of the procedure for the verification of the clients' details aiming to the timely restriction of the fraudulent transactions.

Greek Banks have set up a state of the art on-line payment infrastructure and sophisticated and efficient security measures such as:

- Specialized security mechanisms of multiple levels of defense.
- Monitoring and detection of fraudulent card transactions.
- MasterCard® Secure Code™ or Verified by VISA services as authentication services of the identity of the cardholder during purchases over the internet.

On top of all that, in the last years, banks have been educating customers not to share their card data (card number, PIN, CCV2) as well personal data (such as ID number, birth date) with anybody and protect them adequately.

The role of the private sector in the prevention of and fight against cybercrime is of fundamental importance. By conducting risk assessments, taking the appropriate security measures and applying a structured security policy, providers of electronic communications networks and services may not only prevent the occurrence of certain types of cybercrime but may also assist the law enforcement agencies with the provision of substantial evidence, under the condition that it is acquired through the procedures prescribed by law.

Up to date, there is no legal framework which would provide the possibility of cooperation with the private sector, to what concerns the laboratory examinations on electronic crime evidence.

The contribution of the banks to the judicial and police authorities is continuous and unceasing. In terms of repressive level, involves/consists of the provision of

- audiovisual material, especially in cases of ATM fraud,
- transaction data of fraudulent payment cards,
- account statement details that have been used for money transfers because of phishing attacks (mule accounts),
- sending the IP addresses that are used by internet fraudsters, etc.

Additionally, at a proactive level, there is constant cooperation and exchange of information among the stakeholders (banks – Hellenic Police and Bank of Greece) in the framework of regular meetings of the HBA interbank committee regarding prevention and combating of fraud in payment systems and means of payment. As part of this committee international, European and national respective initiatives are being thoroughly discussed.

The National Authority for the Confrontation of Cyber Attacks – National CERT cooperates with companies of the private sector for getting information related to ways of detection and confrontation of cyber attacks, evidence taking as well as for victims - attack targets.

It also cooperates with companies of the private sector by providing electronic security directions in order to deactivate computer systems and functions of them where interventions have been made and are used for illegal purposes.

The mentioned cooperation of the National Authority for the Confrontation of Cyber Attacks – National CERT with the private sector is not based on legal or regulative obligations that are determined by the legislation, but on the context of good cooperation for a common purpose that is the maintenance of a high level of security in the cyber space.

In the national legislation, by the integration of the article 25 of the Directive 2011-93/EU, specific provisions have been included in the article 18 of the l. 4267/2014 for taking measures against websites that contain or disperse child pornography material. By an order of the competent District Attorney, it is ordered the deletion of a website that is hosted in Greece and contains or disperses child pornography material. Such Order is notified on the provider of the hosting services of such website and is immediately executed (article 18 par.1). Similar provisions have been set for the case that a website containing or dispersing child pornography material and cannot be verified whether such website is hosted in Greece or out of Greece and it is found in a space or subspace with domain name granted in Greece. In such a case, the relevant Order of the District Attorney commanding the provisional deactivation of the domain is notified on the holder of the domain name and the National Communication and Post Committee (N.C.P.C.) and is immediately executed.

If it concerns a website that contains or disperses child pornography material, it is not hosted in Greece and does not belong to a space or a subspace that has been granted in Greece, by Order of the District Attorney it is commanded the barring of access to such website. If the holder is detected, then the district attorney's Order is notified on him, as well as on the N.C.P.C. which then notifies the same to the internet access providers and asks for the immediate implementation thereof and the users' updating. Consequently, the internet access providers also contribute to the implementation of the measures that the judicial authorities have decided to be implemented against websites that contain or disperse child pornography material. It should be also noted that, in integration of the Directive 2006/24/EC (which was found invalid by the decisions of the Di.E.C.P. on the cases C-293/12 and C-594/12) to national legal order, the provider's' obligation to maintain specific data, in order for those to be available to the competent authorities for the verification of especially serious crimes, is regulated in the articles 1-13 of the l. 3917/2011.

As to the participation of the private sector to the prevention and fight against the crimes related to the internet and especially content related crimes, it could be mentioned the operation of an open line for complaints against illegal content in the Internet, by union and non profiteering associations, such as the Safeline which is, since 18.10.2005, member of the International Association of Internet Hotlines (INHOPE). The specific line has established in 2003 by a private company of Internet access provision, the Hellenic Organ of Self-Regulation for the Internet Content (SAFENET) and two foundations, while it operates with the support of the Safer Internet Program of the European Committee (www.safeline.gr).

4.4.2. Resources allocated to improve cooperation

The Directorate of Electronic Crime Prosecution avails the necessary equipment (Machinery) for fighting the online frauds. Additionally, in order to keep up with the new technologies used in the sector of the payment cards, the Service participates in congresses throughout the universe while, at the same time, it cooperates with inland University institutes. Special software for the online frauds is not available in the Service. However, it is continuously pursued a search for technology aiming to the prosecution and fight against these online frauds.

Every year, D.C.C./N.D.G.H. organizes and conducts the national cyber defense exercise "PANOPTIS" where are called to participate the security forces, the wider public sector, the academic community, as well as the private sector. Via the scenarios of the exercise, it is pursued the training of the exercised participants in the confrontation of modern cyber threats as well as the reinforcement of the cooperation and information exchange between each other. Additionally, the Directorate participates in European exercises where it pursues the involvement of the private sector as trainee as well, wherever this is feasible.

4.5. Conclusions

- At the judicial level there are no specialized courts or judges dealing with cybercrime. There are neither specialized prosecutors, except 2 prosecutors within the Public Prosecutor's Office of Athens District. Therefore, in the opinion of the Evaluation Team raising awareness and acquiring specific knowledge of this type of crime among judges and prosecutors require regular and specialized training.
- The central law enforcement agency in fighting against cybercrime is the Hellenic Police Directorate of Electronic Crime Prosecution which seat in Athens with five departments and a Sub-Directorate of Electronic Crime Prosecution which seat in Thessaloniki. The mission of the Directorate includes prevention, research and repression of crimes or antisocial behaviors that are committed via the Internet or other means of electronic communication. According to the personal experiences of the evaluation team the organizational structure covers all fields of fighting against cybercrime.
- According to the presentations and the personal discussions during the evaluation visit the experience of the police seems to be very good, law enforcement work is proactive on all fields including cyberattacks, payment card frauds and child online sexual exploitation.
- The central unit responsible for forensic examinations is the Hellenic Police Department of Digital Evidence Examination, Directorate of Criminal Investigations. According to Evaluation Team the forensic knowledge and experience of the department seems to be very good but comparing the number of cases with the number of personnel it seems that additional staff is strongly needed in order to decrease the time of forensic examination processes. The length of the forensic examination may affect sometimes the length of criminal trial.
- Most of the digital evidence needs to be handled by the forensic division. To be able to meet the future it is needed to examine what is the best practise to have an effective process in the forensic work to avoid the problem with “funnel-phenomenon”.

- As a best practice it must be highlighted that within the Directorate of Electronic Crime Prosecution is established the special 24/7 cybercrime emergency service, called the Cyber Alert, where specialized officers deal with every incident, including those that require immediate handling (i.e. suicidal intention signs). Additionally, for mobiles and tablets, there has been created a free application with useful information regarding the Internet surfing while a phone call is automatically made to the call center by simply pushing a button.
- The Cybercrime division are doing a good work regarding the online card fraud, in the cooperation with the aviation companies and travel agents. Greece is the first country to work with this area on a daily basis (it started as a project in EC3, Europol). They are also co-leaders in EMPACT work.
- It would be beneficial if there were developed a specific division for cybercrime consisting of specialist cybercrime prosecutors handling these cases, which according to the evaluators is a useful method of sharing information and experience. The experience at police level seems to be very good. Therefore, the existence of regional prosecutors specialised in cybercrime could lead to the establishment of similar structures within law enforcement authorities since there is a close relationship between prosecutors and the police on legal and operational aspects.

5. LEGAL ASPECTS

5.1. Substantive criminal law pertaining to cybercrime

5.1.1. Council of Europe Convention on Cybercrime

- Greece signed (23.01.2001) but has not ratified the Convention on cybercrime, of the Council of Europe (Budapest Convention, CETS 185). To this effect, a special law preparatory committee has been created (no. 84280/22.10.213 Decision of the Minister of Justice, Transparency and Human Rights). The object of the works of the same committee was also the Directive 2013/40/EC for the attacks against information systems.

- Furthermore, as to the protocol additional to the above mentioned Convention, which was also signed on 28.01.2003 and has not been ratified yet, it should be noted that recently, Greece, by the law 4285/2014 (A'191), has modified its national legislation (l.927/1979) for the crimes related to acts of racism and xenophobia, in order to be harmonized with the Decision-Framework 2008/913/DEY dated November 28th, 2008. The articles 3 and 6 of the Protocol enact the obligation of the states-members to penalize specific behaviors, which, if we respectively refer to the articles 1 and 2 of the l. 4285/2014, we will see that they are covered by their predictions. In specific, the distribution of racist material (articles 1 par. 1 and 3 of the Protocol) could be integrated in the crime of the public incitement of violence or hatred as per art. 1 of the L. 927/1979, as modified by the l. 4285/2014, under the mode of commitment of the incitement, provocation or excitation. Besides the commission of such acts via the Internet is expressly prescribed as a crime of such article as well as crime of the article 2.

Respectively, the provisions of the article 6 of the Protocol regarding refusal, downgrading of the significance and the approval or the justification of genocides or crimes against humanity, are standardized in the art 2 .l. 927/1979, as modified by the article 2 L. 4285/2014. In this article, there are determined as criminal, also behaviors as the applause of such actions, which are not expressly considered as such in the letter of the Protocol, while there are expressly referred other crimes as well the refusal of which becomes criminal such as war crimes, the Holocaust and Nazism crimes.

In the L. 927/1979, there was added by the article 3 of the L. 4285/2014, a special provision as article 3, for the implementation of the Hellenic criminal laws and consequently the expansion of the jurisdiction of the Hellenic State. In particular, it is prescribed that in cases that the crimes of the articles 1 and 2 of the l. 927/1979, are committed via internet or other mean of communication, provided there is access granted to these means by the Hellenic State and regardless the mode of their installation, as place of commission is considered Greece as well. It is, however, noted that the rest behaviors prescribed in the articles 4 and 5 of the Protocol (threat and insult, respectively due to racist or xenophobic motives) cannot be included in the L. 927/1979 as modified by the L. 4285/2015, but they are standardized as respective crimes of the Criminal Code or other legislative statutes. The threat constitutes a crime as per article 333 of the Criminal Code, when committed originating from specific motives; the combination of this article with the article 81A of the Criminal Code (supplemented with the art. 10 l. 4285/2014) increases the lowest prescribed penalty limit.

Actually, if there is a case for the implementation of the article 81 A of the Criminal Code, it has been prescribed the imputation of the secondary penalty of the political rights deprivation (Art. 61 b of the Criminal Code). The public insult may not be a crime as per Hellenic Criminal Code, but a crime is the vilification as per art. 361 of the Criminal Code and the previous provisions may apply on this, according to the article 81 A of the Criminal Code**.**

Following the evaluation visit, article 81A of Penal Law has been modified, by virtue of article 21 of L. 4356/2015. Before the modification article 81A was applicable only in case it was proved that the perpetrator had acted with animosity. As a result article 81A was rarely applicable, taking into account that proving an internal mood like "animosity" faces major difficulties. The new title of article 81A is "Crimes with racist features". According to this modified version, article 81A applies in any case a perpetrator is motivated against a certain victim because of the special characteristics of the latter, such as race, skin color, nationality or ethnicity, genealogical origin, religion, physical or mental disability, sexual orientation or sec characteristics. The new modified version not only extends the scope of the disposition but also facilitates the proof: instead of requiring the difficult proof of an internal mood like "animosity" it is content with the proof of an objective fact, such as the choice of the victim because of its special characteristics.

5.1.2. Description of national legislation

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

Generally speaking, Greek national legislation does not provide for criminal liability of legal persons. Still, in cases of crimes committed by a legal person, Greek national legislation provides for liability of physical persons entitled for representing the legal entity (e.g. managing directors, directors).

As far as personal data protection is concerned, the national law 2472/1997 on personal data protection foresees sanctions for any violation of its provisions by a data controller. More specifically the HDPA can impose administrative sanctions up to the amount of 150.000 euros.
In the law on data protection (2472/1997) no such explicit criteria are provided for. However, article 10 on confidentiality and security of processing states that the controller must implement appropriate technical and organisation security measures that shall ensure a level of security appropriate to the risks presented by processing and the nature of the data processed. This appropriate level of security entails such criteria as the number of data subjects, volume of personal data etc.

Regarding the minor cases, as per art. 19 of the data protection law (under number 2472/1997), the HDPA shall examine all of the complaints of data subjects relating to the implementation of the law and the protection of the applicants' rights when such rights are affected by the processing of data relating to them. However, the HDPA can file/dismiss applications or complaints which are deemed broadly vague, unfounded or are submitted inappropriately or anonymously. On the other hand, petitions, complaints and questions can be examined by priority on the basis of their importance and general interest of the issue.

Additionally to what it has already been mentioned in answer 1.9, we intend to ratify shortly the Cybercrime Convention and to transpose into the national law the Directive 2013/40/EU on attacks against information systems, as well as the additional protocol to the aforementioned Convention, signed on 01/28/2003 and not ratified yet.

The aim is that all the necessary steps for this transposition to be fulfilled as soon as possible. A special legislative committee working on this purpose has almost finished its work, so a draft of the relevant law will be forwarded to the Parliament immediately.

The delay of this procedure is due to the heavy schedule of both the Ministry and the Parliament, resulting of the strong effort of Greece to take all the necessary measures (legislative and structural) in order to accomplish its obligations towards the EU and the IMF according to the financial facility agreement.

Three, up to date, opinion reports given by the Chief Public Prosecutor are referring to communication privacy.

It is characteristically reported that requests by district attorneys, interrogative and pre-interrogative authorities addressed to providers of electronic communication (fixed-mobile telephony, internet etc.), concerning the identities of persons, do not violate Constitution.

The Directive 2013/40/EU has not been transposed yet.

Nevertheless, a special legislative committee has been established for the incorporation of the Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems (replacing Council Framework Decision 2005/222/JHA), under Greek Law, as well as the re-examination, updating and re-drafting of the draft law that has been drafted for the transposition of the Council of Europe (CoE) Convention on Cybercrime into national law (it should be noted that the update of this draft law is necessary as it transposes into national legislation the provisions of the Framework Decision 2005/222/JHA).

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

The directive has been transposed by the L. 4267/2014.

The integration has caused changes to the already applicable crimes as per articles 348 A, 348 B, 339 par. 4 of the Criminal Code, by introducing the crime of the pornographic minors' depictions as per 348C. As far as to the enactment of executive measures for the provisions of the Directive, it is noted that difficulties have been detected in the article 10 thereof (the Directive) for the access to the criminal records of persons having regular contacts with children, since such access, according to the Directive, is made in compliance with the national law (par.2) which, according to the Hellenic Code of Criminal Procedure and the l. 2472/1997, determined specifically who can have access to information related to criminal convictions or prosecutions. Also, the Directive prescribes the exchange of such information via the provisions of the Decision-Framework 2009/315/DEY which has not yet transposed into the national legal order. In the article 10 par.2 of the Directive, there is enacted the obligation of the States Members to take measures that will ensure the employers' right to ask for information according to the national law and in every advisable mode, as the access upon request (to the criminal records of persons), while in the point 41 of the preamble thereof, it is stressed the respect to the legal traditions of the States Members and the non establishment, by the said Directive, of any obligation for modification of the national systems that govern the criminal records. Furthermore, while in the par. 3 of the article 10 of the Directive for the exchange of that kind of information, reference is made to the provisions of the Decision-Framework 2009/315/DEY.

Another issue concerned the programs or the intervention measures for the minimization of the risk for the repetition of such crimes against children (art. 24 of the Directive) and especially the evaluation of the dangerousness of such persons for the determination of the programs or the interventional measures.

As to the behaviors that need to be standardized as crimes, according to the article 5 of the Directive, in the par. 3 it is prescribed that the knowingly acquisition of access to child pornography via the information and communication technology, is punished by custodial sentence the maximum limit of which is one year at least. It is not however determined in the text, the meaning of the term "knowingly" and only in the preamble, point 18, it is explained that, in order for responsibility to exist, the person will have to have pursued the access to a website where such material is available and to know that there will be such pictures. The voluntary nature will have, according to the Preamble, to be concluded from the fact that the offence has been committed via payment service or by repetition. On the contrary, it leaves to the discretion of the State Member to assess whether the acquisition or possession of child pornography material or the production thereof which concerns pictures' imprint made for own use and provided there is no risk of dispersion, and to judge whether such person will be punished or not (article 5 par. 8). The knowingly violation however, must imperatively be standardized as criminal fact.

C/ Online Card fraud

The citizens (complainant or attorney-at-law) as well as the private companies are entitled to file a sworn examination-complaint report concerning fraud via the Internet, to the law enforcement authorities and the District Attorneys' Authorities. The submission of a complaint to the law enforcement authorities may be effected either at the locally competent police station of the area where the citizen lives or the company has its seat, or directly to the Di.E.C.P. by physical presence.

The submission of a complaint, except for the law enforcement authorities, may be submitted, according to the paragraph 2 of the article 42 of the Code of Criminal Procedure, directly to the district attorney of magistrates.

Additionally, the citizens and the private companies are entitled to file complaints for offences related to online fraud by the use of Di.E.C.P. payment card, via an e-mail message since this is an *ex officio* offence.

There is cooperation and mutual updating between the National Authority for the Confrontation of Cyber Attacks and the banking sector for cyber attacks incidents as well as tools-techniques that are used b the attackers.

