A Survey of Cyber Crime in Greece

Alexandros Papanikolaou, Vasileios Vlachos, Anastasios Papathanasiou,
Konstantinos Chaikalis, Maria Dimou, and Magdalini Karadimou

***Abstract* — During the past years, the Internet has evolved into the so-called "Web 2.0". Nevertheless, the wide use of the offered Internet services has rendered individual users a potential target to cyber criminals. The paper presents a review and analysis of various cyber crimes, based on the cases that were reported to the Cyber Crime and Computer Crime Unit of the Greek Police Force and compares them to similar data of other EU countries.**

***Keywords* — Cyber crime, Greek cyber crime, EU cyber crime.**

I. Introduction

PERSONAL computers, smart phones and mobile devices are ubiquitous in modern, technologically-advanced societies. In addition, the expansion of the Internet and Web 2.0 has given citizens a vast variety of options and services, thus allowing communication and collaboration among them. On the other hand, the so-called *cyberspace* tends to be exploited by *cyber criminals*, who are able to attack their victims beyond any geographical constraints, as long as they are online. Thus, the wide proliferation of Information and Communications Technology (ICT), in addition to the numerous positive effects to citizens and society in general, provided a new field of criminality in cyberspace. The term *cyber crime* integrates all these criminal activities that are made with the use of computers and the Internet, including economic frauds, child pornography, identity theft and intellectual property crimes. It is worth pointing out that in many cases the use of computers does not change the fundamental character of a crime. For instance, a bribery remains a bribery, regardless of how the money was transferred (electronically, in the case of cyber crime) and despite the fact that the use of a computer may affect the degree of the offence. Nevertheless, the introduction of information and communication systems has certainly triggered a qualitative change.

The Internet is attractive to technologically-savvy criminals because it provides them with the opportunity to locate and research their victims' behaviour, widens their field of activity and offers them the potential to change their identity. More importantly, they can operate from another country, thus making their prosecution a complex matter, due to the different legal frameworks and the international procedures that should be followed in order to arrest them. Contrary to traditional crimes, the perpetrator and the victim are seldom in the same geographical location. Therefore, the law enforcement agencies face several difficulties in both investigating and closing such crime cases.

Cyberspace is nowadays characterised as the fifth common domain (the others being land, sea, air and outer space) and is in great need for coordination, cooperation and legal measures among all nations [1], as cyber crimes tend to increase day by day, leading to soaring revenues for the criminals and lack of trust for Internet users. According to recent reports, over 80% of online shoppers cited security as a primary issue to worry about when conducting business over the Internet [2]. In Australia, cyber crime costs to businesses are more than $600 million a year, while in the US one in five online consumers has been a victim of cyber crime in the last two years, equating to $8 billion [2]. Another report on cyber crime remarks 556 millions of users being manipulated each year, which in fact is more than the entire population of the European Union [3]. More alarmingly, less than half of all victims call their financial institution or the police and just over a third contact the website owner or email provider. A serious effort to combat these types of crimes would demand collaboration among countries and businesses, in order to form a common defence strategy to come into prominence and affront the problem in the best possible way. It is necessary to achieve a safe and reliable cyberspace environment in the context of an emerging information society to maximise the benefits of the ICT [1].

This paper is an extended version of the work presented in [4]. The rest of the paper is organised as follows. Section II looks at the related work and similar initiatives, both domestic and international. Section III presents and analyses the statistical data. Section IV discusses some aspects of cyber crime in relation to the presented statistical data. Section V briefly presents statistics related to cyber crime among EU countries, while Section VI concludes this paper with some remarks regarding the future direction of this research.

Paper received February 27, 2014; revised September 12, 2014; accepted September 19, 2014. Date of publication November 15, 2014. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Vlado Delić.

This paper is a revised and expanded version of the paper presented at the 21th Telecommunications Forum TELFOR 2013.

Corresponding Alexandros Papanikolaou, Vasileios Vlachos, Konstantinos Chaikalis and Magdalini Karadimou are with the Department of Computer Science & Engineering, Technological Educational Institute of Thessaly, Larissa, Greece (email: alxpapanikolaou@gmail.com, {vsvlachos, kchaikalis}@teilar.gr, m_karadimou@hotmail.com).