There is effective cooperation between banks and LEAs to prevent and fight online card fraud.
In the HBA, a dedicated Interbanking Committee has been created for encountering fraud in the payment systems. Members of this Committee are representatives of the Banks, the Bank of Greece and the Hellenic Police. In the Committee, the new trends of fraud, incidents and countermeasures/ technologies are discussed in order to take appropriate measures. Inside this Committee, an alert contact list operates with contact details of the competent representatives. The contact list is concerning any kind of payment card fraud incidents (e.g. ATM & POS skimming, e-commerce fraud, etc.)

- **notify police/LEA if they become aware of any abuse of new payment tools developed by industry?**

The law enforcement authorities are in cooperation with the private sector of the country. Especially, as to the credit institutes of the country, in the context of the interbanking committee for the prevention and confrontation of fraud in the means and he payment systems as well as the *ad hoc* interbanking task group that receives updating with confidential content, transferred by Europol, there is made an exchange of confidential information via the European Central Bank and EC3 which concern new methods or new tools of payment. Respectively, the exchange of confidential information in national level between the credit institutes and the law enforcement principles, is made via the work group for fighting against internet fraud).

- **increase the security of non-cash payment and minimize the vulnerability of magnetic stripes?**

For the most effective cooperation between the private sector and the law enforcement authorities, Di.E.C.P., in the context of its authorities, make sensitization updates to the private sector with regard to new tendencies in the topic of the online frauds as well as provision of advice for taking appropriate prevention measures.

The adoption of the new EMV technology in the total of the portfolio cards from the credit institutes of the country, results now to the reinforcement, to the maximum extent, of the security in the payments by the presence of card, thus minimizing the vulnerability of the magnetic tapes.
Greek payment cards industry is EMV/chip and PIN oriented. Anti-fraud monitoring systems for payment card transactions have been implemented by all issuing banks. Special security routines are taking place when a Greek payment card is used abroad and more specifically on a non-EMV country (e.g. USA).

- **strengthen the authorisation of online transactions and authentication of customers?**

For fighting against the frauds through the Internet, every company has adopted its own system of protection from frauds. The systems for the protection from frauds, perform controls in real time, for the detection of cases of fraud in the online internet transactions by the use of payment cards.
As to the credit institutes of the country, there is a channel of communication and direct cooperation between them for the reinforcement of the procedure for the verification of the clients' details aiming to the timely restriction of the fraudulent transactions.

Greek Banks have set up a state of the art on-line payment infrastructure and sophisticated and efficient security measures such as:

- Specialized security mechanisms of multiple levels of defense.
- Monitoring and detection of fraudulent card transactions.
- MasterCard® SecureCode™ or Verified by VISA services as authentication services of the identity of the cardholder during purchases over the internet.

On top of all that, in the last years, banks have been educating customers not to share their card data (card number, PIN, CCV2) as well personal data (such as ID number, birth date) with anybody and protect them adequately.

5.2. Procedural issues

5.2.1. Investigative Techniques

All the special investigative techniques **mentioned in the questionnaire** are allowed by the national law. To The 7th Department of Digital Evidence Examination of the Directorate of Criminal Researches, based on the article 30 par.22 of the P.D. 178/204, in combination with the articles 183-208, 243, 251, 333, 362 and 458 of the Code of Criminal Procedure, makes forensic examinations on the digital evidence sent by the Pre-Interrogative/Interrogative Authorities. Therefore, these Authorities are responsible for the pre-interrogatory procedure (such as research, confiscation, trapping in a real time/collection of trafficked data/content etc.). After confiscation, this evidence is sent for further forensic examination, asking by clear questions, for data/information related to the case in question.

In the end of the examination a Forensics Report is drafted which, escorted by the digital evidence, is sent to the Requesting Service. It is worth mentioning that the mentioned Department assists the Pre-Interrogatory/Interrogatory Authorities by providing technical information at any stage of the pre-interrogatory procedure and especially the stage of the digital evidence confiscation. Finally, the total of the actions undertaken since the moment of the evidence' receipt until the preparation of the Forensics' Report and shipment thereof, are implemented by specific procedures that are described in the Standards I.S.O. (ELOT EN ISO 9001:2008, ELOT EN ISO/IEC 17020) and are in compliance with the Principles and the Guidelines of the European Network of Forensic Science Institutes (ENFSI).

According to Article 19 par. 1 point h) of law 2472/1997, the HDPA has the power to conduct inspections following a complaint. In the course of these inspections, it has the right to access personal data and to collect any kind of information for the purpose of the investigation, notwithstanding any kind of confidentiality.

The procedure for the lawful interception of communications is set out in Presidential Decree 47/2005 "Procedure, technical and organizational guarantees for ensuring lawful interception" (G.G.A'64/10.03.2005).

The main special techniques of investigation used for fighting against minors' pornography is the use of a specialized software or the on-line discovery of trafficking of such material or interrogative penetration techniques, to wit, upon relevant Ordinance, we are allowed to use-manage profiles that pretend minors or minors' pornography material traffickers. Additionally, there is a close cooperation with Europol and Interpol while we have been recently integrated in the Interpol base for the recognition of minor victims of sexual harassment.

Additionally, the Department of Examination of Digital Evidence, Directorate of Criminal Investigations, at the examination of the digital evidence in cases of electronic crime, follows appropriate and internationally recognized criminal procedures.

HDPA uses a variety of techniques, the most common of which is simulating the perpetrator's modus operandi regarding the programs used for the illicit activity. This has been done in 2 ways; a) virtualizing in read-only mode the forensic copy of the perpetrator's computer(s) hard disk. b) Executing a perpetrator's program (ex. a spammer's mass mailer) in a sandboxed environment and loading in the program all items related to the perpetrator's usage of the program (ex. configuration files, mail campaigns data, etc).

The Directorate of Electronic Crime Prosecution, using interrogatory penetration, managed to trace down seventy eight (78) persons, who communicate minors' pornographic material via a specific website; these persons were traced in thirty two (32) different countries. As far as Greece is concerned, three (3) users have been identified.

As to digital evidence examination, a good practice related to creation of a fictitious copy, in cases that the hard discs to be examined present many reading errors, is copying of sectors in reverse order and not the usual procedure.

The lesson one always learns by using cybercrime investigation techniques is that each case is unique and that tools used in one case will not necessarily work in every case. So one must, as best practices also describe, know its tools to the extent that one knows what they are capable of, if they change data (in regards to volatile data collection tools) and what their data flows are. This has to be done in order a) to produce forensically sound reports and b) to be able to constantly improve one's methodology by incorporating in the process, lessons learned from each specific investigation.

5.2.2. Forensics and Encryption

The Department of Examination of Digital Evidence, Directorate of Criminal Investigations makes only electronic forensic examination of the subjected evidence and not a distant examination. Criminal examination of digital evidence is ruled by specific principles, which should be unswervingly respected, in order to establish proof and guarantee credibility of the laboratory examinations and findings. These principles are prescribed and analytically described in the I.S.O. procedures of the mentioned Service.

HDPA has not performed remote forensic examination, but they are performing forensic examination and analysis of collected evidence in the lab that they have in the premises of the HDPA. This examination entails volatile and non-volatile data ranging from web server log files to memory images and forensic copies of acquired hard disks. During the examination they use both open-source (ex. Volatility Memory Forensics Framework) and commercial tools (ex. Encase), in order to find the perpetrators' modus operandi, the traces of his activity and correlate all found evidence to other possible illicit activities performed by other third parties previously unknown to us (perpetrator's clientele, suppliers, etc.).

Encryption might be the biggest problem of the forensic examination of the digital evidence since, in case of non-successful decryption, there is not the ability of examination and therefore there is no information given to the requesting Authorities. For the decryption of the data, the Hellenic Police, uses a special criminal software as well as computers with high processing power.

In case the data have been encrypted either by great number of characters, or by combination of files instead of code, the above mentioned Department cannot decrypt the digital data. In serious case (such as cases of terrorism and organized crime) when the mentioned Department cannot decrypt the data, it is requested the assistance from the EC3 Europol Department.

Additionally, there is no legal framework in which we are given the ability to cooperate with private companies.

HDPA encountered cases where they needed to decrypt files that were zipped and encrypted as well as encrypted excel and word files. These files were decrypted by using tools that either exploit known vulnerabilities or simply brute-force the passwords of these files.

HDPA has also encountered a case where they could not decrypt the suspect's password files due to the suspect's usage of specific password management software whose master key could not be broken with the equipment available.

5.2.3. E-Evidence

Notions as computer data, content data, traffic data, order for search/seizure of information system, networks managed or controlled by suspects of cybercrime are not defined by National Legislation, but only in the Budapest Convention, which however, up to date, has not been integrated in the national legislation. Consequently, only as practice we follow the terms/concepts described in the above mentioned Convention.

Traffic data are defined in article 2 of Law 3471/2006, which transposes Directive 2002/58/EC into the national legal order, includes me definition of "traffic data" .

There is no special regulation for e-evidence. Regarding collection, storage and transfer of e-evidence, HDPA keeps a chain of custody and follow internationally accepted guidelines such as ACPO guidelines.

Article 19 par.3 of the Hellenic Constitution states that the use of evidence acquired in violation of this article and of articles 9 and 9A is prohibited.

During the procedure of confiscation and then submission of the electronic evidence, specific rules should be observed by the Authorities that proceed to confiscation :

1st RULE

No action that is made by the person who proceeds to the seizure, should change the data that are found stored in a computer system or storage mean, which will be later confiscated and sent as a piece of evidence.

2nd RULE

In the case that the person who proceeds to the confiscation, finds necessary the access of the digital data that are stored in a computer system or storage mean, such person will have to be educated to do this and be in a position to substantiate such acts of his, as well as the changes he caused to the digital data and the computer system in general.

3rd RULE

The person who proceeds to the confiscation will have to register in writing, any of his actions on the computer systems and the stored data thereof, which will have to escort the report of seizure and the transfer document to the District Attorney and this Service. By the use of the mentioned notes, a third person will have to be able to end up to the same result, if he makes the same actions.

4th Rule

The Manager of the confiscation at the crime scene has overall responsibility to ensure that the foregoing principles are observed.

Then, the Authorities that have confiscated the digital evidence will have, by their document which should be escorted by the report of confiscation and the transfer document of the requesting Authority to the District Attorney, to contain the following :

- ✓ to contain information related to an offence purported as committed, by the mentioned evidence,
- ✓ to contain information about the holders of the evidence and the perpetrators
- ✓ pointed questions to be clearly expressed, that are in need of forensic reply and may help the interrogative investigation of the crime (not vague and unclear questions, nor only the general question : "anything that accrues from your science"). In case the questions are not clear and specific, the examiner will not be in position to know which are those findings which would help to solving the crime, with the result to be consumed to the examination of the total of the computer systems data, thus consuming time and resources that could be disposed to the examination of another case.

-The description of the evidence should be complete, including manufacturing brand, model, serial number, any attritions or any other feature that makes it unique.

It is worth noting that the Department of Digital Evidence Examination of the Directorate of Criminal Investigation does not accept for examination, any evidence for which the correct process of confiscation, packaging, transfer and safeguarding has not been observed or evidence that does not present criminal interest or does not contain digital data (monitors, keyboards, "mouse" etc.)

Concluding, we would say that the procedure remains as it is, also in the case that the electronic evidence has been received from another E.U. State Member.

5.3. Protection of Human Rights/Fundamental Freedoms

There are competent independent authorities such as the ADAE, EETT and the HDPA that care for the privacy of communications as well as the protection of personal data.

The HDPA is competent for investigating cybercrimes that involve the processing of personal data.

The Hellenic Authority for Communication Security and Privacy (ADAE) was established in 2003 as prescribed by article 19 par.2 of the Hellenic Constitution, which calls for the establishment of an independent authority with the mission to ensure the confidentiality of mail and all other forms of free correspondence and communication.

Details regarding ADAE's powers and functions are given in answer 3.C.1 here below. Law 3471/2006, which transposes Directive 2002/58/EC into the national legal order, designates ADAE as the competent authority for the implementation of article 5 of the Directive ("confidentiality of the communications"), as well as for the implementation of the articles of the Directive which refer to the presentation of calling line identification for the tracing of malicious or nuisance calls and for emergency calls. The same Law designates ADAE, together with the national Data Protection Authority, as the competent national authority to receive data breach notifications. Moreover, ADAE has issued Regulation 165/2011 "for the Assurance of confidentiality in Electronic Communications" (GG B' 2715). Both ADAE's Regulation 165/2011, as well as article 8 of Law 3674/2008 (GG A' 136) include provisions for the immediate notification of communication confidentiality breaches or risk of such breaches to ADAE and to the subscribers concerned.

EETT is the National Regulatory Authority, which supervises and regulates the telecommunications as well as the postal services market. EETT's institutional purpose is to promote the development of the two sectors, to ensure the proper operation of the relevant market in the context of sound competition and to provide for the protection of the interests of the end-users. EETT is an independent self- funded decision-making body.

Article 19(1) of the Hellenic Constitution states that the privacy of correspondence and of free communication in any other way is absolutely inviolable. The law shall determine the guarantees under which the judicial authority is released from the obligation to observe the abovementioned right, for reasons of national security or for the investigation of particularly serious crimes. Law 2225/1994 "For the protection of freedom of correspondence and communication and other Provisions" (G.G.A'l21/20.07.1994) determines the specific serious crimes, the investigation of which justifies the measure of lawful interception of communications, and describes the legal requirements thereof.

According to article 12 of the data protection law (2472/1997), the obligation to inform and the right to access of the data subject may be lifted in whole or in part, provided that the processing of personal data is carried out on national security grounds or for the detection of particularly serious crimes.

Similarly, as per article 3 of the same law, the provision of the law on data protection shall not apply to the processing of personal data carried out by judicial-public prosecution authorities and authorities which act under their supervision in the framework of attributing justice or for their proper operation needs with the aim of verifying crimes which are punished as felonies or misdemeanours with intent, and especially with the aim of verifying crimes against life, against sexual freedom, crimes involving the economic exploitation of sexual life, crimes against personal freedom, against property, against the right to property, violations of legislation regarding drugs, plotting against public order, as well as crimes against minors. This may be applicable when an investigation involves a type of cybercrime that falls also into the above categories of crimes.

5.4. Jurisdiction

5.4.1. Principles applied to the investigation of cybercrime

With reference to the expansion of the jurisdiction of the Hellenic legal order for crimes using the Internet as a mean of their commission, it should be noted that a par.a3 was added to the art. 5 of the Criminal Code, also for the crimes related to the sexual exploitation or maltreatment of minors, the art. 8h of the Criminal Code has been modified. These changes were made by the art. 2 and 3 of the l. 4267/2014 by which, the Directive 2011/93/EU of the European Parliament and the Council was integrated in the national legal order, with regard to the fighting against the sexual harassment and exploitation of children and the child pornography.

The addition of the said provision is an obligation which derives from various legal texts of the European Union, among which is also the Directive integrated by the present draft law as well as the Directive 2013/40/EU concerning the attacks against information systems for which there is also an obligation of compliance.

The addition of the crimes to the article 8 period (h) of the Criminal Code is made in order for the mentioned provisions to harmonize with the paragraphs 1, 2 and 4 of the article 17 of the Directive 2011/93/EC. The foregoing crimes are added because, when turned against the sexual liberty of the minors, they constitute, for the European legal order, serious violations of fundamental rights and especially the rights of the children (point 1 of the Directive's Preamble). For this reason and, in order of their prosecution to become feasible, they are integrated in the principle of universal justice (See Reasoning Report L. 4267/2014).

In accordance with the provision of the article 16 of the Criminal Code, as place of commission of the criminal act is considered the place where the liable party has totally or partially performed the criminal act, action or omission and the place where the criminal result has occurred or should have occurred, according to the perpetrator's intention. The distant crimes, as are those committed via the Internet, as place of commission of the overall crime, is both the place where the criminal behavior was manifested - that is the place where the electronic mail was sent from - as well as the place where the message was received, even if this is found abroad. In the article 5 of the Criminal Code "Crimes committed abroad", by the provision of the article 2 of the L. 4267/2014 the national legislation was harmonized with the Directive 2011/93/EC and a paragraph 3 was added where is mentioned that : "*When the act is committed via the Internet or other Media of communication, as place of commission is considered also the Hellenic State as long as access is provided to the specific Media on its territory, regardless the place where these Media have establishment*".

According to art. 3 par. 3 of the national law 2472/1997, the HDPA is competent for processing, and therefore cybercrime acts committed a) by a Controller or a Processor established in Greek Territory or in a place where Greek law applies by virtue of public international law, and b) by a Controller who is not established in the territory of a member-state of the European Union or of a member of the European Economic Area (EEA) but in a third country and who, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the Greek territory, unless such equipment is used only for purposes of transit through such territory. In this case, the Controller must designate in writing, by a statement addressed to the Authority, a representative established in the Greek territory, who will substitute the Controller to all the Controller's rights and duties, without prejudice to any liability the latter may be subject to.

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

The assistance of EUROJUST is very significant since, by the organization of Coordinative Groups between the Judicial or/and the Police Authorities of the States involved, in cases that concern several States-Members, the solution of the problem of any parallel jurisdiction is achieved as well as the avoidance of several prosecutions starting against the same perpetrator for the same criminal acts in the cyber space.

HDPA do not investigate acts committed outside the respective territory. In case the HDPA becomes aware of such an act in the course of an investigation, they will forward to the respective national DPA (in case the act takes place in EU MS) all the relevant records and evidence.

As to the predictions of the Decision-Framework 2009/948/DEY for the prevention and the settlement of jurisdiction conflicts in criminal matters in the context of the European Union, it is noted that it has not been integrated in the national legal order, but it has been established, a special legal preparation committee (no. 84295/4-11-2013 Decision of the Minister of Justice, Transparency and Human Rights) which has completed its task and has filed the relevant texts to the competent Ministry.

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

Greece does not have any relevant experience. However, in case that such a matter would arise in the context of criminal proceedings, the EUROJUST and EUROPOL channel could be used.

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

The legal context in Greece has not fully incorporated the cases of the crimes committed by the use of the Internet in its total. An effort is made for the modernization of the legal provisions but there are still remain pending, many necessary changes to be implemented, especially via the ratification of the Convention of Budapest.