Anastasios Papathanasiou is with the Cyber Crime Prosecution Subdivision, Financial Police and Cyber Crime Unit, Hellenic Police (email: a.papathanasiou@cybercrimeunit.gr).

Maria Dimou is with the Department of Electrical and Computer Engineering, University of Thessaly, Volos, Greece (email: mdimou@uth.gr).

II. Related Work

The importance of user education as a critical point in defeating cyber crime should not be neglected. The majority of Internet users do not know or are not well informed about the threats they may face. For instance, there is evidence that low self-control is a significant predictor of person-based cyber crime victimisation [5]. According to RAT (Routine Activities Theory), crime results when three things converge in time and space: a motivated offender, a suitable target and the lack of a capable guardian [5]. Therefore, clicking on pop-up messages, downloading games or music or even opening unknown email attachments increases exceedingly the likelihood of online victimisation. Recent evidence identifies the web's most dangerous search terms from a malware perspective, as well as the most dangerous domains [6].

Modern trends and the need for socialisation that led to social networks brought up a whole new perspective for cyber criminals and a wide area for them to exploit. Attackers take advantage of the still-evolving understanding of online social networking safety practices to defraud people and organisations [5]. From the empirical evidence of the first endeavours of Kevin Mitnick to the latest theoretical development on the social engineering methodologies, people are the weakest link [7]. Therefore, skilled adversaries have the skills to approach them and bypass all security measures. Most of the indicators show that future cyber crimes are expected to be more severe, more complex and more difficult to prevent, detect and address than current ones [8].

Individuals are not the only target of cyber criminals. In many cases, most of them known, the public sector has been trespassed and exposed by upcoming and ambitious perpetrators. Recent evidence correlates cyber criminals with state actors as an effective way to perform various hostile acts, such as industrial espionage, denial-of-service (DoS) attacks etc. with plausible deniability [9]. Hence, establishing common strategic directions all over the world, common legislation and a great level of coordination among countries is required, in order to defeat cyber crime. Governmental agencies seem to be understaffed of highly educated personnel and technologically advanced equipment, with respect to the workload they have to cope with, though recently most central governments realise the level of the threat and outlay significant funds to protect themselves from upcoming and aspiring cyber criminals [10].

Research regarding cyber crime is still in its early stages in Greece, where people tend to believe that cyber crime is not one of their primary concerns. In fact, research conducted by PricewaterhouseCoopers, a London-based services firm, collected some really interesting and at the same time alarming results about Greece [11]. A high percentage of Greek companies declared not having been trespassed over the last year, while the maximum number of attacks reported by companies was 2. There is a very high chance that these companies did not even realise that they were being attacked and they were therefore not able to report it. Cybex is a system used in Greece, in order to mitigate the problem of cyber crime [12]. Under the auspice of UNICIR, Greece is trying to develop effective mechanisms to enhance cyber security. Cybex is a three-year programme that calls upon countries to select representatives who will act as tutors in educating the countries officers and public servants. Greece has been subscribed to this program since 2008 along with ten other European countries. In [13] a detailed report on law measurements taken against cyber crime is presented. It analysed what a cyber crime is, the terms under which cyber crime is committed, as well as the means that cyber criminals use. Furthermore, it presents references to the Greek Criminal Code that are related to cyber crime, with respect to the sentences fined by the Greek Justice in each case.

Extensive research results on the addictive effects of the Internet, focusing on the concerns of the effects of social networking sites, are presented in [14]. Their dominating role into an individual's life is emphasised, as well as the way cyber criminals use them in order to manipulate human mind and retrieve information. In the same work there is also an extended investigation of sexual offences towards minors and a study of how all these actions constitute illegal acts [15].

In [16] the Greek Internet Safety Hotline (SafeLine) is introduced. Its mission is to eliminate any photographic and audiovisual content that implies violation on children's human rights. The authors arrived at the conclusion that all upcoming frauds aim at financial profits. SafeLine was also studied by another group of researchers, who provided all the necessary information on how a cyber crime should be reported, the importance of the collaboration with the police, as well as useful advice on how children can be protected from ambitious criminals [17].

According to the Presidential Decree 100/2004, within the Police Division of Attica, Subdivision of Financial Crimes Antiquities and Ethics, the 5th Department of Cyber Crime was founded and put into operation, which was responsible for the prosecution of crimes committed over the Internet. Then, on January 3, 2005 the respective department within the jurisdiction of the Police Division of Thessaloniki was founded and was made operational. Subsequently, the structure of these cyber crime departments was re-organised, improved and specialised. Hence, with the P.D. 9/2011 entitled "Establishment, organisation and operation of the Financial and Cyber Crime Police Unit" [18], the Financial and Cyber Crime Police Unit (FCCPU) was founded and came into operation in July 2011, as an independent Central Office subjected to the Hellenic Police and supervised/controlled by the Chief of the Hellenic Police.

III. Cyber Crime Incidents in Greece in 2011 and 2012

A. Cyber Crime Examples

Several instances of the well-known "Nigerian letters" cyber crime occurred in December 2011. These involved sending emails to Internet users for supposedly pending

large amounts of money, mainly earned by participation in lotteries. The purpose was to collect personal information of the recipients of these letters. The messages were written in English and were also sent to mobile phone numbers. These messages were announcing to the recipient that they had won e.g. two million euros. In a second cyber crime case on September 2011, three people were accused for fraud and for exploiting a mobile phone company. By using advanced techniques, they succeeded in hacking into the company's computer systems and they managed to illegally sell Internet connections to Cuba. The result was the company to be charged with the amount of 690,501 euros.

Another cyber crime case in 2011 had to do with accessing pornographic websites. While the website was still loading, a message appeared automatically, informing the users that they had visited sites with child pornography and for this reason the computer had been blocked by the Cyber Crime Police. The user would then have to pay to avoid being accused by the police. Eventually, it was discovered that the data was being stored on a Ukrainian server. Finally, in May 2012 a travel agency owner in Thessaloniki was accused of Internet fraud, because travel packages were advertised through different Facebook profiles. Tickets or hotel reservations were proved to be fake, while in other cases overcharging of credit cards was noticed.

B. *Cyber Crime Statistics for 2011*

According to statistical data provided by the Ministry of Citizen Protection of the Greek Government for 2011, the majority of cyber crime cases using social networks had been made through Facebook, as it is shown in Table 1. Significantly fewer cases using other social networks were recorded (e.g. Twitter, Zoo, Badoo, Adoos, Windows Live).

TABLE 1. SOCIAL NETWORKING CRIMES IN GREECE IN 2011.

Social network	***Number of crimes***
Facebook	327
Windows Live	1
Adoos	5
Twitter	2
Zoo	5
Badoo	2
Total	**342**

The most important cyber crime cases in 2011 using Facebook, out of a total of 327, are broken down as follows (Fig. 1): 203 cases of potential suicide, 30 cases of hacking of personal data (photos posted without permission, fake profiles, etc.), 17 cases of statutory rape and 15 cases of threats. Fewer cases were observed for drugs, guns, kidnapping and so on. As can be seen, the majority of the cases have to do with suicides. The second most frequent cases have to do with personal data hacking, while child seduction follows. It can therefore be concluded that suicides are a significant problem for social networks and special care must be taken, given that such networks are very popular among young people.

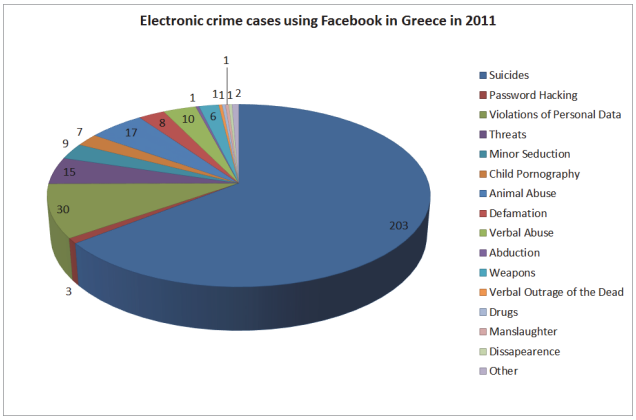

Fig. 1. Cyber crime cases using Facebook social networking service in Greece in 2011.