As to the existing legal framework, with regard to the investigation of the electronic evidence, this is considered to be sufficient.

5.5. Conclusions

- Greece signed (23.01.2001) but has not ratified the Council of Europe Convention on Cybercrime. Subsequently the Additional Protocol to Convention on Cybercrime was neither ratified.
- Directive 2011/93/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography was transposed into national law (4267/2014).
- In relation to the investigative techniques, there are a number of measures for seizing and retaining data for the purpose of gathering evidence.
- Cybercrime committed via the "cloud" was highlighted during the evaluation visit as an area creating issues for investigation and prosecution, particularly in relation to retrieving the actual physical location of data. The method of cloud computing creates a problem not only with regard to the national law but also to international legislation which is based on the acknowledgement of states' independence.

- European Council Convention on the protection of children against sexual exploitation and sexual abuse has been ratified. The article 348 A Criminal Code was amended and also enacted the disqualification of people who has been convicted of any of these offences temporarily or permanently from exercising at least professional activities involving direct and regular contacts with children. This sanction is also provided by the Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. Online grooming is criminalized in Greece.
- In the national criminal law the definition of child pornography material is wider than set in the Directive. According to that definition (art. 348 A par. 3 Criminal Code) the depiction or the representation could include not only the sexual organs of a child but the body in general as well. It is also considered a crime when a child witnesses sexual activities despite the fact that he or she has or has not reached the age of sexual consent.
- There is also a special measure provided by art. 73 para. 3 Criminal Code which requires to the convicted person to announce the police their home address and inform for the next three years about every change to that, in case of a second conviction.

6. OPERATIONAL ASPECTS

6.1. Cyber attacks

6.1.1. Nature of cyber attacks

According to the National Defense General Headquarters (NDGH), the incidents mostly concern networks scans, receipt of malicious electronic correspondence and networks' and computers' control by the use of virus-like software.

Based on information of the National CERT, basic categories of attacks to the cyber space that have taken place in Greece, are the following:

1) Defacements in websites
2) Denials of Services (DOS) attacks
3) Acquisition of non authorized access to information systems
4) Acquisition of access to data bases – SQL Injections
5) Posts of malicious files with the purpose of either phishing (username, passwords) or the distribution of malicious software that will convert the user downloading the same to a botnet member.
6) Spear phishing mail attacks
7) Ransomware

6.1.2. Mechanism to respond to cyber attacks

The National Authority for the Confrontation of Cyber Attacks is the competent governmental authority that coordinates the confrontation of the cyber attacks between the parties involved, as far as this concerns the public sector or crucial infrastructures. Also, in cases of quite extended cyber attack, it will notify the security services.

Greece has signed and integrated in the Hellenic legal order, many bilateral and multi-lateral conventions regarding Judicial Cooperation in criminal matters. Conventions which constitute sufficient grounds for the fulfillment of Requests of Judicial Assistance with object the crime in the cyber space. Also, in the cases there is no bilateral or multilateral convention, applicable is the Principle of Mutuality according to what is particularly prescribed in the article 457 et seq. of the Hellenic Code of Criminal Procedure.

6.2. Actions against child pornography and sexual abuse online

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

The Department of Digital Evidence Examination of the Directorate of Criminal Investigations contributes to the database of Interpol "International Child Sexual Exploitation Database" that is related to the recognition of children victims of sexual abuse.

The competent authorities proceed to confiscation of the hard disks with the illegal content. The illegal pictures and the illegal videos are integrated in the relevant national and international (especially EUROPOL's) databases so that a potential new supply or trafficking be prosecuted.

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

Di.E.C.P. officers carry constant events-daily congresses throughout the Hellenic State regarding the confrontation of the above issues. Additionally, in cooperation with the Ministry of Education and Religion, there are implemented twice (2) every week during the school year, updates via special suite, in all schools of the country. In this mode it is achieved that all students get to know the Internet traps and the modes of confronting them.

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

By the article 2 par. 5 of the L. 3625/2007 "Ratification, implementation of the Optional Protocol to the Convention for the Rights of the Children, with regard to the children trade, the child adultery, the child pornography and other provisions" the article 323 B of the Criminal Code was added entitled "Making trips aiming to committing sexual intercourse or other lecherous acts against a minor (sexual tourism)". According to the content of the article 323 B of the Criminal Code, anyone who organizes, funds, directs, supervises, advertises or mediates in any mode or by any mean whatsoever, for making trips aiming to committing sexual intercourse or other lecherous acts against a minor, is punished to a degree of felony. Anyone who, with the mentioned intention participates in trips as per foregoing sentence, is punished to a degree of offence, regardless his liability for the commission of other criminal acts.

Additionally, by the article 2 par. 1 of the L. 36252007, as replaced with the article 3 L. 4267/2014, it was prescribed in the article 8 of the Criminal Code "Crimes committed abroad that are always punished according to the Greek laws" that the Greek criminal laws apply on natives and foreigners, regardless the laws of the place of commission, for the act, among others of "making trips aiming to commission of sexual intercourse or other lecherous acts against minors".

The protection of the minors is among the basic priorities of the Hellenic Police Headquarters, as these accrue from the Program of Anti-Crime Policy of the years 2015-2019 (Question 1.1.) and is integrated in the central core of its interest. In such content, particular goals have been set, that concern mainly the protection of the students' community and the cooperation with competent agencies of minors' protection, via the development of particular actions which include among others:

- ✓ Specialized actions for the minors aiming mainly to their protection from drugs, the dissuasion of their participation in criminal groups and their protection from the possibility of their victimization.
- ✓ Surveillance of areas where minors hang out or remain such as school areas, private institutes, sporting campuses, parks, playgrounds etc. Continuation of cooperation with the co-competent Ministries and the rest of the agencies (school communities, associations etc.) for taking the requisite measures, aiming to the security and protection of the students and the schools.
- ✓ Development of contacts and cooperation with co-competent public and private agencies and organizations in issues of minors.
- ✓ Updating of the staff for the activation of the AMBER ALERT system that concerns to the timely warning in cases of minors' disappearance, developing the required cooperation.
- ✓ Sensitization and education of the staff that handles cases of minors (victims' assistance-perpetrators' treatment)

Additionally, for the protection of the minors, specialized Services of the Hellenic Police have been established and operate.

In central level, in the structure of the Directorate of Public Security of the Hellenic Police Headquarters, it operates the Department for the Fighting of Drugs and Minors' Delinquency, which is a Headquarters Service, of strategic nature, which has been assigned with the follow up of the delinquency and the victimization of minors.

In regional-operational level, the following apply :

- ✓ The Sub-Directorate of Minors Protection of the Directorate of Security of Attica, which is structured in two (2) Departments, to wit the Department of Minors' Surveillance and the Department of Minors' Special treatment.
- ✓ The Department of Minors of the Directorate of Security of Thessaloniki.
- ✓ The Minors Offices of the Sub-Directorates of Security of Herakleion-Crete and Patras.

It is noted that, up to date, from the mentioned Services as well as from the rest competent Services of the Hellenic Police (Sub-Directorates and Departments of Security throughout the State), it has not been verified the violation of the article 323B of the Criminal Code. In a similar case, there will be applied by them, the relevant mentioned legislation against the violators thereof.

There have been developed specific measures to counteract real time web-based child pornographic performance by the use of a special software (Child Protection System), which allows the use of the online trafficking of minors pornography material via P2P networks.

An NGO, "The Smile of The Child" (SotC), operates the SOS 1056 Helpline since 1997. In 2007 it was recognised by the Ministry of Health and Social Solidarity as "the National Helpline for Children". The Helpline is staffed by Social workers and Psychologists and operates 24/7. The calls are free of charge and all telephone conversations are confidential and are NOT recorded. Through the Helpline we receive formal complaints for children victims of cybercrime which are sent to the component authorities (prosecutors and law enforcement) in order to investigate them.

The Helpline is interconnected to the European Emergency Number 112 of the Civil Protection Secretariat and it is recognized as an Emergency line. Furthermore, "The Smile of the Child" have signed a Memorandum of Understanding with the Ministry of Citizen's Protection determining that "The Smile of the Child" will receive formal complaints for children victims of cyber-crimes. During 2014 the National Helpline SOS 1056 received 283.369 calls.

"The Smile of The Child" operates the European Hotline for Missing Children 116000 since 2008. It is staffed by Social workers and Psychologists and operates 24/7 and the calls are anonymous and free of charge. The Hotline is interconnected to the European Emergency Number 112 of the Civil Protection Secretariat and it is recognized as an Emergency line. Through the Hotline which is operational in 29 countries (27 EU MS, Albania & Serbia) "The Smile of The Child" we receives calls regarding missing and exploited children. In 2014 the 116 000 received 7.151 calls.

- **developing information tools for children for safe use of Internet;**

Digital Services

The National Helpline SOS 1056 line operates a free, 24/7 emergency and counselling digital service for children and teenagers (up to 18 years) in Greece using Social Media and conventional email, available also to adults with concerns about children, which is strictly confidential and on a one-on-one basis. The Digital Service of the Helpline provides:

- Psychological support for children and teenagers, as well as counselling for parents and educators using Social Media (Facebook,Twitter, Instagram, Youtube), email and an instant chat application (to be established);
- Reference to the telephone Helpline for registering anonymous and named complaints regarding children who are victims of abuse or neglect;
- Reference to the Telephone Helpline of requests from authorities, organizations, services, or the general public;
- Dissemination of information about cyber-crime through Social Media and emails, Website (primary prevention- awareness raising)
- Monitoring and evaluation of information and referral to authorities (secondary prevention);

- In cases of victims of cyber-bullying "The Smile of the Child" upon the request of the authorities provides psychological support to the child and the family;
- Raising awareness in matters concerning children's rights and protection through Social Media and the Website;
- Training programs using Pod Cast format (Webinars and Video Web Casts) to parents, scientists and the general public, about child protection and well –being (primary prevention).

• **developing information tools on harmful/illegal behaviour online?**

"The Smile of the Child" is in the process of using new digital tools in cooperation with international authorities and partners for the purposes of combating child pornography and other cybercrimes setting these tools to the disposal of law enforcement authorities.

In the context of the Hellenic Police, there has been developed a special round-the-clock call center of complaints (11188) within the Directorate of Electronic Crime Prosecution where specialized officers deal with every incident, including those that require immediate handling (i.e. suicidal intention signs). Additionally, a safe website (www.cyberkid.gr) has been created by the staff of the mentioned Service, where the minors as well as the parents may, via interactive activities and constant updating, be informed about the modes of safer surfing. Additionally, for mobiles and tablets, there has been created a free application with useful information regarding the internet surfing while a phone call is automatically made to the call center of this Service by simply pressing a button.

Di.E.C.P. officers carry constant events-daily congresses throughout the Hellenic State regarding the confrontation of the above issues. Additionally, in cooperation with the Ministry of Education and Religion, there are implemented twice (2) every week during the school year, updates via special suite, in all schools of the country. In this mode it is achieved that all student get to know the Internet traps and the modes of confronting the same.

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

Filtering, access blockage and website removal are applied.

The national authorities use a special software (Child Protection System) that makes possible control of the online trafficking of minors' pornography material via P2P networks.

Upon relevant request to the District Attorney's Authorities and the issuance of an Order, the N.C.P.C. or the Internet access providers are obligated to remove the website that contains minors' pornography materials.

The procedure is as follows:

a. If the web page is hosted in territory and the Hosting Internet Service Provider (HISP) is known, then the competent authority orders the HISP to deactivate or remove the web page.
b. If the HISP is unknown and the web page is under a .gr domain name, then the competent authority orders the Hellenic Telecommunications & Post Commission to temporarily deactivate the domain name for a period of two months. Within the above period of time, the owner of the domain name can appeal to the prosecutor. Within a period of two months, the prosecutor issues a final decision regarding either the removal or the reactivation of the domain name. If there is no reaction on behalf of the owner, the domain name is permanently removed.

In these cases where the server is abroad there is a close cooperation via the Directorate of International Police Cooperation with the Europol and Interpol Units for their updating and their own further actions, due to material and local competence.

c. In case a web page is not hosted in territory and is not under a .gr domain name, then the competent authority decides to block access to the web page. The respective decision shall be notified to EETT. EETT informs the Internet Service Providers asking them to immediately block the access to the web page and to inform their customers. The respective decision shall be notified to the owner of the web page, who can appeal to the prosecutor. Within a period of two months, the prosecutor issues a final decision regarding the access blocking of the web page.

The Directorate of Electronic Crime Prosecution of the Hellenic police use as communication channels with other countries INTERPOL, Europol and SIRENE Departments of the Directorate of International Police Cooperation.

6.3. Online card fraud

6.3.1. Online reporting

The citizens (complainant or attorney-at-law) as well as the private companies are entitled to file a sworn examination-complaint report concerning fraud via the Internet, to the law enforcement authorities and the District Attorneys' Authorities. The submission of a complaint to the law enforcement authorities may be effected either at the locally competent police station of the area where the citizen lives or the company has its seat, or directly to the Di.E.C.P. by physical presence.

The submission of a complaint, except for the law enforcement authorities, may be submitted, according to the paragraph 2 of the article 42 of the Code of Criminal Procedure, directly to the district attorney of magistrates.

Additionally, the citizens and the private companies are entitled to file complaints for offences related to online fraud by the use of Di.E.C.P. payment card, via an e-mail message since this is an *ex officio* offence.

There is cooperation and mutual updating between the National Authority for the Confrontation of Cyber Attacks and the banking sector for cyber attacks incidents as well as tools-techniques that are used b the attackers.

6.3.2. Role of the private sector

The private sector may notify cyber attacks, without however being obliged to, electronic attacks incidents to the cyber space, on the National Authority for the Confrontation of Cyber Attacks and get advice of handling as well as business-technical assistance from it, for the confrontation of the incidents if requested.

Credit institutions operating in Greece are obliged to report without causal delay cyber-attack incidents that target both the credit institutions and/or their customers. The report is addressed to the Bank of Greece as well as to the SSM of the ECB. As a matter of close cooperation the report is also addressed to the Cyber Crime Division of the Hellenic Police although there is no such an obligation for the credit institutions.

The HBA created and maintains two alert contact lists with contact details of the competent representatives of credit institutions, Cyber Crime Division of the Hellenic Police and Bank of Greece. The 1st alert contact list is concerning any kind of payment card fraud incidents (e.g. ATM & POS skimming, e-commerce fraud, etc.) whereas the 2nd alert contact list is concerning any kind of internet fraud (e.g. sophisticated phishing techniques, identity theft, sharing of customer secret credentials with third parties and man-in-the-middle/browser attacks which intercept/modify/divert customer data, malware, social engineering, DDoS and breaching the perimeter zone, etc.).

Law 3471/2006 (GG A' 133), which transposes Directive 2002/58/EC into the national legal order, designates ADAE, together with the national Data Protection Authority, as the competent national authority to receive data breach notifications. Moreover, ADAE has issued Regulation 165/2011 "for the Assurance of confidentiality in Electronic Communications" (GG B' 2715). Both ADAE's Regulation 165/2011, as well as article 8 of Law 3674/2008 (GG A' 136) include provisions for the immediate notification of communication confidentiality breaches or risk of such breaches to ADAE and to the subscribers concerned.

6.4. Other cybercrime phenomena

According to the no. 15/2011 (Gov. Gaz. B’419/16.03.2011) decision of the Communication Privacy Protection Authority (C.P.P.A.), the Credit Institutes care for the direct protection of the users during the use of the Automatic Teller Machines (ATMs) as well as for the users’ correct and valid update regarding the dangers that might threat the privacy of the communication when using the ATMs. Additionally, the credit institutes care for the physical protection of the ATMs as well as for the material used for the provision of services by them.

From the above it accrues that the basic competence to restrict the access of the organized crime groups to financial data and certifications, is held by the credit institutes themselves, via the obligation to secure their computer information system.

As to the restriction of access of the organized crime groups to skimming devices, software and know-how, it should be stressed that the majority of software was not provided by domestic suppliers and almost the total number of the arrested persons involved in skimming incidents were foreign citizens.

Credit institutions have organization charts for information security governance (CISOs, Information Security Units) in place, as well as strong information security frameworks which include security policies, procedures and standards.

Regarding security infrastructure, they have implemented perimeter and internal specialized security measures, in a multiple level of defense model and in separate zones. Based on each bank's internal policy, security measures include, amongst others:

Network firewalls,
Web application and database firewalls,
IPSs – Intrusion Prevention Systems,
IDSs – Intrusion Detection Systems,

- DDos (Distributed Denial of Service Attacks) security systems,
- Data Leakage Prevention,
- Malware protection,
- Content filtering,
- Strong access control mechanisms,
- SIEM (Security Information and Event Management) Systems, which identify (24X7X365) and prevent on timely potential intrusions.

Furthermore, credit institutions carry out security checks (penetration tests, vulnerability assessments) periodically both internally and in collaboration with external partners according to the provisions of the Bank of Greece Governor's Act No. 2577/2006. They also certify that their Operating System of applications is fully updated with the latest patches.

ATMs are secured (at the system and network level) and equipped with anti-skimming/antifraud devices and antimalware software.

A close cooperation among the CISOs of the Greek banks, the Hellenic Police Cybercrime Unit and the Bank of Greece exists through the HBA Interbank Committee and/or on an one-to-one basis for exchanging of information and adoption of common security measures and practices. Additionally, they are in constant communication with representatives of the ATM manufacturers (e.g. NCR, Wincor Nixdorf, Diebold, etc.) in Greece for information and exchange of views.

Last but not least credit institutions have been already certified or are under the final phase of their certification process according to the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing payment card security process including prevention, detection and appropriate reaction to security actions.

6.5. Conclusions

- The Criminal Code incriminates the sexual tourism as an offence "Making trips aiming to committing sexual intercourse or other lecherous acts against a minor", so it goes beyond the minimum standards provided by the Directive against child pornography.
- Another good practice is the possibility provided by national law to filter, access blocking and removal of websites related to the child pornography phenomenon.
- It must be highlighted that the Department of Digital Evidence Examination of the Directorate of Criminal Investigations has access to the Interpol "International Child Sexual Exploitation Database".
- The evaluation team considers as a good practice the fact that credit institutions operating in Greece are obliged to report without delay cyber-attack incidents that target both the credit institutions and/or their customers. The report must be addressed to the Bank of Greece. As a matter of close cooperation the report is also addressed to the Cyber Crime Division of the Hellenic Police although there is no such an obligation for the credit institutions.
- Good practice example is also the establishment within the HBA the Interbanking Committee with representatives of the banks, the Bank of Greece and the Hellenic Police. In the Committee, the new trends of fraud, incidents and countermeasures/technologies are discussed in order to take appropriate measures. In order to respond quickly the Hellenic Banking Association maintains alert contact lists regarding to cybercrime (skimming, e-commerce fraud, cyberattack, internet fraud, etc.).

7. INTERNATIONAL COOPERATION

7.1. Cooperation with EU agencies

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

No special requirements or particular provisions are provided by the national legislation, concerning the cooperation of the National Authorities with Eurojust, Europol EC3 and ENISA in the cyber crime cases, since the common framework is applicable as for every other offence.

Greek banking sector is in cooperation with the Cyber Crime Division of the Hellenic Police and participates in Europol/EC3 project concerning the "Intelligence Requirement on Banking Malware.

On September 2014 the European Banking Federation (EBF) and Europol's European Cybercrime Centre (EC3) signed a Memorandum of Understanding (MoU) which paves the way for intensifying cooperation between law enforcement and the financial sector in the EU.

The MoU allows the exchange of expertise, statistics and other strategic information between both parties. It will facilitate the exchange of data on threats to enable financial institutions to protect themselves, whilst the immediate reporting of new malware and evolving means of payment fraud allow law enforcement to investigate and arrest the perpetrators. HBA as a member of the EBF participates actively on this EBF/EUROPOL-EC3 initiative.

Concerning the ENISA cooperation, HBA also actively participates on ENISAs Expert Group for Finance ICT (EG-FI).

HBA participates in EBF/Cyber Security Group and EPC/Payment Security Support Group and it also supports the Crime Cyber Crime Division of the Hellenic Police in its European leadership in EMPACT project regarding the customer's security awareness.

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

Greece disposes of experience of cooperation with the above mentioned organizations. Especially, in Eurojust, two cases were introduced in 2014 (one for child pornography and one for fraud via Internet) and three cases in 2015 (slanderous defamations via the Internet).

Di.E.C.P. cooperates on every day level via Europol with competent foreign authorities as well as with Eurojust via a request of judicial assistance in making case solving and perpetrators arrest easier as well as getting information (intelligence).

In particular, Di.E.C.P. had a case related to illegal betting via the Internet, which needed cooperation via Europol channel with foreign countries for exchange of information and provision of evidence.

The National CERT directly cooperates with ENISA especially in :

1) It has participated in the planning and the performance of all three European Cyber Exercises organized by ENISA. Also, there is cooperation with ENISA in order for a National Strategy of Cyber Security to be drafted. Finally, it participates on regular basis in workshops and trainings of ENISA.

2) Also, the National CERT contributes to the coordinated efforts made at Europol/EC3 aiming to reacting to cyber attacks, such as the taking-down Ramnit botnet.

The contribution of the Europol/EC3, Eurojust and ENISA in international cooperation is very useful, since they assist to the acceleration and analysis of the requests. The cooperation experience of Eurojust with EC3 is positive since EC3, as capable of taking knowledge of the newer modus operandi in the cyber crimes, may proceed also to a successful strategic analysis.

The cooperation with Europol/EC3 aims to preventing and fighting serious international criminal activities via the Internet. NISA assists to the formation of political and publication of best practices for the prevention and fighting against the cyber crimes.

Greece participates in the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol, represented by the Director of the Directorate of Electronic Crime Prosecution.

7.1.3. Operational performance of JITs and cyber patrols

Up to date, Greece has not participated in JITS and cyber patrols and no EU funds have been used up to date.

It is however noted that specialized staff makes every day Internet inspections, with further purpose the prevention and suppression of the Internet crimes committed in the Worldwide Web.

7.2. Cooperation between the Greece authorities and Interpol

The Directorate of Electronic Crime Prosecution was very recently connected to the said database and the quality's connection was satisfactory. The use of such database is expected to expand the operational capacity of the mentioned Service in fighting against the phenomenon of child pornography, with parallel upgrading of the role of Greece to the global alliance for the confrontation of the child sexual exploitation.

It is also noted that, during the period as of 27th to 29th May 2015, staff of the mentioned Service and particularly, the Department of Minors' Internet Protection and Digital Investigation was trained at its premises by two INTERPOL instructors.

Furthermore, the Department of Digital Evidence Examinations of the Directorate of Criminal Investigations contributes to the data base of Interpol "International Child Sexual Exploitation Database" .

Greece is one of the founding members of INTERPOL. The competent National Central Office of INTERPOL at the Directorate of International Police Cooperation of the Hellenic Police Headquarters, is the contact point with the INTERPOL's General Secretariat. Via the National Central Office of Interpol, Greece exchanges information regarding crimes in the cyber space and participates in all initiatives taken by the INTERPOL's General Secretariat.

7.3. Cooperation with third states

The national policy applies the provisions and bilateral agreements related to police and judicial cooperation.

Europol offered assistance via the AWF SOC F.P. TWINS and the EUROPOL file exchange program.

EUROJUST decisively contributes to the cooperation with third states via the cooperation of the National Offices with the contact links that exist in the third states.

7.4. Cooperation with the private sector

Di.E.C.P. has developed a cooperation with the domestic air companies and travelling agencies. In particular, the latter, in case they detect suspect of fraud transactions (air ticket bookings) by making use of a payment card, send this information to Di.E.C.P. and then the information is transferred to the competent police authorities of the respective departure airport of the passenger. The further aim of this procedure is the participation of all air companies active and the report of suspects for transactional fraud concerning passenger flights departing from the airports of the country.

Credit institutions operating in Greece try to overcome any obstacles through enduring cooperation with:

- the international payment schemes (VISA/ MasterCard / AmEx / Diners / China Unionpay)
- the Cyber Crime Division of the Hellenic Police which afterwards informs Europol
- the competent contact persons of foreign financial institutions that issue or acquire payment cards transactions.

Furthermore, as a pan-European banking sector initiative (from the Payment Security Support Group of the European Payments Council) Greek banks participate with competent contact persons on the Emergency Contact List for Prioritising Payment Blocking Requests related to Fraud.

The Internet service providers, according to the Law 3917/2011 for the Data Retention, are obliged to retain data for one year.

The National CERT directly cooperates with all telecommunication providers for whom no additional obligations have been assigned for the prevention and confrontation of the cyber crime.
The Internet access providers must also observe the Ethics Codes provisions for networks and electronic communication services. Also the providers must have been registered in the Network and Electronic Communication Providers Register at the NC.P.C. (see art. 18 par.3, l. 4267/2014, art. 12 l. 4070.2012 and art.7 of the no. 676/41 dated 20.12.2012 decision of the N.C.P.C.-General Licenses Regulation).

Especially for games, the Game Supervision and Control Committee may issue regulative decisions aiming to the protection of minors and generally vulnerable groups of the population and the implementation of specific prevention and suppression measures, the prohibition of games with racist, xenophobic, pornographic content or opposed to public order rules (art. 28 par.3e L. 4002/2011) by which further obligations may be enacted also for the game providers. As to the data retention, criminal and administrative sanctions for the providers are prescribed in the articles 11 and 12 of the L. 3912/2011 respectively.

The Directorate of Electronic Crime Prosecution as the competent service for fighting against the cyber crime, in the context of the criminal investigation during the preliminary interrogation, directly communicates with almost all big companies managing information on the social media. The communication varies depending on the way proposed by each company. In most of the cases, there is access via a specific platform. However, their positive response to the requests is often hindered by the different applicable legal status of the State where the private company has its seat.

7.5. Tools of international cooperation

7.5.1. Mutual Legal Assistance

Greece applies the provisions of the European Convention of the Council of Europe regarding Mutual Legal Assistance in Criminal Matters 1959 (integrated in the Hellenic legal order by the L.D. 4218/1961), the articles 48 et seq. of the SCHENGEN Agreement (integrated in the Hellenic legal order by the L. 2514/1997) and article 457 et seq. of the Code of Criminal Procedure related to the mutual legal assistance.

Furthermore, it should be noted that in the fields of the Judicial Assistance, Greece has signed bilateral and multilateral Agreements with many countries.

The requests of Mutual Legal Assistance may be transferred directly, via the competent District Attorneys of Appeal. Within the 19 District Attorney's Offices of Appeal there are Extradition and Judicial Assistance Departments.

As to the District Attorney's office of Appeal of Athens, by a recent Decision of the Three-Member Council of Administration of the First Instance Court of Athens, the execution of the Requests of Judicial Assistance for the region of the Court of Appeal of Athens, was exclusively assigned to the 7th Special Interrogatory Department of the First Instance Court of Athens. In this Department, a senior Judicial Officiator (President of First Instance) is serving and he possesses exceptional experience in handling the Requests of Judicial Assistance.

The requests of Mutual Legal Assistance of third countries are transferred via the diplomacy channels, that is via the Ministry of Foreign Affairs or the Ministry of Justice (depending on the provisions of the current applicable bilateral or multilateral Convention), to the locally competent District Attorney of Appeal and then the currently competent Interrogator (article 458 Code of Criminal Procedure).

If the Request of Judicial Assistance is an emergency, then the channel of the Directorate of International Police Cooperation of the Hellenic Police Headquarters (D.I.P.C.-EUROPOL, SIRENE, INTERPOL) may be activated.

In case the request of Judicial Assistance concerns the possibility of starting a prosecution, then this is imperatively transferred to the Ministry of Justice, then to the locally competent District Attorney of Appeal and finally to the locally competent District Attorney of Magistrates.

In case any explanations or additional information is required, then the above described procedure is followed while channels such as the European Judicial Networks Contact Points and the EUROJUST channel, may be also activated.

It is difficult for full statistical data to be supplied, regarding the requests of Mutual Judicial Assistance that concern the crimes in cyberspace, as these are directly transferred via the competent Judicial Authorities, without the services of the Ministry of Justice to take knowledge thereof.

In the context of execution of Requests of Mutual Judicial Assistance regarding the cyber crimes, it is usually requested the undertaking of interrogative acts such as the removal of e-privacy and the removal of banking privacy.

The most frequent reason for Requests of Judicial Assistance is the fraud via computer (article 386A of the Hellenic Criminal Code).

As to the most frequent reason of sending Requests of Judicial Assistance abroad, this is the vilification and the slanderous defamation via the social media (Facebook etc.) and the fraud via computer (article 386 A of the Hellenic Criminal Code).

Greece has not encountered specific problems in sending Requests of Mutual Judicial Assistance for offences committed in the “cloud”.

Greece send many Requests of Judicial Assistance to the U.S.A. based on the bilateral agreement regarding Mutual Judicial Assistance signed in Washington on 26.05.1999 and ratified by the L. 2804/2000 (Gov. Gaz. 49/3-3-2000, Issue A') in combination with the Protocol to the Convention of mutual judicial assistance in criminal matters between the Government of the Hellenic Republic and the Government of the United States of America, signed on 26.05.1999 as prescribed in the Article 3(2) of the Agreement between the European Union and the United States of America regarding the mutual judicial assistance signed on 25.06.2003 and the Verbal Notes with numbers AS 199 of the Ministry of Foreign Affairs of the Hellenic Republic and 116/POL/09 of the Embassy of the United States of America and ratified by Greece, by the L. 3771/2009 (Gov. Gaz. 111/9-7-2009, Issue A').

Especially with the U.S.A., the problem that arose was the lack of the dual criminality and the consequential non fulfillment of the Requests of Judicial Assistance of the Hellenic Judicial Authorities, for offences such as vilification or slanderous defamation which, in the legal order of the United States of America, fall under the protection of the freedom of speech.

Another issue concerning more cases is the short period of time for the retention of the electronic traces (IP) and thus, the Request of the Hellenic Judicial Authorities, might not be able to be fulfilled due to lapse of the time for the retention thereof.

7.5.2. Mutual recognition instruments

By the L. 4307/2014, the following were integrated in the Hellenic Law : a) the Decision Framework 2008/909/DEY regarding the application of mutual recognition in criminal decisions that impose custodial penalties, b) the Decision Framework 2008/947/DEY regarding the implementation of mutual recognition in criminal judgments concerning the suspension of sentence execution and the conditional dismissal and c) the Decision Framework 2009/829/DEY regarding the implementation of mutual recognition in criminal judgments that concern alternative surveillance measures aiming to the execution of such criminal judgments inside the European Union.

7.5.3. Surrender/Extradition

By the L. 3251/2004, the Framework Decision regarding the European Arrest Warrant and the procedures of surrender between the states members 2002/584 was transposed into the national law.

The criminal acts in the cyber space may fall under the crimes for which a European Arrest Warrant may be executed, are all acts punished by custodial penalties the maximum term of which is twelve months at least or for which a durable sentence has been imputed of at least four months, according to the provisions of the articles 5 and 10 of the L. 3251/2004 of which others fall directly into the category of the crimes in the cyber space (Art. 10 para. 2 computer-related crimes) and others which per case may be subjected to it (i.e. fraud by computer, minors' pornography via the internet etc.).

European Arrest Warrant (L. 3251/2004) :

For the crimes at the cyber space as well as for all criminal acts, according to the provisions of the articles 3 and 4 of the L. 3251/2004, the Ministry of Justice is appointed as Central Authority to assist the competent judicial authorities for the administrative transfer and receipt of the European Arrest Warrant as well as the official correspondence while the competent judicial authority for the issuance of a European Arrest Warrant is the district attorney of appeal to whose' region is subjected the local competence a) for hearing the criminal act for which the arrest and the adduction of the prosecuted party is sought, or b) for the execution of the custodial sentence or security measure.

As to the execution of European Arrest Warrants, competent Authority for receiving the same, is the District Attorney of Appeal at whose region has been arrested or the currently prosecuted party was arrested or resides. If the place of stay of such prosecuted party is unknown, then a competent District Attorney for receiving the European Arrest Warrant is the District Attorney of Appeal of Athens.

Extradition Proceedings (based on a bilateral, multilateral convention or based on the principle of mutuality)

The procedure for the criminals' extradition in the Hellenic legal order has two (**2) stages, the judicial and the administrative stage. Only** in the case of execution of a European Arrest Warrant, the procedure of surrender comprises only a judicial stage.

For the extradition of criminals, Greece has signed and integrated in the Hellenic legal order, a pile of bilateral and multilateral conventions while even if when no such a convention exists, there are applicable the provisions of the articles 436 – 454 of the Hellenic Code of Criminal Procedure which regulate the procedure to be followed for an extradition case.

In general lines, the extradition proceedings in Greece are as follows :

A.Case : The supportive documents have reached, via the diplomacy channels, the Hellenic Ministry of Justice, Transparency and Human Rights :

A. According therefore to the par. 2 of the **article 443 of the Code of Criminal Procedure :**

"2. The Petition for the extradition together with the documents required as per par. 1 and with the official translation thereof, are transferred by the Minister of Foreign Affairs to the Minister of Justice and the latter, having first verified the legality of the petition, forwards the same together with the document and by the care of the district attorney of appeal, to the President of Appeal at whose region stays the party whose extradition is sought." Immediately afterwards and according to the provisions of the **article 445 par. 1** : "*The President of Appeal is obliged, as soon as he receives the documents, to order, with no adjournment, by a warrant, the arrest of the person whose extradition is sought and the confiscation of all evidence…" Right afterwards, the locally competent District Attorney of Appeal cares for the execution of the arrest warrant and the adduction of the arrested/sought person and the proceedings prescribed in the article 446 of the Code of Criminal Procedure takes place. In particular : "The party arrested is led with no adjournment, together with the reports of arrest and confiscation to the District Attorney of Appeal, who examines him in order to verify his identity, taking into account also the information from the Authority that has made the arrest. When the identity is verified, the District attorney of Appeal orders for his detention at the prison for defendant awaiting trial and he sends all reports for the arrest, the confiscation and the verification of the identity to the President of Appeal."*

Immediately afterwards and within twenty four (24) hours, the locally competent President of Appeal summons the Council of Appeal to a three-member composition in order that it give an opinion in favor or against the extradition, according to the provisions of the **article 448 par.1** of the Code of Criminal Procedure. Before the Council there should be also summoned and adducted, if he consents, the person arrested who is also entitled to attend by an attorney and an interpreter of his choice or, if he has not, to ask for the nomination of attorneys by the president of appeal. The Council of Appeal comes to public session, unless the person arrested asks for the session to take place behind closed doors or he does not attend the council at all. The council may also *ex officio* order for the session to take place behind closed doors. The Council of Appeal, after the examination of the person arrested, if he has shown up, and after the oral arguments of the District Attorney and the party whose extradition is sought, or his attorney, **gives a reasoned opinion for the request of the extradition and decides : a) about whether the person arrested is the same person with that whose extradition is sought, b) about the existence of the supportive documents required by the Code or by the convention for the extradition, c) whether the party arrested and the crime attributed to him or (in case of a request for extradition upon a convicting judgment) the crime he has been convicted for is among those which the extradition is allowed, d) whether the terms of the art. 438d are fulfilled, to wit some of the reasons the extradition may be prohibited for (article 450 par.1 of the Code of Criminal Procedure).**

2. The Council of Appeal also examines, if not hindered by the convention, whether there are indications for the merits of the accusation attributed to the person sought who has been arrested, based on the official pieces of evidence that are produced by the State requesting the extradition and it decides whether these would allow for the arrest and his indictment to trial in Greece, if the crime had been committed at Hellenic territory. The Council may, in order to formulate an opinion on the merits of the case, proceed with one of its members, to the collection of all useful evidential material, **adjourning the final judgment for fifteen days at most.**

If the Council of Appeal gives an opinion in favor of the extradition of the sought person, the sought person has the right to exercise the **legal remedy of appeal** according to the provisions of the article 451 of the Code of Criminal procedure. In specific : "1. *Against the final judgment of the Council of Appeal, it is allowed to the person whose extradition is sought and the district attorney, to lodge an appeal at the b' division of the Supreme Court* ***within twenty four (24) hours as of the publication of the judgment****. For the appeal, a report is drafted by the clerk of appeal.*

2. The Supreme Court in Council decides within eight days by proportionate implementation of the articles 448 and 450. The person whose extradition is sought, is summoned in person or via his attorney-at-law, twenty four hours at least, before the hearing, by case of the District Attorney of the Supreme Court".