C. *Cyber Crime Statistics for 2012*

In Fig. 2 the various cyber crime categories in Greece for 2012 are shown. The category with the highest percentage is the one involving e-commerce and web-based services protection, followed by frauds regarding social security. Further down the list are illegal online games and casinos, followed by satellite piracy.

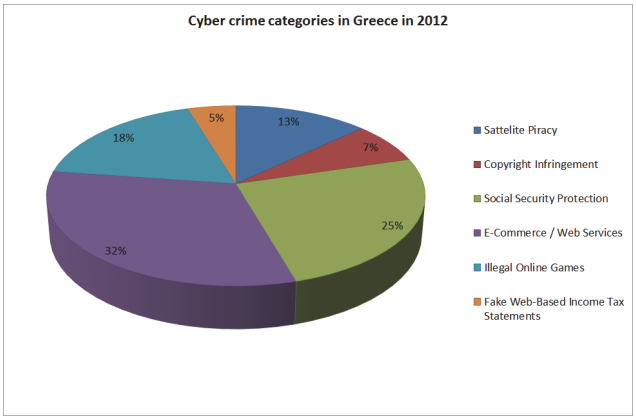

Fig. 2. Cyber crime categories in Greece in 2012.

Table 2 presents a summary of the number of accused and arrested people for cyber crime in Greece in 2012. The graph also shows seven different categories of cyber crime (satellite piracy, child pornography, fraud using the Internet, computing systems hacking, telecommunications hacking, personal data hacking, copyright infringement). As can be seen, the majority of people accused and arrested were for child pornography and Internet fraud.

Fig. 3 shows a statistical analysis of the number of arrests concerning cyber crime for different Greek prefectures in 2012. It was quite expectable for Athens to have the lead in the number of recorded arrests, as it is significantly larger compared to other cities. In the next two larger cities, Thessaloniki and Irakleio, an approximately equal number of arrests have occurred. It is also interesting that in some small cities (e.g. Drama) a considerably large number of arrests with respect to their population have been made. On the other hand, there are instances of relatively large cities (e.g. Larissa) which exhibit a much smaller number of arrests.

TABLE 2. CYBER CRIME ACCUSES AND ARRESTS IN GREECE IN 2012.

Cyber crime description	*Accused*	*Arrested*
Satellite piracy	33	6
Copyright infringement	37	12
Telecommunications privacy hacking	8	4
Child pornography	113	58
Internet fraud	105	6
Computer systems hacking	16	1
Personal data hacking	20	3
Other	126	14
Total	**458**	**104**

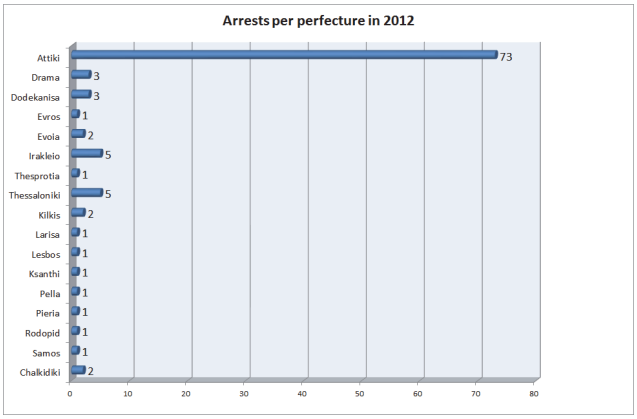

Fig. 3. Arrests per prefecture in 2012.

Table 3 presents the flagrant cyber crime for the two halves of 2012. Child pornography has the largest number of instances for both periods of 2012, followed by copyright infringement.

TABLE 3. FLAGRANT CYBER CRIME IN GREECE IN 2012.