If the Judgment of the Supreme Court rejects in merits the appeal of the party sought, against the Decision of the Council of Appeal that has given an opinion in favor of the extradition, then **the party sought is dismissed and the proceedings of extradition are terminated at this point without the administrative stage to follow (article 452 par.2 of the Code of Criminal Procedure).**

The same happens also if the Council of Appeal irrevocably decides that no extradition should be made. In such a case, it is considered that the judgment of the Council of Appeal is irrevocable, if the legal remedy of appeal is not lodged by the locally competent District Attorney of Appeal.

Against the Judgment of the Minister of Justice in favor of the extradition, the sought person may lodge the legal remedy of the Petition for the Cancellation of the Proceedings, before the locally competent Administrative Court of Appeal, which however, does not have a suspending result. Nevertheless, the above named sought party may, together with the petition for Cassation, file a Petition for Suspension, asking for the suspension of the execution of the disputed Ministerial Decision which, if favored, will suspend also the extradition of the sought party until the issuance of a Judgment on the Petition of Cassation.

B' Case : The supportive documents have not come via the diplomacy channels to the Hellenic Ministry of Justice, Transparency and Human Rights, however there is an emergency case and a provisional arrest of the sought person is made and then follow the proceedings described in **the article 445 par.2 of the Code of Criminal Procedure,** which is as follows :

"Article 445

2. Even without a warrant, an arrest may be issued in case of emergency and especially when there is well-grounded suspicion of evasion of the persons whose extradition is sought, before the filing of the petition for extradition, by order of the district attorney of appeal; for the arrest, there is no need for diplomatic mediation but it is required an announcement that is transferred by post or telegram by the judicial or other competent authority of the State requesting the extradition. The announcement needs to refer the warrant arrest or the decision and the crime. The District Attorney of Appeal immediately announces the arrest to the Minister of Justice, who may order for the dismissal of the person arrested.

3. If, within one month at most, after the arrest, the petition for extradition is not submitted according to the article 443, the detainee is provisionally dismissed by order of the District Attorney of Appeal. If the documents are timely submitted, then the provisions of the par.1 and the articles 448 et seq. will apply.

4. If, after the dismissal of the person whose extradition is sought according to the above, the petition for extradition reaches the Ministry of Foreign Affairs, according to the article 443, then the proceedings of extradition follow.

5. The person provisionally arrested may, by disputing his identity, appeal to the Council of Appeal within twenty four (24) hours as of his adduction to the District Attorney of Appeal, and the Council will irrevocably decide, having heard the party filing the appeal and his attorney-at-law. The appeal may be lodged in oral too, before the District Attorney of Appeal."

The deadline of the provisional detention varies depending on the each time bilateral or multilateral convention that is applied.
As to the rest, the procedure is as described right hereinabove, in the case A.

It should be noted that the SIRENE Department of the Directorate of International Police Cooperation of the Hellenic Police Headquarters, according to the article 8 par.4h of the p.d. 178/2014 regarding Organization of the Services of the Hellenic Police, among others cares, in cooperation with the judicial authorities, or the introduction, modification and deletion of the measures of the European Arrest Warrants that are issued based on the L. 3251/2004 and the article 26 of the Decision 2007/533, in the 2nd Generation Schengen Information System.

It is difficult for full statistical data to be supplied, regarding the requests that concern the crimes in the cyberspace, between the E.U. States –Members given that as these are directly transferred via the competent Judicial Authorities, without the Services of the Ministry of Justice to take knowledge thereof.

There are no specific procedures regarding requests concerning criminal acts in the cyber space, nor is there any determined special procedure for emergencies, which in every case are forwarded and processed by the competent judicial authorities by priority, without delays and within the limits set by the convention that happens to be applicable or the Code of Criminal Procedure.

In every case, it is required a European Arrest Warrant, for the arrest and surrender in another State-Member of a person prosecuted for cyber crimes.

They are treated by immediate updating either the competent Hellenic authority or the foreign one, via the respective channels of communication.

There is the possibility of provisional arrest, upon the issuance of a relevant order by the competent District Attorney.

The time of response depends on every case, the data, the conditions, the existing evidence etc. With regard to requests which do not concern the arrest of a person but they are exchanged in the context of police cooperation for the prevention and investigation of criminal acts, these are transferred to the competent Directorate of Electronic Crime Prosecution and provided they are complaint with national legislation, they are executed the soonest possible, even within the same day.
During the years 2011-2015, two prosecuted persons have been arrested based on European Arrest Warrants for offences related to the cyber space (electronic frauds etc.) One of them was surrendered to the country that issued the warrant while the second served the sentence imputed.

Currently, it is pending for examination, before the Italian Authorities, a European Arrest Warrant of the District Attorney's Office of Appeal of Athens against a Romanian citizen that concerns to frauds with credit cards and specifically the criminal acts of : i) fraud by computer in continuation, by liable parties liable who commit frauds by profession and by habit and the total benefit and the respective total damage exceed the amount of 15.l000 euro and ii) violation of the art. 22 par.6 of the l. 2472/97 (violation of personal nature data) in continuation.

In the year 2013, Greece received and executed a Request of extradition from the U.S.A. for a prosecuted-defendant, for a criminal act that is a crime in the cyber space and in specific, he was sought in order to be judged for the criminal acts of : 1) information extraction from a protected P/C, 2) possession of non-authorized means (devices) of access, 3) distinguished theft of personal data (identity) that ifs for violation of the title 18 of the U.S. Criminal Code, section 1030(a)(2), title 18 of the U.S. Criminal Code, section 1029 (a)(3), title 18 of the U.S. Criminal Code section 1028(a)(1). The whole procedure took place on the legal base of the bilateral convention between Greece and U.S.A. for mutual extradition of criminals ratified by Greece by the Law 5554/1932 in combination with the provisions of the Protocol to the Convention for mutual extradition of criminals between Greece and United States of America, signed on 06.05.1931 and the Interpretative Protocol thereof, signed on 2.9.1937 as prescribed in the article 3(2) of the Agreement between the European Union and the United States of America, regarding the extradition, signed on 25.06.2003 and the Verbal Notes with nos. AS200 of the Ministry of Foreign Affairs of the Hellenic Republic and 117/POL/09 of the Embassy of the United States of America and was integrated in the Hellenic legal order by the L. 3770/2009.

Also, there is an exchange of requests in the context of the international police and judicial cooperation via the INTERPOL channels. In cases of search/arrest/extradition, there are applicable the provisions of judicial assistance of the Code of Criminal Procedure, while, by virtue of an international arrest warrant, an INTERPOL Red Notice of International Searches is issued. In cases of exchange of information and requests for interrogatory acts, applicable are the provisions for mutual police and judicial cooperation.

7.6. Conclusions

- The implementation of the "Budapest Convention" would create a good and fast possibility of preservation of digital evidence before sending an MLA. After the implementation Greek law enforcement agencies would be able the send out fast preservation requests via the COE 24/7 contact point list which would be a useful tool for the country on the field of fighting against international cybercrime.
- It must be highlighted that Hellenic Police Directorate of Electronic Crime Prosecution takes part – for some Operational Action Plan activities as a leader or co-leader - in the work of all Empact Cybercrime sub-priorities such as Cyberattacks, Payment Card Fraud and Child Sexual Exploitation Online.
- The national authorities consider that there is a good cooperation with Europol, Eurojust and ENISA. However, up to date of the evaluation visit, Greece has no experience in JITS and cyber patrols.
- The mutual legal assistance requests may be addressed directly to the judicial authorities, via local prosecutions services. For this reason the central level couldn't provide any statistics related to these requests.
- Greece presented information that they had requsted for information from countries like China and Russia in cases related to Child Sexual Explotation. Ministry of Justice and Eurojust have an important role in this work.
- According to the national authorities, Greece sent requests for mutual legal assistance to the USA. The main difficulties encountered in practice derive from the lack of dual criminality , which lead to the non-fulfilment of these request due to the fact that some facts as slanderous defamation fall under the protection of freedom of speech in the USA legislation.

8. TRAINING, AWARENESS-RAISING AND PREVENTION

8.1. Specific training

A) *HELLENIC POLICE*

There is education granted related to the crime in the cyberspace, to the Police Academy students, in basic as well as in post-graduate level. Also, there is such kind of education granted via the internet seminars (webinars) as well as with the participation of officers form the Hellenic Police in seminars organized by CEPOL and other international and European agencies.
In particular :

A. BASIC LEVEL :

Hellenic Police Officers Academy

Course :" Public Security Police

a. Thematic Unit : "Electronic Crime"
b. Aim (of the Court of Public Security-there is no separate goal from the thematic unit : Electronic Crime) : The educated Cadets Lieutenants are pursued to acquire : (A) the specialized knowledge of Police Methodology for the effective prosecution, fight against the crime and successful execution of the interrogatory duties, (2) the capacity to approach the depictions, tendencies and the measures of confrontation of the domestic delinquency as well as the channels of the international police cooperation.
c. Term of Education : two (2) didactic hours.
d. Frequency of Education : The education is made every educational year at the 2nd educational department.
e. Also, the mentioned issue is also an object of dissertation by the Academy's students.

Course : Material Criminal Law

a. Thematic Unit : "Computer Fraud" Article 386A of the Criminal Code
b. Aim (of the course of Material Criminal Law – there is no separate aim of the mentioned thematic unit) : Understanding the provisions of the special part of the Criminal Code, emphasizing into the crimes that appear more frequently at the police action and which will be encountered by the Cadets Lieutenants after their graduation, at the exercise of their duties.
c. Term of Education : two (2) didactic hours
d. Frequency of Education : The education is made every educational year at the 3rd educational department.
e. Course : Scientific Police-Interrogation Science
f. a) Thematic Unit of the Scientific Police : Issues for the examination of digital and sound evidence and syllabus : Examination of digital evidence (way of confiscation, trafficking, safeguarding, examination, etc.)- examination of issues for the trafficking of evidence via the Internet (digital frauds).

b) Aim (of the courts: Scientific Police-Interrogation Science-there is no separate aim of the thematic unit : Issues for the examination of digital and sound evidence-) : The educated Cadets Lieutenants to understand and consolidate the necessity of the substantiated evidential material that accrue from the scientific investigation of the crime scene and the laboratory examinations.
c) Term of Education : Three (3) didactic hours
d) Frequency of Education : The education is made every educational year at the 3rd educational department.
Police Academy

Course : Public Safety Issues

a. Thematic Unit : "Electronic Crime"

b. Aim (of the course : "Public Safety Issues – there is no special goal of the thematic unity : Electronic Crime-) : The educated parties to become capable of understanding the ways of crimes commission that concern the Public Safety and apply appropriate modes for the prevention and suppression of those. To bring the Cadets Policemen to contact with the problem for the delinquency confrontation and especially, to make them aware of the causes of criminal behavior of persons and social groups, their personality, the particularities in the mode of their action as well as the available capabilities, scientific or police related ones.

c. Term of Education : One (1) didactic hour

d. Frequency of Education : The education is made every educational year at the Cadets policemen of the 1st Educational period.

B. POST-EDUCATIONAL LEVEL

✓ Post-Education and Further Training Academy / Department of Professional Police Warrant Officers Post-Education

Course : Public Safety Issues

a. Obligatory Lecture : Electronic Crime

b. Aim (of the course of Public Safety) : The completion of the students' professional education, the discussion and analysis of problems encountered while exercising their duties and their updating in modern and general issues.

c. Term of Education : Two (2) didactic hours

d. Frequency of Education : The education is made every educational year to the students of the Department of Professional Police Warrant Officers Education.

National Security Academy

Cognitive Object : Public Security Issues

a. Lecture Topic : The Internet Science and the electronic crime.
b. Aim (of the cognitive object "Public Safety Issues") : The post-education and further training in postgraduate level, of its students in issues concerning the Public Safety and related to the National Safety Strategy and Policy, so that they be able to respond to the duties of the Senior Public Official.
c. Term of Education : three (3) didactic
d. Frequency of Education : The education is made every educational year to the students of the National Security Academy.
e. Also, the mentioned topic is the object of postgraduate research and work by the students of the Academy.

C. Internet Seminars (Webinars) that have been organized since the year 2011 up to date.

Especially significant on post-educational level is the possibility of the Hellenic Police staff to participate in internet seminars webinars organized by initiative of the European Police Academy (CEPOL).

It is noted that the term of the internet seminars are almost 90' minutes and staff of the Hellenic Police has participated in the following Webinars :

✓ **CEPOL webinar 111/2012 "Cyber Crime Online Learning Module", 21.02.2012.**

In such Webinar thirty two (32) officers of the Hellenic Police participated and its aim was for the participants :

- to enter the electronic unit of the Cyber crime that is available at the CEPOL electronic platform
- to determine and propose manners and examples regarding how the instructors, the teachers and the parties in charge of the development of a series of courses/programs of studies in the Police Academies may incorporate the same in their didactic units.

✓ **CEPOL Webinar 10/2014 "Cybercrime : Forensic and Digital Evidence", 04.12.2014**

In such Webinar, eleven (11) officers of the Hellenic Police participated and its aim was that the present situation be presented to the E.U. countries regarding the digital evidence and the most recent trends, as well as future perspectives.

- ✓ **CEPOL Webinar 09/2014 "Cybercrime : Disclosure, Investigation and Prevention", 27.11.2014.**

In such Webinar, 10 officers of the Hellenic Police participated and its aim was to present the last tendencies and future perspectives in the sector of cyber crime.

- ✓ **CEPOL Webinar 08/214 "Cybercrime : E-Frauds", 06.11.2014**

In such Webinar, 15 officers of the Hellenic Police participated and its aim was to present the last tendencies in the electronic frauds via credit cards and the cooperation between court authorities and private sector.

D. Seminars that have been organized by CEPO since the year 2010 up to date

At the same time, the Hellenic Police takes advantage of the Seminars implemented by the European Police Academy (CEPOL) while staff from t, has participated in the following seminars :

- ✓ "Cybercrime and crime by the use of high technology" (18-21 May 2010, Athens) - 3 participants
- ✓ "Cybercrime and crime by the use of high technology – General Tendencies " (16-19 October 2012, Avila, Spain) – Participation of one (1) representative of the Directorate of Electronic Crime Prosecution
- ✓ "Minors' Exploitation in the Internet" (01-04 October 2013, Barcelona, Spain) – Participation of 2 representatives of the Directorate of Electronic Crime Prosecution.
- ✓ "Capacity of the EU and the States-Members to detect, investigate and prosecute the cybercrimes" (23-26 April 2013, Stockholm, Sweden) – Participation of one (1) representative of the Directorate of Electronic Crime Prosecution
- ✓ "Child Abuse in the cyberspace" (08-11/04/2014, Barcelona, Spain) – Participation of one (1) representative of the Directorate of Electronic Crime Prosecution
- ✓ "Cybercrime and cyberspace security" (27-30 October 2015, Finland) – Participation of one (1) representative of the Directorate of Electronic Crime Prosecution

- ✓ Presidential Congress of Latvia in the context of the European Police Academy (CEPOL) with the topic "Fight against cybercrime in strategic level. Future challenges in confrontation of internet delinquency" (Jurmala, Latvia, 25-27.03.2015)) – Participation of two (2) representatives of the Directorate of Electronic Crime Prosecution and one (1) representative of the Directorate of Information Science / Hellenic Police Headquarters
- ✓ "The first correspondents and the forensic investigations in the cyberspace"(8-12 June 2015, Estonia) -) – Participation of one (1) representative of the Sub-Directorate of Criminal Investigations of Northern Greece
- ✓

E. PARTICIPATION IN OTHER POST-EDUCATIONAL ACTIVITIES

a. Indicatively is mentioned the participation of Hellenic Police staff to the following educational activities :

- ✓ In the year 2013 an educational seminar was held in the context of the antiterrorism assistance program, of the Ministry of Foreign Affairs of the U.S.A, with the topic "Alert in Cyberspace/Internet Issues" with the participation of fifteen (15) officers.
- ✓ Participation of four (4) officers of the Security Directorate of Attica, in the Annual Congress for the Investigation and Security in the Cyberspace (Abu Dhabi United Arab Emirates, 10-11/11/2010)
- ✓ Participation of one (1) officer of the Security Directorate of Attica, to the 2nd International Congress for the fight against illegal internet material and child abuse (2nd INHOPE Building Collaboration Conference)-(Amsterdam-The Netherlands, 04-05.11.2010)
- ✓ Participation of one (1) officer of the Directorate of Electronic Crime Prosecution/HPH in educational International Conference of the F.B.I. about "Crime in the Cyberspace" (Prague, Czech Republic, 17.05.2012)
- ✓ Participation of one (1) officer of the Directorate of Electronic Crime Prosecution/HPH in educational International Conference of the EUROPOL for the confrontation of the Sexual Exploitation of Minors via the Internet (Selm, Germany 21-29.10.2013).

- ✓ Participation of one (1) officer of the Directorate of Electronic Crime Prosecution/HPH in the Educational Workshop of George Marshall Center in matters of security in the internet (Program on Cyber Security studies)-(Garmish-Partenkirchen, Germany, 05-08/05/2014)
- ✓ Participation of one (1) officer of the Directorate of Electronic Crime Prosecution/HPH in the Educational Programme of EUROPOL with the topic of fighting against the sexual exploitation of minors, via the Internet (Salm, Germany, 06-12/10/2014).
- ✓ Participation of one (1) officer of the Directorate of Crime Investigations in the meeting of National Experts of the ECTEG Networks (European Cybercrime Training and Education Group (EUROPOL(Hague, The Netherlands, 06-07/05/2015).

b. Furthermore, staff of the Directorate of Electronic Crime Prosecution participated in the following educational programs, upon sponsorship-grant.