Flagrant cyber crime description	*Jan–Jun 2012*	*Jul–Dec 2012*
Satellite piracy	3	3
Copyright infringement	7	5
Violations of privacy in telecommunications	3	1
Child pornography	22	36
Internet frauds	6	0
Violation of computer systems	1	0
Violation of privacy legislation	1	2
Other	8	6
Total	**51**	**53**

Table 4 presents the cyber crime cases for the two halves of 2012. As can be seen, the vast majority of the cases filed were also processed, despite the fact that the total number of cases was quite large. Furthermore, although an increase of approximately 9% in the number of filed cyber crime cases for the second half of 2012 is observed, the number of processed cases also increased by approximately 10.5%, meaning that the Department of Cyber Crime of Hellenic Police successfully managed to keep up with the additional workload.

TABLE 4. NUMBER OF CYBER CRIME CASES IN GREECE THAT WERE FILED AND PROCESSED IN 2012.

	Cases filed	*Cases processed*	*Difference*
Jan–Jun 2012	775	746	29 (3.74%)
Jul–Dec 2012	848	824	24 (2.83%)
Total	**1623**	**1570**	**53 (3.27%)**

Fig. 4 shows the suicide prevention cases by the Department of Cyber Crime of Hellenic Police in 2012. Most of suicide attempts occur in December, followed by September and October. Furthermore, the fewest occurrences of suicide attempts were noted in March, which happens to be the beginning of spring.

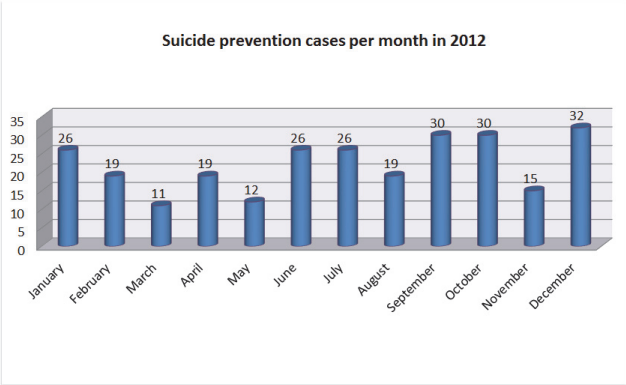

Fig. 4. Suicide prevention cases per month in 2012.

Finally, Fig. 5 shows that most cyber crime confiscations in 2012 involve desktops (hard drives and DVDs). On the other hand, confiscations regarding wireless devices (mobile phones, smartphones, etc.) are fewer. Nevertheless, since such wireless devices have penetrated our everyday lives, it is quite expectable that in the near future there will be an increase in the confiscations of such devices.

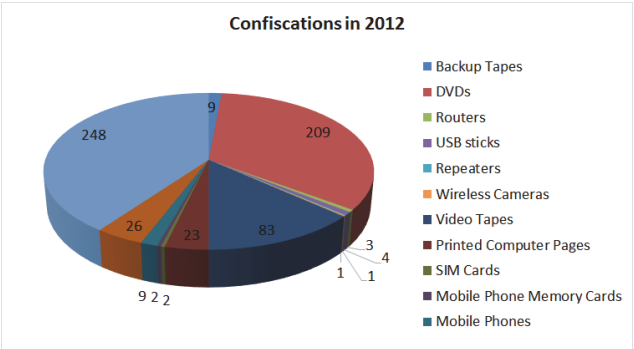

Fig. 5. Confiscations in 2012.

IV. DISCUSSION

The statistical data presented in Section III, make it evident that almost one year after its establishment, the Greek Cyber Crime Prosecution Subdivision (GCCPS) has significant results to exhibit for 2012. More specifically, a total of 458 people were accused of committing various cyber crimes and a total of 104 people were arrested. One of its most important achievements was the prevention of

suicide attempts that were detected, where the individuals were motivated either by personal reasons (and were publicising their intentions mainly via Facebook), or because they had become victims of other cyber crimes and could not cope any more with the psychological pressure exerted on them by the perpetrators.

The lack of appropriate user awareness and training is possibly one of the most important reasons that allow such cyber crime incidents to take place or helps them prolong their lifecycle (e.g. for hoax e-mails and chain letters). Generally speaking, unaware users tend not to pay enough attention to privacy matters, either due to their inability to think/foresee ways that their publicly-available information could be exploited so as to cause harm to them, or because they are under the impression that "they have nothing to hide". What is more, the various personal electronic devices with the ability to connect to the Internet increase the attack surface dramatically, with the possibility of granting a remote attacker access to a large collection of personal information (photographs, contacts' details, authentication credentials). In cases where users realise that they have become victims of a cyber attack specifically targeting them, their lack of knowledge and experience can trigger extreme reactions from their side, sometimes leading to even committing suicide.

Cyber crime is also related to the current socio-political circumstances. For instance, during the past years, Greece is suffering from an economic crisis, featuring quite a strong presence of financial cyber crimes. Examples of such incidents are fake employment agencies that require a fee in advance and promise to offer jobs, though they never do so; travel agents offering extremely cheap vacation packages that never reach the customers who have paid for them; illegal online gambling services advertising particularly tempting payouts. By using the data of an e-mail help service, the authors in [19] estimated that between the years 2007 and 2009 (preceding the beginning of the economic crisis) the number of cyber crime cases related to financial fraud were 49.4% of the 491 total cases. The observed increase in financial cyber crime since then is therefore a strong indicator of a possible correlation with the Greek economic crisis that started around mid 2010.

V. Cyber Crime across the EU

This section presents statistics regarding cyber crime in the EU, so as to enable an evaluation of the status which Greece is currently in. Due to space limitations, it is not possible to give a detailed account of cyber crime statistics among other EU countries, therefore a summary of indicative statistics will be provided.

According to a recent report [20], 73% of the EU citizens surveyed answered that they had seen or heard something about cyber crime in the last 12 months (March 2011 to March 2012). They were primarily informed about cyber crime via television (59%), although the presence of other sources was quite significant too (ranging from 19% to 27%). The vast majority of them therefore know that cyber crime exists and it is quite probable that they are aware of the severity of its consequences or even that they can identify it correctly when they see instances of it. The respondents from the Scandinavian countries and the Netherlands are most likely to say that they have seen or heard anything about cyber crime (percentages ranged from 90% to 95%), whereas the lowest scores were observed in Portugal (53%) and Italy (51%), followed by Poland (62%) and Bulgaria (63%). Nevertheless, there is considerable variation among EU countries in the extent to which respondents feel well informed about cyber crime. Respondents in Denmark (73%), Sweden (69%) and Finland (63%) feel quite well informed, whereas the lowest scores were observed in Bulgaria (24%), Italy (24%), Portugal (24%), Romania (25%), Greece (27%) and Spain (28%).

As far as personal experience of cyber crime is concerned, 38% of Internet users across the EU have received phishing e-mails that were either asking them for money or personal details. In particular, Internet users of the Netherlands (54%), Denmark (54%), Malta (53%), Sweden (53%), UK (52%) and Luxembourg (51%) are the most frequent recipients of scam e-mails, whereas the ones in Poland (19%), Bulgaria (18%) and Greece (18%) are the least frequent ones.

Moreover, 15% of Internet users have come across material promoting racial hatred or religious extremism and 13% were unable to access online services (e.g. web banking) due to denial-of-service (DoS) attacks. The highest figures of offensive material were observed in Hungary (30%), Romania (26%) and Slovakia (26%), and the lowest ones in Denmark (7%) and Greece (9%). In Finland (31%) and the Netherlands (28%) the percentages of users not being able to access online services is considerably higher than the average, while the lowest figures occur in Greece (4%), Czech Republic (6%), Latvia (6%) and Cyprus (7%).

What is more, a total of 21% of the EU Internet users have experienced cyber crime themselves, either by not receiving the goods they ordered online (13%), or by becoming victims of identity theft (8%). The vast majority of EU countries exhibit levels close to the calculated average. The highest figures were observed in Romania (16%), Hungary (12%), UK (12%) and Austria, whereas the lowest ones were observed in Slovenia (2%), Lithuania (2%), Greece (3%) and Denmark (3%).