- ✓ Computer Forensics-Online Infosec Institute Seminar : Distant Education, term 45 hours, participation of one (1) officer
- ✓ Electronic Learning Platform ACM (Association for Computing Machinery) and electronic learning platform-electronic journals “Hakin9, eForensics and SDJ” with the topics of cybercrime and digital criminology. Especially, the participants acquire access to material that is available on the Internet. In the first platform , five (5) Officers and in the second, one (1) Police Warrant Officer, acquired access.
- ✓ Seminar on MCITP Server 2012 Administrator which is organized by the Hellenic-American Union with total term of 200 hours. Participation of one (10 Officer.
- ✓ Seminar Advanced Ethical Hacking, which is organized by the Infosec Institute. This is a distant education programme with potential time schedule for implementation : one (1) year. Participation of one (1) Officer.

- ✓ Ethical Hacking Live OnLine Seminar : This is organized by the Infosec Institute this is a distant 107 programmed that may be completed in one year. Participation of one Officer.
- ✓ Postgraduate Studies Program "Technical Economic Administration and Security of Digital Systems" of the Department of Digital Systems of the University of Piraeus Participation of two (2) Officers.

c) Furthermore, it is worth stressing that, as mentioned hereinabove as well (see question 3B2), at the Directorate of Electronic Crime Prosecution and the Department of Digital Evidence Examination of the Directorate of Criminal Investigations, police officers with general and special duties are serving, who hold titles of studies of undergraduate, postgraduate and certain of them, even doctorate level, in computer science related topics.

B) Judicial Corps

By its decision, the Council of Studies of the National Academy of Judicial Officiators has integrated in the Program of Studies with Major for District Attorneys, for the year 2015, the course

15. LEGAL INFORMATION SCIENCE

Criminal Issues of Legal Information Science

Cybercrime

Teacher ; Ioannis Angelis, District Attorney of Appeal

Teaching Hours : 9 two-hour sessions

And in the Major of Civil-Criminal Justice, for the year 2015, the course :

4. Electronic Crime

Teacher: Ioannis Angelis, District Attorney of Appeal

Teaching Hours : 6 two-hour sessions

Final Explanations

The communication-teaching with the School's students is made in a way so as, they "direct" the issues (by proposals, submission of questions etc.) according to their needs and depending on their knowledge in technical and legal issues of new technologies. It has been ascertained that, almost everybody posses "a minimum percentage of technical and legal knowledge" which they have normally acquired by their own initiative (it is explained that the legal information since is taught as an elective course in the Law Schools).

Teaching is made by the use of computers. The students have received various legal articles and studies (among which my papers and presentations in congresses as well), and judicial judgments for legal (and technical) analysis. Various practical issues are also discussed, such as the mode of research in legal databases, the search of legal issues in the Internet, the way of file keeping by the Judge and the District Attorney.

On an annual basis, there is a special educational seminar of "OLAF" to a specific number of persons of the Department of Digital Evidence of the Directorate of Criminal Investigations / H.P.H. in order that they be examined in issues of examination of digital evidence, by the International Organization IACIS.

Additionally, respective educational events are organized by CEPOL, ECTEG (European Cybercrime Training and Education Group) and EUROPOL/EC3 during the year where we participate depending on the case.

Finally, a two-day educational seminar is annually organized in Greece by the Center for Security Studies (C.S.S.).

Furthermore, the Department of Digital Evidence Examination organizes every year conservative educational trainings for the staff of the Criminal Investigations Stations and Offices (CISs & CIOs) of the country, on issues appertaining to the criminal examination of computer systems and digital evidence. In particular, education is granted in the following sectors :

- in recognizing the computer system evidence,
- in collecting the evidence
- in the mode of sending the evidence (as to the protection-security and the questions posed) for examination, either to the Directorate of Criminal Researches or the respective Department of the Sub-Directorate of Criminal Researches of Northern Greece (depending on the territorial competence of the respective C.I.S or C.I.O.)

There are more authorities and institutions responsible with the cybercrime training:
a) Responsible for providing education with regard to the crime in the cyberspace on basic as well as post-educational level, is every School that implements the education, as described in the question 10B1, as manager of tits educational program and specifically, the Hellenic Police Officers Academy, the Policeman Academy, the Post-Education and Further Training Academy and the Academy of National Security.
b) Responsible for providing education with regard to the crime in the cyber space, via the seminars organized by CEPOL as well as via the internet seminars (webinars), is CEPOL.
c) As to the degree of contribution of the European Organizations in the education of the law enforcement principles, this is highly important and beneficial as analytically.

The annual expenses in the Expenses Code Number (ECN) 0881 (Rewards for education, post-education, further training) as well as in the ECN 0517 (Rewards of hourly salaried teachers and other persons for rendering didactic work) for the current year, has been anticipated in height, to the amounts of 800.000,00€ and 1.600.000,00€ respectively (total amount of expenses for the total spectrum of education and not only for the particular object of the electronic crime).

As to the internet seminars (webinars), it is noted that zero annual expenses are charged for the Hellenic Police, while it is charged with 25% of the out-of-seat compensation of the participant police officer in seminars organized by CEPOL abroad or inland.

Taking into mind that, the authorities of the Directorate of International Police Cooperation do not include the investigation of cybercrime cases, but the exchange of information, experiences and knowledge between the Hellenic Police and the foreign police agencies (this is in other words a communication channel via the Departments of INTERPOL, EUROPOL, SIRENE) in the ordinary programmes of the Post-Education School, no education is prescribed with regard to the cyber crime for the persons who participate in the procedure of international cooperation.

Every year, a two-day Seminar is organized by the Hellenic Center for the cybercrime, of the Center for Security Studies, where domestic and foreign experts participate as well.

The ForthCERT in Herakleion Crete, is the sole relevant excellence center in cyberspace security issues, as well as the Computer Technology Institute DIOFANTOS and the C.S.S.

A) PRIMARY AND SECONDARY EDUCATION

Institutions and actions for the prevention of bullying

A. The Ministry of Education and the General Secretariat for Youth is one of the founding members of the Network against Violence in Schools founded in 2011 on the initiative of the Association for the Psychosocial Health of Children and Adolescents (APHCA) in Greece.

B. Many Health Education programs are introduced in schools on issues related to: violence prevention, conflict management, racism, interpersonal relationships (with teachers, parents, peer groups), gender equality, gender relations, sexual abuse, violence on the Internet, children exploitation and domestic violence.

C. The Ministry of Education established the Centre for the Prevention of school violence and bullying. The purpose of the Centre is to design and implement measures to prevent school violence and bullying by identifying, studying and channel to management in certified bodies, incidents of school violence and bullying.

Actions and programs especially for online safety

Especially for online safety, the following actions have been realized:

The Ministry of Education in cooperation with the Ministry for Citizen Protection and Public Order, / Division of Electronic Crime held meetings through teleconferences with school units of Primary and Secondary Education, entitled "Safe surfing the net".

-In the framework of e-twinning

l. Webinar with esafety theme and eTwinning (www.youtubexom/watch?v=bMirHUp8NEQ&feature=voutu.be)

2. Presentation in plenary of the conference «e^2 (twinning + safety): A responsible and safe cooperation" (http://conf2014.etwinning.gr/index.php/2014-06-02-15-21-07)
3. Lesson in module platform e-twinning on "Copyright and the importance of reference sources used on the Internet", which is aimed at teachers on Primary and Secondary Education (2014) and it is included on the online courses of Greek Support Office (NSS) for eTwinning in order to explore ways of using the web material, which is subject to the same rules concerning copyright in general, without violating them on the e-Twinning projects.
4. Many Greek school partnerships with schools abroad on bulling and general Internet security issues.

In the framework of NSRF (National Strategic Reference Framework)

l. Action "Comprehensive Services for Enhancement of Digital Trust'

The Act "Comprehensive Services for Enhancement of Digital Trust" under the Operational Program Digital Convergence (Start: 01/10/2009 - End: 10/31/2015). The aim of the Act is to cover security and trust issues for Information and Communication Technologies in Education with emphasis on production of information and education services / content as well as the production of digital security and trust services. The Act consists of two subprojects:

Subproject 1: Portal Digital Security and Digital Safety in the first grade of lower secondary education comprising

Activity 1: Portal Digital Security

This gate (portal) aimed primarily at students, parents and teachers (education community), aspires to become a reference and meeting point for users interested in digital security and reliability in education.

Activity 2: "Digital Security in first grade of lower secondary education"

As part of Step 2 they are developed both a) distance courses (e-Learning) for Digital Security (with the relevant material regarding the safety of the Internet and the dangers of using the Internet and computers in general) and also b) an interactive educational game including in his environment activities that are aimed at familiarizing students with potential risks from the use of computers and the Internet.

Subproject 2: Digital Security Services including

Activity A: "Early Warning System for internet risk" (PROTOS) [protos.cti.gr]

This early warning system attacks (Intrusion Detection System) available for MS Windows and Linux (Ubuntu) and is expected to escalate to over 100,000 users

Activity B: "Computer Security Check" (Security Distribution) [secure-distro.cti.gr]

Concerns suite of applications that are installed on computers that have the Ubuntu operating system (14.04) with the aim of creating a secure environment for use by high school students.

2. Action "Call an Expert for the Safe Internet"

For the support of schools in a safe navigation model on the Internet and to supply the students with the skills needed to use safely and responsibly the Internet, the Ministry of Culture, Education and Religious Affairs (YPOPAITH) via the Panhellenic School Network (PSN) operates the information hub "Internet Safety» http://internet-safetv.sch.gr which provides reliable , targeted information and support as well as quality educational materials for students, teachers and parents.

In addition, the GSN as national coordinator of the action eSafety Label http://www.esafetylabel.eu/) of European Schoolnet (EUN) provides in Greek schools a special certification, which aims to support schools to formulate a policy Safer Internet and provide a more secure online environment for teachers and students. Through a specially-defined certification process are investigated those factors that can affect the level of Internet security. Based on the concrete results, a specialized Action Plan on internet safety is formed for every school. On top of the above, the PSN proceeded to the new action "Call an Expert for the Safe Internet»

http://internet-safety.sch.gr/call-an-expert , which offers schools the opportunity to invite a trainer trained in the safe Internet issues, in order to realize one in person session educating the school community. The body of experts is composed of specially trained and certified teachers and education officials.

The schools participating in the action "Call a Special for the Safe Internet" is simple and user friendly. Interested schools may submit their request via a form located at http://internet-safety.sch.gr/call-an-expert.

After completion of school training they will complete a questionnaire with observations on education and suggestions for overall improvement of the action. Similarly, the specialist will submit a short debriefing report with simple statistics such as the date of the event, number of students were informed, etc.

This action will take place at no cost to schools and YPOPAITH as all the actors involved participate voluntarily.

B) UNIVERSITIES

The following courses and actions in higher education curricula are indicative :

-In the curriculum of the **Department of Audio and Visual Arts of the Ionian University** it is included the optional course "Internet Communication".They are taught and discussed related issues -under the broad sense, from theoretical and technical perspective on internet security and cybercrime.

-In the **Faculty of Education, Aristotle University of Thessaloniki,** the following courses are offered:

a) In the Department for Primary Education t he optional subject in the 5th semester of the undergraduate course of study entitled: "Digital Literacy" (Secretariat Code: E44). About 1/3 of the course deals with the raising and development of attitudes , perceptions towards digital and electronic media and awareness in relation to the social, ethical, legal and human issues of building on ICT in everyday life. Within this section there clear and unambiguous references to the phenomenon of cyber-bullying or bullying on the Internet and a number of issues on crime and safety on the internet.

b) ln The Department of Early Childhood Education the course "Technologies of information and Communication in Teaching and Learning" is offered as Base course which will include units on security and crime issues on the Internet, cyber-bullying and in general on protection of privacy.

- In the Computer Science Department of the University of Crete the following two courses ARE taught (one undergraduate and one postgraduate) regarding internet safety: -Introduction to Information Security Systems (4th year undergraduate course). Every acad. year in the winter semester

- Safe Systems (Graduate course every academic year(spring semester)

The Computer Science Department participates also in the organization of conferences, seminars and summer schools in cooperation with the Foundation for Research and Technology (FORTH) and the European Agency for Networks and Information Security Agency (ENISA) concerning Internet security and preventing criminal activity in cyberspace. These actions can attend the graduate and undergraduate students of the Department.

-In the Faculty of Informatics of the University of Economics of Athens provided specific courses for cybercrime and safety online are provided such as: "Information Systems Security" with lecturer Prof. D. Gritzalis.

Professor of the Department Mr. D. Gritzalis systematically organized 2-3 times per year information and awareness programs on threats and prevent criminal activity in cyberspace, which are open to the general public under the auspices University of Economics of Athens.

- The School of Economy, Administration and Law Sciences (SODNE) of the International Hellenic

University (DiPAE)

a) The cybercrime and Internet security is part of the curriculum of the optional course «Internet Law and E-Business» of the Postgraduate Program (PSP) "LLM in in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law "School of Economics, Administration and Law Sciences DIPAE.

b) Within the above PSP, the 22/11/2013 , an International Conference on "Internet Safety and Security on the Internet" was held in DIPAE.

- The Faculty of Technology (SET) of the International Hellenic University.

a) The Faculty of Technology offers the last 5 academic years the PSP 'Systems Information Technologies and Telecommunications ", a compulsory course on Information Systems Security, which describes the various kinds of cyber-threats and the practices to face them.. The curriculum of the course includes a range of topics, techniques (network security, databases, cryptography, etc.), management (safety management, business continuity planning, logical security, analysis and risk management, etc.) and legal and ethical issues.

b) Recognizing the need of the market and society for cybersecurity, from (2015-16), the SET has planned for next academic year and will offer PSP "Telecommunications and Cybersecurity» (Communications and Cyber Security), which includes courses as Cyber Crime and Computer Forensics and Legal and Ethical Foundations of Privacy and Security.

The SET plans related events, conferences and educational seminars in order to raise awareness on society and business about cyber-security.

- Open University. Faculty of Sciences and Technology

Undergraduate studies include the teaching of the cybercrime and the security in the internet. In the curriculum of "Informatics" in the framework of "Protection and Security Informatics Systems". Students are also invited to participate to events on the above topic.

- University of Western Macedonia

a) In the Department of Computer and Technology Engineers of the Polytechnic Faculty, the course "Security of Computers and Networks " it is taught. The topics of the cybercrime and the security to the network are included in this curriculum.

b) In the Pedagogical Department of Preschool Education the undergraduate courses on "Applications of Informatics to the Education" "New Technologies and Artistic Creation". "Development of Educational software" /'Literature" and "Educational policy" as well as the post graduate courses "1TC in teaching and learning" and " Digital narrative", they have references to cybercrime and the security in the network.

Also interesting is the effort made at the Technological Educational Institute of Thessaly with Dr. Vasilis Vlachos and the OWASP Hackademic Challengers project where the students are called to think as attackers in order to understand the vulnerability of the existing computer information systems when these have not been adequately secured.

8.2. Awareness-raising

A) HELLENIC POLICE

The Internet is the greater computer network in the world, which allows for the communication and the exchange of information between any spots on the planet. It has been characterized as the greatest invention of all eras, conquering the whole universe within only few decades of life and being now the globally greatest organized society. This is a parallel “fictitious” universal community which abolishes all social and cultural separation lines that exist in the real world and which the traditional communication means find impossible to overcome.

In opposition to the traditional information and communication media, it makes possible the live bilateral communication and gives the ability of the direct participation for all users, by the free selection of reception, provision and diffusion of the information. By abolishing the borders and eliminating the distances, the Internet seems to make the balance bend evidently now in favor of the communications in the perpetual fight between transports and communications.

Based on the previous developments and the tendency for evolution, the future is expected to present us new innovative solutions and services. In the context of the future developments, the Hellenic Police Headquarters has developed various innovative actions, aiming to the information of the citizens about the dangers lying in their Internet surfing and the ways to evade such dangers. All innovative actions which are analytically described herein below, are implemented by the specialized staff of the Directorate of Electronic Crime Prosecution while the implementation expenses are covered by sponsorships from companies of the sector of information science and communications that are sensitive in issues of Safe Surfing, without aggravating the State Budget.

Safer Internet Day Congresses

The Hellenic Police Headquarters, via the Directorate of Electronic Crime Prosecution, organizes day congresses throughout the Hellenic State, aiming to inform the students, parents and teachers about the Internet violence phenomenon, the risks hidden in the social media websites and generally the prevention and the confrontation of the risks related to the new technologies.

It is characteristically mentioned that 132 informative day congresses have been made in various cities f the country (Athens, Thessaloniki, Preveza, Igoumenitsa, Tripolis, Rhodes, Herakleion-Crete, Chania etc.) during the years 2011 up to date, while during such period, 515 requests for the implementation of day congress have been filed by various agencies (municipalities, Parents & Guardians Associations, Schools etc.), a fact that proves the intense interest of the citizens for information on Internet risk issues.

Congress Organization in European Level

During the years 2012 until 2015 included, on the cause of celebrating the Universal Day of Safer Internet, our Service has implemented four (4) congresses related to the Safer Internet Surfing which included presentations by distinguished and specialized in issues concerning Safer Internet Service scientists of Greece and abroad. In such congresses, the topics developed were related to the future evolutions in Internet issues as well as relevant to the legislation implemented in the cybercrime sector. The congresses had an open structure and communication, given that they were transmitted via the Internet, by live-streaming applications, from the Hellenic Police Website.
Analytically :

- *1st Congress of Safer Internet on Wednesday February 8th, 2012 in Divani Caravel*

The event comprised three (3) units which have been held in parallel, at three different halls where the following issues were presented :

- The positive aspects of the internet, including analysis and discussion related to the advantages introduced by the Internet and the new technologies into people's everyday life. Additionally, new information systems were presented which contribute to the creation and reinforcement of the innovative entrepreneurship.
- Addiction to Internet, which included the risk analysis and presentation involved in the irrational use of the Internet, in psychological and physical level.
- Legal Approach and Safer Internet that included the briefing of the representatives of the District Attorney and Judicial Authorities as well as the legalists regarding the new technologies and the cyber crime since the traditional crime has been transmuted into cybercrime, actually to a percentage of more than 82%.