VI. Conclusion

Cyber crime represents a new and fast-growing crime category in Greece within the last few years. In this paper, a statistical analysis of cyber crime has been presented, considering various parameters. In particular, for 2011 our analysis shows that suicide attempts through Facebook were the most frequently occurring cyber crime type, whereas for the following year the most predominant cyber crime type was related to e-commerce and web services. In 2012 the majority of accuses and arrests occurred for child pornography, which exhibits the sensitivity of the law enforcement body on this matter, as well as good efficiency in dealing with it. Furthermore, statistics show that there were approximately 10% more cyber crime cases in the second semester of 2012. Another

interesting remark is that the highest number of suicide cases occurs in December, followed by September and October. Finally, the majority of confiscations in 2012 involve desktop computers, something that was quite expectable, as they are the main means for committing most of the cyber crimes.

In the future we expect cyber crime to become the dominant crime category, since the various technological advancements have caused our societies to gradually become "e-societies". We hope that technological revolution of the past 20 years which gave birth to cyber crime, will find the way to fight this new crime type.

ACKNOWLEDGMENT

The authors would like to kindly acknowledge the Cyber Crime Department of Hellenic Police Force for providing anonymous statistical data.

REFERENCES

[1] S. Schjolberg and S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*, 2nd ed. AiTOslo, 2011.

[2] H. Saini, Y. S. Rao, and T. C. Panda, "Cyber-crimes and their impacts: A review," *International Journal of Engineering Research and Applications*, vol. 2, pp. 202–209, 2012.

[3] "2012 Norton cybercrime report," Symantec, Tech. Rep., 2012.

[4] A. Papanikolaou, V. Vlachos, A. Papathanasiou, K. Chaikalis, M. Dimou, and M. Karadimou, "Cyber crime in Greece: How bad is it?," in *Proc. 21st Telecommunications Forum (TELFOR)*, Belgrade, Serbia, 2013, pp. 1–4.

[5] F. T. Ngo and R. Paternoster, "Cybercrime victimization: An examination of individual and situational level factors," *International Journal of Cyber Criminology*, vol. 5, pp. 773–793, 2011.

[6] S. Keats and E. Koshy, "The Web's most dangerous search terms," McAfee Inc., Technical Report, 2008.

[7] C. Hadnagy, *Social Engineering: The Art of Human Hacking*. Wiley, 2011.

[8] "Cyber crime: A clear and present danger combating the fastest growing cyber security threat," Deloitte's New Center for Security & Privacy solution, Technical Report, 2010.

[9] R. Clarke and R. Knake, Cyber War. New York, NY: HarperCollins, 2010.

[10] "The UK cyber security strategy – Protecting and promoting the UK in a digital world," UK Cabinet Office, Tech. Rep., 2011.

[11] "Cybercrime goes unreported in Greece," Phys.Org. Available: http://phys.org/news/2013-02-cybercrime-unreported-greece.html, 2013.

[12] D. Brystowski, "Cybercrime". Available: http://yu.edu/admissions/events/yunmun/UNODC/UNDOC-cybercrime-greece.pdf, 2013.

[13] P. Markopoulou, "The convention on cybercrime". Available: http://intellectum.org/articles/issues/intellectum4/en/ITL04p043052 The%20Convention%20on%20Cybercrime_Pagona%20Markopoulou.pdf, 2008.

[14] E. Papanis, "Research about the Facebook," http://www.dart.gov.gr/data/files/facebook.pdf, 2010.

[15] ——, "Research about the Facebook," http://www.dart.gov.gr/data/files/paidofilia&diadiktyo.pdf, 2010.

[16] M. Christdoulaki and P. Fragopoulou, "Safeline: Reporting illegal internet content," *International Management and Computer Security*, vol. 18, pp. 54–65, 2010.

[17] "SafeLine2: Continuing and advancing the Greek internet hotline in the fight against cyber crime," FORTHnet SA, Technical Report, 2008.

[18] Presidential Decree 9/2011, "Establishment, Organisation and Operation of the Financial Police and Cyber Crime Unit (FPCCU)," Government Gazette A-24 21/02/2011, 2011.

[19] V. Vlachos, M. Minou, V. Assimakoloulos, and A. Toska. The Landscape of Cybercrime in Greece, *Information Management & Computer Security*, vol. 19, no. 2, pp. 113–123, 2011.

[20] "Cyber security", Eurobarometer Special Surveys, Report 390. Available: http://ec.europa.eu/public_opinion/archives/eb_special_399_380_en.htm#390, 2012.