2nd Congress of Safer Internet on Thursday 7th February 2013, at Athenaum Intercontinental

The event comprised three (3) units which have been held in parallel, at three different halls where the following issues were presented :

- **Electronic Information Security** - Industrial Intelligence. The purpose of this unit was the presentation of the problem of the electronic information security and specifically the phenomenon of the electronic Industrial Intelligence. The audience was made up of representatives of enterprises, business persons and companies managing directors. The speakers who have developed these topics were University professors and distinguished personalities from such area.
- **Cybercrime and Legislation** – Desperation Cries-Prevention of Suicides. The purpose of this unit was the briefing of the judicial-district attorney's authorities and extensively, the legalists, for the Internet terms, the transmutation of the traditional-conventional crime to electronic and the phenomenon that takes alarming dimensions regarding the suicidal attempts. The audience was made up of Judges, District Attorneys, Professors of relevant Sciences, Lawyers, Law Students and Cadets Officers of the Production Schools of the Armed and Security Forces. The speakers who have developed these topics were university professors of relevant sciences and representatives of the judicial authorities and the Personal Data Protection Authority.
- **Cyber Bullying**. The purpose of this unit was to raise concerns and activate to the direction of mitigating the consequences from the psychosomatic violence and the bullying that is exercised via the Internet on the children. The audience was composed of three hundred and fifty (350) children-students of the 3rd class of elementary school up to the 3rd grade of the High School, from public and private schools of Attica. The speakers who have developed this topic, due to the particularity thereof, were university teachers, specialized in matters of adolescent health, clinical psychologists, pedagogues and instructors.

At the beginning of the Congress proceedings, audiovisual material was projected that was sent for the needs of the congress by the European Commissioner, responsible for the Digital Agenda of the European Union, Ms. Neelie Kroes, especially for the Hellenic Police Headquarters and the Directorate of Electronic Crime Prosecution.

3rd Congress of Safer Internet, on Thursday 6th February 2014, at the Athenaum Intercontinental

Specifically, the two thematic units developed were the following :

- **"The actions of the Hellenic Police related to the Internet"** during which it was presented the program of the actions in the field of informing students, parents and other agencies concerned, about the positive and negative effects of the Internet and consequently the dangers underlying during their surfing. During such unit, it was presented the work of the Hellenic Police in such sector up to date, as well as the program of the future acts for 2014. Additionally, it was projected the TV spot of the new information campaign for 2014.
- **"The Internet in our life" :** what it is going to be, in the context of which the possibilities were developed as granted via the Internet, being a source of knowledge, learning, communication, amusement, updating, while the purpose of this unit was to bring up the significance of the Internet on the everyday life of the modern person.

4th Congress of Safer Internet, on Friday 13th February 2015, at the Athens Concert Hall

The event comprised two (2) thematic units and in specific :

- **"The floor is to our children !"** At this congress the floor was given to the children who informed their classmates about the Internet and the dangers of it, in order that they, in their turn, transfer the useful information and the knowledge they acquired, to their friends and to their parents as well. It was stressed out that the Internet is "LIGHT" since it has only 2% cons and 98% pros. For the cons, the children may address themselves to the Directorate of Electronic Crime Prosecution, on the phone number 11188 or the Cyber Alert.

- The Internet in our life, in the context of which have been developed the possibilities granted via the Internet, by being a resource of knowledge, learning, communication, amusement, information. The purpose of the unit was to bring up the significance of the Internet on the everyday life of the modern person.

Congress at the Athens Concert Hall for the students of the Special High-Schol – Lyceum of Athens and the Special High-School – Lyceum of Ilion : The congress took place on the Wednesday, December 17th , at the Athens Concert Hall and the audience was comprised of almost one hundred (100) students of the Special High-School – Lyceum of Athens and the Special High School-Lyceum of Ilion, with their escorting teachers. Its purpose was the information of the vulnerable group of children for the dangers involved with the Internet and the ways for their confrontation, the challenges posed by the digital world, since it is of the highest importance the equal participation of these students to the society of the knowledge and the modern technologies.

-Day Congress for the presentation of the website www.cyberkid.gr : The day congress took place on Wednesday May 7th, 2014 at the Intercontinental Hotel. The audience was comprised of almost 1.000 students, from all school levels, with their escorting teachers. In the day congress it was presented the new unit of the website www.cyberkid.gr which is called "Digital Sandlot" and includes the digitization of sixteen traditional board games (ludo, chess, checkers etc.) which are accessible to all visitors depending on their age.

-**Issuance of Congress Minutes :** After the completion of four congresses, the Directorate of Electronic Crime Prosecution proceeded to the issuance of the congresses minutes in printed and electronic form, via which the citizens are given the possibility to be analytically informed about the proposals made in the congresses.

-Teleconferences with School Units :

Every week (Tuesday and Thursday), updates are made with great success, in schools all over the State, via the adoption of the teleconference technology with parallel links at many points. The teleconference is made in real time and is allowed for a presentation, intercourse, questions and replies to be made between speakers and distant listeners.

The schools that participate in the teleconference receive an invitation via the "meeting.sch.gr" system, of the Hellenic School Network. Thus, they are integrated in the teleconference.

Ever since the beginning of the school year up to date, the Directorate of Electronic Crime Prosecution, was connected via multiple teleconferences with 5.225 schools all over the country, while the aim is that, by the end of the school years, the students of all schools of the state, have been informed for the safe surfing in the Internet and the ways they can confront such dangers.

-TV commercials: The Directorate of Electronic Crime Prosecution proceeded to the production and presentation via radio and TV stations of panhellenic velocity, of three TV commercials in the context of the information campaign of vulnerable social groups for their protection from the Internet traps. The Internet may have become a part of our everyday life but this entails many and serious risks for both us and the children. Our little friends, imitating their parents, own a tablet since their young age which has unfortunately replaced their playing.

- The first concerns the vague risks of the Internet and was presented in 2010. The purpose is the awakening of the children and the parents, since the latters are the sole protective "wall" of the children face to the predators. The parents may always be near their children and talk with them. Only then the child will be able to talk about threats that approach.
- The second concerned cyber bullying and was presented in 2014. It is reminded that, according to recent researches, 1 out of 20 high-school students has been the victim of cyber bullying, while this percentage is double among students of Lyceum.

-The third concerned the risks involved in the contacts with unknown persons and was presented in 2014. The purpose is to protect the children from the so-called predators that lurk in the Internet wearing the coat of a "friend" or the "peer" who talks to them on issues that concern them in order to gain their trust and then seduce them.

-Authorship and Distribution of Informative Brochures:

The Directorate of the Electronic Crime Prosecution has proceeded to the issuance of informative brochures with ten (10) different thematic units for the provision of advice related to the safer surfing in the Internet.

-Educational Visits: The Directorate of Electronic Crime Prosecution every day receives many requests from schools and various agencies that wish to visit its premises and be informed in topics concerning security in the Internet. Up to date it has received 12 informative visits (1st General Lyceum of Hellinikon, 1st High-School of Zografou, Research Association of Law Students, Doukas Schools, Psychikon College, etc.)

-Participation in the Hellenic Police Information Center at the 79th International Exhibition of Thessaloniki: More than 37.000 citizens visited the kiosk of the Hellenic Police and were informed regarding the "Safe Internet Surfing" with the result for the kiosk to become a significant attraction pole. The HELEXPO Exhibition administrative executives awarded a Certificate of Participation, to the Hellenic Police Information Center.

- Website "cyberkid.gr": In the www.cyberkid.gr useful information and advice is given regarding how all family members can take advantage of the positive aspects of the modern technologies that surround us and certainly, the internet's.

In the context of constant updating and development of the website www.cyberkid.gr, the unity "Digital Sandlot" was created where the children can play their favorite electronic games with absolute protection from the risks lurking in the internet. The games, 31 in their total, have modern graphics and quick evolution so as to keep the children's interest within the Digital Sandlot".

Also, the website was enriched with two new units. The unit "CyberAlert" where the audience may be informed about the most frequently appearing risks entailed in the Internet and the unit "News" where are posted the announcements concerning the Directorate of Electronic Crime Prosecution.

- Cyberkid applications for portable devices (Apps): The cyberkid application for mobiles was created with the purpose to daily inform the parents and the children of every family for the safe internet surfing and the dangers underlying in it. At the same time, it is an interactive application which gives the ability of direct communication with the Directorate of the Electronic Crime Prosecution via the CYBER ALERT line but also via the sending of a direct email message, by simply pressing a button, while there is the possibility of entertainment via the various games.

-Cyberkid Profile in the Facebook : The Cyberkid profile in the Facebook was created in May 2014 with the purpose to reinforce the promotion of the www.cyberkid.gr website in the social media. It presents high popularity since 2.450 Facebook users have already declared they "like" it and "follow" the Profile's activity. Also, many times they "Share" its posts via the Facebook platform. Totally 108 posts have been made in the mentioned Profile by the Service.

-"@CyberAlertGR" account in Twitter : In April 2015 the Twitter account "@CyberAlertGR" started operating aiming to the immediate and in real time updating of the citizens about the dangers that arise every day in the Internet, while, at the same time, they could also inform the Directorate of Electronic Crime Prosecution in case of danger or threat in the Internet.

B) Hellenic Bank Association

The Hellenic Bank Association, complimentary to the own initiatives of its member banks, assists in raising the awareness of their customers through publications (newsletters, press releases, etc.) and participation in specific thematic events and conferences.

Moreover, under its statutory role, HBA informs its members of the respective initiatives in other Member States of the European Union, coordinates specialized presentations regarding security issues and promotes best international and European practices addressing cybercrime in the financial sector.

C) DCD/NDGH

The D.C.D. assists to the prevention of the cyber attacks, by preparing and disposing to the wide public, directions for safe customization of the information systems. At the same time, it organizes and conducts educational programs which are addressed to the staff of the Armed Forces and the public agencies. The D.C.D. organizes a cyber defense school (of four weeks) where the trained parties acquire the possibility to understand the way of location and confrontation of the cyber attacks.

D) HDPA

The HDPA, as previously mentioned, raises awareness both to the data controllers and to the data subjects for matters relating to data protection and privacy through its website, its annual activity report that it is also published online, as well as the talks that its auditors give frequently.

E) "The Smile of the Child"

A. Odysseas – 1st Mobile Lab of Information, Education & Technology

"The Smile of the Child" using technology as a main "tool" of education created "ODYSSEAS" the 1st Mobile Lab of Information, Education & Technology. "ODYSSEAS" is a unique "tool" for Greece, with full autonomy and equipped with: Call Center, Photovoltaic Center of alternative energy, Satellite Cable for data transfer, 10 internal and external cameras (1 robotic camera included), 35 job positions with Internet access, smart TVs, Internal and External Speakers Laptops, Tablets and Smart phones.

The unit operates under the auspices of the Ministry of Education & Religious Affairs. In the framework of providing information to students, parents and teachers at ODYSSEAS, the main thematic area is Safe Internet Use. With the use of interactive tools, and staffed with specialized scientific personnel, ODYSSEAS provides knowledge regarding safe Internet use, cybercrime and the risks that stem from the irresponsible use of social media. "ODYSSEAS" came to reality thanks to the precious and invaluable contribution of some of the largest companies in Greece especially from the Telecommunications and ICT field, such as Cisco, Microsoft, Hewlett Packard, Dell, OTE group (Deutsche Telekom), Dixons, Vodafone, Cyta, Wind and others.

From November 2014 to March 2015 ODYSSEAS organized 160 interventions for 3.287 students all across Greece. The awareness raising activities performed at ODYSSEAS fall into the category of prevention of cyber-crime among students, parents and school communities (10. A. Prevention).

B. YouSmile

YouSmile is a safe online interactive environment for teenagers that enhance the skills and learning development of students with the use of new technologies. It also promotes the National Helpline for Children SOS 1056 and the European Hotline for Missing children 116 000 and encourages young people to call or –email the Helpline in different situations when they encounter problems, want to report or to seek help and assistance or just need to talk to someone who will listen to them.

The tool of YouSmile includes an interactive website, a Web Radio and Web TV, an e-learning platform that allows an online live communication that gives children an opportunity to enhance their learning skills and e-sharing, a space where children can share their ideas and work. Since the YouSmile started in 2012, 300 teenagers in Greece from 27 schools have participated to its activities. YouSmile aims among others to empower students, promote the interactive communication, raise awareness on various issues among others responsible use of technology and provide a safe internet environment for teenagers.

YouSmile platform is officially recognized by the Hellenic Ministry of Education & Religious Affairs as a training and raising awareness platform and aspires to expand its activities across Europe in the form of a European Student Volunteer Network.
More information about YouSmile can be found at www.yousmile.gr.

C. "Safer Internet Day" by Microsoft Hellas and "The Smile of the Child"

Every year, on the occasion of Safer Internet Day, a European Union initiative that emphasizes on the responsible use of online technologies, Microsoft Hellas in cooperation with "The Smile of the Child" organize a special event in order to raise awareness among young people on safety issues and the proper use of the internet.

The main aim of this cooperation is to educate children on the risks and inform them on the responsible use of technology. This event is one of the best examples of effective cooperation between the private technology sector and an organization on children's rights in the field of safe Internet prevention and awareness-raising.

D. Awareness- raising Campaign - International Day against Sexual Abuse

On the occasion of 19 November, International Day against Sexual Abuse and in the framework of 19 Days of Activism for Prevention of Violence Against Children and Youth 1-19 November (Women's World Summit Foundation – WWSF), "The Smile of the Child" presents every year statistical data and raises awareness on the phenomenon and the risks for children. Last year (2014) this event was held in Thessaloniki, where ODYSSEAS, the mobile unit of Information, Education and Technology raised awareness among students in the city centre on the responsible use of technology. A similar event will take place as every year this coming November 2015.

E. The European Anti-bullying Network (EAN)

"The Smile of the Child" is coordinating the European Anti-bullying Network (EAN) where 19 organizations from 14 EU MS are represented. One of the main aims of the Network is to better coordinate the actions of European organizations against bullying and cyberbullying and raise awareness on the phenomenon and the risks among the general public, children, parents and teachers. The exchange of good practices and tools in the field of prevention as well as raising awareness and develop cooperation in safety internet issues for children is part of the work of the Network. On June 2014 the 1st Scientific Conference on bullying and cyberbullying took place in Athens, Greece under the auspices of the Hellenic Presidency of the Council of the EU covering among others the thematic area of cyberbullying and Internet safety issues.

F. European Financial Coalition

"The Smile of the Child", a member of Missing Children Europe (MCE) and International Centre for Missing and Exploited Children (ICMEC) participates to the European Financial Coalition against Commercial Sexual Exploitation of Children Online (EFC). This initiative brings together key actors from law enforcement, the private sector and civil society in Europe with the common goal of fighting the commercial sexual exploitation of children online. Members of the EFC join forces to take action on the payment and ICT systems that are used to run these illegal operations. For more information click here: http://www.europeanfinancialcoalition.eu/index.php

Most of the actions of informative nature are implemented by the E.C.P. but also various Non Governmental Organizations that are focused on the safer use of Internet.

The Hellenic Police Headquarters and the Directorate of Electronic Crime Prosecution, apart the electronic crime suppression, gives special emphasis on the prevention via updating and sensitization of the citizens. In such context, an integrated campaign for the information and sensitization has been planned which includes many innovative actions, aiming to inform the citizens, emphasizing to the students' community updating, about the dangers underlying during their Internet surfing and the ways to avoid such dangers. Such actions are the following :

- Cyberkid applications for portable devices (Apps) : The cyberkid application for mobiles was created with the purpose to daily inform the parents and the children of every family for the safe internet surfing and the dangers underlying in it. At the same time, it is an interactive application which gives the ability of direct communication with the Directorate of the Electronic Crime Prosecution via the CYBER ALERT line but also via the sending of a direct email message, by simply pressing a button, while there is the possibility of entertainment via the various games.

- Hellenic Police Website www.hellenic police.gr : In the mentioned site and especially in the Unit : Citizen's Guide, useful advice has been included by care of the Di.E.C.P. with regard to the safe surfing in the Internet. Furthermore, the Di.E.C.P. issues on a daily basis, Press Releases which are published in the mentioned website and by which it informs the citizens regarding its activity, as well as newly arising methods for the commission of electronic crimes. Indicatively it is mentioned that, on 03.03.2015 it published for the information and sensitization of the parents, the "Communication Code" of the Pedophiles in the Internet, which was presented in summary together with the symbols used by the pedophiles to recognize their sexual preferences between each other and which arose from a relevant manual detected in the darknet, after many months of investigations by specialized Officers of such Service.

The National CERT contributes to the cyber crime prevention by organizing trainings (day congresses, seminars) addresses mainly to staff of the public sector and crucial infrastructures.
Prevention is not addressed or mentioned explicitly in the national law 2472/1997. However, according to its powers as described in article 19, the HDPA shall

- issue instructions for the purpose of a uniform application of the rules pertaining to the protection of individuals against the processing of personal data,
- shall call on and assist trade unions and other associations of legal and natural persons keeping personal data files in the preparation of codes of conduct for the more effective protection of the right to privacy and in general the rights and fundamental liberties of all natural persons active in their field,

- deliver opinions with respect to any rules relating to the processing and protection of personal data,
- issue regulations pertaining to special, technical and detailed matters to which the data protection law refers.
- Exercising the above powers contributes to the raising of awareness both among data controllers and data subjects, which in itself constitutes a form of prevention.

8.3. Prevention

8.3.1. National legislation/policy and other measures

The Hellenic Police Headquarters and the Directorate of Electronic Crime Prosecution, apart the electronic crime suppression, gives special emphasis on the prevention via updating and sensitization of the citizens. In such context, an integrated campaign for the information and sensitization has been planned which includes many innovative actions, aiming to inform the citizens, emphasizing to the students' community updating, about the dangers underlying during their Internet surfing and the ways to avoid such dangers. **Protocol of Cooperation with the National Co-Federation of Hellenic Trade (N.C.H.T.)**

A Protocol of Cooperation with the National Co-Federation of Hellenic Trade (N.C.H.T.) was signed by the Directorate of Electronic Crime Prosecution and the National Co-Federation of Hellenic Trade for the promotion and the coordination of actions to the benefit of the healthy organized trade and the consumers. The aim of such cooperation is the commonly systematic and scientific study of the issues and the problems that arise for the trade and the consumers from the electronic transactions, as well as the design and implementation of targeted informative actions, aiming to the updating of merchants and consumers regarding the internet dangers and the safe use of the Internet in the commercial transactions and the internet purchases.

By the increased use of the Internet in electronic purchases and commercial transactions, it was found imperative the expansion of the information for the safer use of the Internet and the further information among others, also of the commercial world. In this context, Di.E.C.P. will proceed to the updating and education of the commercial world in all width of computers use and in all problems that arise from the transactions via the same, aiming to the safe effectuation of transactions via Internet and the protection of the commercial companies as well as the consumers from any form of cyber fraud.

It is noticed that the National Co-Federation of Hellenic Trade (N.C.H.T.) via its action, aims to the constant updating via innovative actions and internet applications of the 630.000 commercial enterprises in matters of safer internet use and safer management of the e-trade procedures, a procedure that will be a tool for the development and increase of productivity and electronic trade via the faster disposition of the products to the "digital" market.

Website cyberkid.gr

Aiming to the better information of the public and due to the wide acceptance of such action but also the heavy visitation of the website by students and citizens, there will be a systematic watch of the website cyberkid.gr and constant updating of the information given, regarding the issues that fall in the field of competence of the Directorate of Electronic Crime Prosecution since this is imposed by the acceptance of the basic information and education interchange via the innovative applications that operate in the mentioned website. Presently, many schools surf in this website every day and they make in there, the internet education of their students, via various innovative applications that exist to this effect.

The HDPA does not organise prevention activities per se. However, we aim at raising awareness regarding data protection and privacy. For example, the HDPA frequently organises talks in schools, where the auditors address privacy and data protection issues arising upon using the internet. Talks have also been recently given to students from relevant fields of study (e.g. law, journalism). A series of talks is also given annually, in the context of the European Data Protection Day on the 28th of January. Finally, the HDPA publishes on its website a quarterly e-newsletter with its recent decisions, current developments in the field of personal data on a national, European and international level, as well as information about other recent activities of the HDPA.

"The Smile of the Child" has developed a wide spectrum of supportive and social actions for children at risk and children who have been victims of sexual abuse. One of the main actions is the National Helpline for Children SOS 1056. As a result of this experience the organization has developed a programme of primary and secondary prevention on thematic areas including safety on the internet. This program refers to the educational community with relevant informational and raising awareness initiatives targeted to students, parents and teachers.

The programme is mainly implemented at school classes in the framework of a Memorandum of Cooperation that has been signed between "The Smile of the Child" and the Ministry of Education and Religious Affairs. The preventive sessions are taking place following an invitation either by the School Advisor, the Health Education Teacher, the Headmaster, the Teacher Association, or the Parents and Legal Guardian Association. However, the programme is also implemented in private schools, sport associations, summer camps, etc., where the Psychologists are also performing preventive interventions.

One of the main tools of this work is the You Learn Interactive Platform of Education and Information that allows us to approach more students, parents and teachers and do prevention at schools in geographically remote areas in Greece and in Greek schools abroad. In 2014 "The Smile of the Child" performed interventions to 35.279 children, 5.636 parents and 1.415 teachers. 614 interventions took place in 13 regions of Greece. In 2014 the team organized 23 interventions on Internet safety issues for parents and guardians and 95 interventions for students. YouSmile platform is also one of the main tools of this work in the levels of prevention and awareness-raising.

8.3.2. Public Private Partnership (PPP)

Judicial and police authorities cooperate with Banks and the Hellenic Bank Association, as already exposed previously.

8.4. Conclusions

- Greece are active in this work and participate in different exercises. In the context of the national exercises of cyber war "Panoptis" wide participation exists from academic institutes, agencies of public and private sector.
- The cybercrime training is not mandatory for all prosecutors and judges but in the future they should have a certain numbers of hours in this field of training.
- Overall, the Greek authorities work strongly with prevention and awareness-raising as well as training in different areas of cybercrime. They have a good cooperation with the private sector and with other departments.
- The awareness campaigns expenses can be covered by sponsorships from companies of the sector of information, science and communications, which constitutes a good practice.

- Good examples of prevention and awareness raising are the work with non-governmental organization “The Smile of the Child". This non-profit voluntary organisation provides services to children on a 24-hour, 7 days a week, 365 days a year-basis, working for their physical, mental, and psychological stability. “The Smile of the Child” is in the process of using new digital tools in cooperation with international authorities and partners for the purposes of combating child pornography and other cybercrimes, setting these tools to the disposal of law enforcement authorities.
- Another good example related also to prevention and awareness raising is the work with *Cyberkid*. A safe website (www.cyberkid.gr) has been created by the staff of The Hellenic Police within the Directorate of Electronic Crime Prosecution. At the website children as well as parents may, via interactive activities and constant updating, be informed about the modes of safer surfing. Additionally, for mobiles and tablets, there has been created a free application with useful information regarding the internet surfing while a phone call is automatically made to the call center of their Service by simply pressing a button. Specialized officers deal with every incident, including those that require immediate handling (i.e. suicidal intention signs). The service can be used through different platforms and througt different social media (Facebook, Twitter).
- The Department of Innovative Actions and Strategy have produced a number of information leaflets and also TV and radio spots to reach out to the citizens regarding to information about Internet and electronic crime.
- Also mentionable is the fact that the Hellenic Police Directorate of Electronic Crime Prosecution will complete the updating via teleconferences of the students of all schools throughout the State – that is approximately 10.000 School Units – for their safer surfing on the Internet, the dangers underlying there and the ways to confront the same.

9. FINAL REMARKS AND RECOMMENDATIONS

9.1. Suggestions from Greece

9.2. Recommendations

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

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

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

9.2.1. Recommendations to Greece[7]

1. Greece should adopt as soon as possible the National Cyber Security Strategy, together with an Action Plan in order to implement it.[8]

2. Greece should put in place a mechanism to provide coherent and standardised statistics on investigations, prosecutions and convictions in cybercrime, which it would be very helpful to create a global image of this phenomenon.[9]

7 By virtue of Law 4411/2016, Greece has (a) ratified the Convention on Cybercrime of the Council of Europe (Budapest Convention, CETS 185) and (b) transposed into the Greek national order the dispositions of Directive 2013/40/EC on attacks against information systems.

8 Since November 2016, a (new) Ministry of Digital Policy has been established, according to art. 4 of Presidential Decree 123/2016). By virtue of Law 4386/2016, a General Secretariat of Digital Policy has been instituted within the new Ministry. These developments reinforce the coordination between Ministries towards a National Strategic Plan for Digital Policy, as well as implement the commitment of our country to have a centralized structure, at the highest level, for the planning and coordination of digital policy projects, monitored by the European Commission as a thematic objective of the PA (Partnership Agreement for the Development Framework) 2014-2020.

9 An "Integrated Management System of Civil and Penal Cases" is currently (after the evaluation visit) under construction, within the judicial system, with the aim, among others, to provide all needed data and statistics regarding cybercrime (mainly prosecutions and convictions).

3. The national authorities should make efforts in order to increase the number of personnel at Hellenic Police Department of Digital Evidence Examination. This would be very helpful for decreasing the length of the forensic examinations and consequently it would have beneficial consequences on the length of trials as well.[10]

4. Greece should take into account the possibility to increase the number of specialized prosecutors in cybercrime, which could be a useful method of sharing information and experience.[11]

5. On the field of fighting against online child sexual exploitation the establishment of an organized national database would be recommended in order to improve the proper use of Interpol ICSE and to develop victim identification.

6. Greece should use more the judicial and police cooperation's instruments, as JITs and cyber patrols.

7. Greece should continue to develop the excellent training programs on cybercrime, including by some other relevant actors involved in fighting against cybercrime, as prosecutors and judges.

[10] Paragraph 2 of article 41 of L. 4249/2014 provides for the recruitment of three hundred policemen with special skills. This personnel will be distributed (placed in) to several police services, including Hellenic Police Department of Digital Evidence Examination, by virtue of a Presidential Decree, which is going to be edited.

[11] Following the establishment of the Sub-Division of Cyber Crime Prosecution in Thessaloniki, specialized prosecutor has been appointed in the Public Prosecutor's Office of District Court Judges of Thessaloniki.

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

1. The Member States should consider developing useful tools and bodies, as the Greek Special 24/7 Cybercrime Emergency Service, called the Cyber Alert, where specialized officers deal with every incident, including those that require immediate handling.

2. Member States should consider the Greek good practice in blocking, filtering and removal of the web sites with illegal content.

3. The Member States are encouraged to consider the possibility of introduction in the national law of the obligation for the credit institutions to report without delay cyber-attack incidents that target both the credit institutions and/or their customers.

4. Following the annulment of Directive 2006/24/EC of 15 March 2006, the European Union and Member States are encouraged to reflect on the most appropriate way to remedy the lack of harmonisation of national laws regarding the electronic traffic data retention, while fully considering both operational needs and the protection of fundamental rights.

5. The European institutions should increase the EU funding to help Member States to organize more training for national practitioners in cybercrime.

6. The European Union and its Member States should reflect how to improve the cooperation with the major international telecommunication companies.

9.2.3. Recommendations to Eurojust/Europol/ENISA

1. Eurojust, Europol and ENISA should consider raising awareness of the services and the existing possibilities for cooperation and specialised training that they offer in the area of cybercrime.

2. Eurojust, Europol and ENISA should consider actively supporting events that strengthen international cooperation with regard to combating cybercrime, such as the Global Cyber Space Conference.

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

7th Round of Mutual Evaluations - Greece 29 September - 2 OCTOBER 2015

Tuesday 29 September 2015

Venue: Ministry of Justice, Transparency and Human Right

9.30-10.00 Welcome speech and opening remarks

10.00-10.30 "Implementation of the Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography"

10.30-11.00 "Provisions of substantive criminal law, statistics on the number of registered cases, investigations, prosecutions and final convictions regarding Mutual Legal Assistance with third countries"

11.00-11.30 "The fight against cybercrime under the Hellenic National Defence General Staff"

11.30-12.00 Coffee break

12.00-12.30 "The competences of the National Authority against Electronic Attacks / handling cybersecurity incidents"

12.30-13.00 Education and training

13.00-13.30 "The contribution of the Greek Desk at Eurojust in cybercrime cases"

13.30-14.00 "Blocking of access to web pages containing or disseminating child pornography"

14.00-15.00 Lunch at the Ministry's premises

15.00-15.30 "Assurance of Infrastructures, Privacy of Services and Internet applications"

15.30-16.30 Presentation of the NGO "The smile of the child"

16.00-16.30 "National Cybersecurity Strategy"

Wednesday 30 September 2015

Venue: the Division of Cybercrime Hellenic Police - Ministry of Interior and Administrative Reconstruction

9.30-11.30 "Cybercrime and online payment card fraud"
"Child sexual exploitation"

11.30-12.00 Coffee Break

12.00-14.00 "Cybercrime: current and future status"
"Innovative actions and strategy of Cyber Crime Division"

14.00-15.00 Lunch in the restaurant of general Police Directorate of Attica

Venue: Public Prosecutor's Office to the Court of Appeals - Athens

15.30-16.00 "International cooperation tools, surrender and extradition"

16.00-16.30 "Case law in relation to the provisions of substantive criminal law on cybercrime"

Thursday 1 October 2015

Venue: Forensic Division - Hellenic Police - Ministry of Interior and Administrative Reconstruction

10.00-10.05 Welcome Speech by the Deputy Director of the Forensic Division

10.05-10.20 "General presentation of the Digital Evidence Examination Laboratory"

10.20-10.45 "Forensic examination of cases regarding child sexual abuse"

10.45-1.05 "Fraud and financial forensics"

11.05-11.30 "Digital forensics in cyber attacks"

11.30-12.00 Coffee break

12.00-12.20 "Digital forensics: research challenges and open problems"

12.20-12.40 "Presentation of the activities of the Division, including trainings initiative"

12.40-13.00 "Education, further education regarding cybercrime"

13.00-13.30 Discussion with representatives of the Division. Presentation of facilities and the Labs

Venue: Hellenic Bank Association

14.00-15.00 Lunch at the Hellenic Bank Association premises

15.00-15.10 "Banking supervision framework for cyber risk"

15.10-15.20 "Supervisory assessment of cyber risk in the Greek banking sector"

15.20-15.25 "Payment systems oversight approach to cyber resilience"

15.25-15.30 "Cybercrime prevention: the HBA's role"

15.30-15.40 "Cyber security dealing in the Greek banking sector"

15.40-15.50 "Web banking and credit card fraud"

15.50-16.00 "Cyber-threats: before and after Capital-Controls"

16.00-16.10 "Distributed denial of Service (DDoS) Attack - a case study anaysis"

16.10-17.00 Questions and answers

Friday 2 October 2014

Venue: Ministry of Justice, Transparency and Human Rights

09.30-11.00 Wrap-up meeting

ANNEX B: PERSONS INTERVIEWED/MET

Meetings

Venue: Ministry of Justice, Transparency and Human rights

Person interviewed/met	**Organisation represented**
Sotiropoulou Sophia	Judge to the Court of Appeal, Athens
Skouvaris Kostas	Judge to the Court of First Instance
Preventis Sergios	Police Lieutenant, Directorate of Organization and Legal Support of the Greek Police Headquarters
Gizis Dimitrios	Prosecutor, had of criminal Prosecution Division, responsible for cybercrime issues
Eleftheriadou Argyro	Head of the Directorate of Legislative Work, International Relations and International Judicial Cooperation
Anastopoulos Vasileios	Captain, Hellenic national Defence General Staff - Cyberdefence Directorate
Trandalidi Magda	Ministry of Culture, Education and Religious Affairs
Angelis Ioannis	Prosecutor to the Court of Appeal, Athens, head of MLA Division, National School of Judges
Paschalis Nikolaos	Deputy national member of the Greek Desk of Eurojust
Giannopoulou Mina	National Telecommunications and Post Commission
Kanakaris Panagiotis	Expert, Hellenic Authority for Communication Security and Privacy
Pardalis Panos	Communications Officer, The Smile of the Child
Athanasiou Irini	Ministry of Infrastructure, Transport and Networks

Venue: Division of cybercrime - Hellenic Police - Ministry of Interior and Administrative reconstruction

Person interviewed/met	**Organisation represented**
Fragkiadaki Despina	Police captain
Germanos Georgios	Police captain
Chatzipanagiotis Panagiotis	Police captain
Kioulafas Christos	Police captain
Doukeli Aimilia	Police captain
Groutzidou Maria	Police lieutenant

Venue: Forensic Division - Hellenic Police - Ministry of Interior and Administrative Reconstruction

Person interviewed/met	**Organisation represented**
Deltsidis Apostolos	Police major
Antonopoulos Panagiotis	Police captain
Antoniou Dimitrios	Police captain
Georgakis Efthimios	Police lieutenant
Antonatos Ioannis	Police lieutenant
Krieris Dimitrios	Police lieutenant

Venue: Hellenic Bank Association

Person interviewed/met	**Organisation represented**
Gallis Dimosthenis	Deputy Head of IT Supervision and Audit Section, Bank of Greece
Kanellopoulos Ioannis	Head of IT Supervision and Audit Section, Bank of Greece
Kaliontzoglou Alexandros	Payment Systems Oversight Section, Bank of Greece
Panagiotidis Vasilis	Director, Hellenic Bank Association
Moschonas Gerasimos	Group Information Security Officer, Alpha Bank
Topakas Christakis	Group IT Security and Control Office, Piraeus Bank
Mavroforakis Michael	Group IT Governance Director, CISO, National Bank of Greece
Tzanos Ioannis	Group Corporate Security Officer, Eurobank

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

List of acronyms, abbreviations and terms	Acronym in original language	Full Name in original language	English
ADAE			Hellenic Authority for Communication, Security and Privacy
BoG			Bank of Greece
CCPA			Communication Privacy Protection Authority
CERT			National Information Agency
CIO			Criminal Investigation Offices
CIS			Criminal Investigation Stations
CSS			Center for Security Studies
Di.E.C.P.			Directorate of Electronic Crime Prosecution
DCD			Directorate of Cyber Defence
DCI			Directorate of Criminal Investigations
EBF			European Banking Federation
EC3			Europol's European Cybercrime Center

List of acronyms, abbreviations and terms	Acronym in original language	Full Name in original language	English
EETT			Hellenic Telecommunications and Post Commission
EFC			European Financial Coalition against Commercial Sexual Exploitation of Children Online
EMPACT			European Multidisciplinary Platform against Crime Threats
ENISA			European Union Agency for Network and Information Security
GENVAL			Working Party on General Matters including Evaluations
HBA			Hellenic Bank Association
HDPA			Hellenic Data Protection Authority
HISP			Hosting Internet Service Provider
ICMEC			International Centre for Missing and Exploited Children
INHOPE			International Association of InternetHotlines
IP			Internet Protocol
MCE			Missing Children Europe
MLA			Mutual Legal Assistance

List of acronyms, abbreviations and terms	Acronym in original language	Full Name in original language	English
MCCC			Military Center for the Confrontation of Cyber incidents
MoU			Memorandum of Understanding
National CERT			National Authority for the Confrontation of cyber Attacks
NCPC			National Communication and Post Commitee
NDGH			National Defence General Headquarters
NIA			National Information Agency
NSRF			National Strategic Reference Framework
SAFENET			Hellenic Organ of Self-Regulation for the Internet Content
SSM			Single Supervisory Mechanism

_____