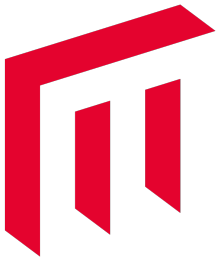


MALMÖ UNIVERSITY
FACULTY OF HEALTH AND SOCIETY

TARGETING THE ESCALATION OF CYBERCRIME IN GREECE

A SYSTEMATIC LITERATURE REVIEW

Katerina Paraskeva

Degree Project in Criminology
30 Credits, Master's Programme

Malmö University
Faculty of Health and Society

TARGETING THE ESCALATION OF CYBERCRIME IN GREECE

A SYSTEMATIC LITERATURE REVIEW

Katerina Paraskeva

Paraskeva, K. Targeting the escalation of cybercrime in Greece. A systematic literature review. *Degree Project in Criminology, 30 credits*. Malmö University: Faculty of Health and Society

Abstract:

Cybercrime refers to any illegal use of the technology- computer, networked device or a network-for criminal acts and constitutes a rapidly evolving and complex phenomenon as the Internet is ruling on almost every sector of human activity. Innovation plays a highly significant role in the growth of an economy. However, every time there is an advancement in the field of technology, there is bound to be other adverse effects. Such is the case with criminology. In this end, the prevalence of cybercrime is alarmingly increasing, and there have been several attempts by the government and other concerned agencies at stemming its escalation (Curtis et al., 2009). The following thesis shows the investigation of the rise of cybercrime in Greece. It is a systematic literature review available on this topic, aiming to explore areas such as the preparedness of the government in the fight against cybercrime and the consideration that in so doing, it is obligated to protect the rights of intellectual property as well as the protection of the rights to privacy of its citizens (Gobran, 2015). Of all the categories of information technology-related crimes, cybercrimes are the most common. The thesis also explores the conventions and laws employed by the law enforcement in the efforts to counter the activities of cybercrime, including their effectiveness. It also establishes the different sectors and industries with the highest rates of cybercrime activities and the ways in which these sectors are fighting against these activities.

Keywords: criminology, cybercrime, escalation, systematic literature review

TABLE OF CONTENTS

INTRODUCTION AND BACKGROUND

Since the discovery of the Internet, a myriad of cybercrime activities has been terrorizing people all over the world (Gobran, 2015). These premeditated crimes are executed by individuals with exclusive and expert knowledge of computers (Alazab et al., 2013). Greece experiences two significant classes of cybercrime activities; the machines are used as a tool to help smugglers in their businesses of smuggling goods and people as well as other conventional criminal activities, and the use of computers to aid individuals in the evasion of taxes through the help of cybercriminals (TNS Opinion & Social, 2012). This thesis follows the results of a vast volume of literature available on the escalation of cybercrime in different regions around the world, including Greece. Several countries have reported difficulties in the detection and prosecution of cybercrimes. Cyber security is increasingly becoming an essential aspect in the protection of intellectual property, not to mention the protection of the privacy of the citizens of a country. In an age where the technology is undergoing unceasing developments and advancement, cybercrimes are taking different shapes and forms, hence the need for constant updates and upgrades to the security systems (Newman and Clarke, 2002; Yar, 2005).

The theoretical foundations to the public policy have been significantly impacted on by the increasingly pervasive nature of the daily lives of the victims taken by cybercrime (Felson and Cohen, 1980). As such, the governance of cyberspace becomes very difficult as different countries present varying ideas and opinions in the solutions thereof. Cybercrime activities have become a very vital important subject in criminology following their dynamic, complex, and multifaceted nature (Maxfield, 1987). They result in very adverse effects on the social and economic aspects of a country. It is evident through research that the cybercrime economy is fueled by several factors, including the availability of cybercriminals at the disposal of those in need of their services. Some economies have experienced very detrimental crises, all attributed to the actions of cybercriminals. This thesis establishes that cybercrime has a very significant importance in society because it has been reported to target approximately

all classes of people and people are increasingly storing and sharing confidential and personal information in platforms that can be accessed by cybercriminals. Cyber-attacks and cybercrime victimization are mainly on the high end of the scale in growing and stabilizing economies such as Greece where cybercriminals target the loopholes existing in an expanding economy (Felson and Cohen, 1980; Harichandran et al., 2016).

AIM

This thesis as a systematic literature review aims at establishing the impacts of the escalated rate of cybercrimes in Greece. An increased volume of research and studies have been conducted on this topic whose results are discussed herein. It is also the focus of this paper to investigate the efforts of the law enforcement with a criminological aspect, in the fight against cybercrimes and their effectiveness. Additionally, it illustrates the different sectors and industries influenced by the activities of cybercriminals and the preventive, protective, and control measures employed in eliminating them as well as reducing their impacts.

RESEARCH QUESTIONS

The thesis aims at addressing the following research questions;

1. What are the impacts of the escalation of cybercrimes on law enforcement and other agencies in their attempts to devise sustainable preventive measures;
2. How has the escalation of cybercrime in Greece influenced the health care, education, and banking and finance sectors in the past decades; and
3. How has the adoption and implementation of new technological upgrades influenced the escalation of cybercrimes in Greece and some detection, preventive, and control measures employed in this regard.

THEORETICAL FRAMEWORK

The Routine Activity Theory , as presented by Cohen and Felson (1979), plays a very vital role in the study of crime rates. It postulates that the occurrence of a crime is highly reliant on the availability of three factors; a motivated offender, an appropriate target, and the absence of a responsible guardian (Cohen and Felson, 1979). As a significant theoretical approach in criminology, Routine Activity Theory, like its relation to the Lifestyle-Exposure Theory (Felson and Cohen, 1980), plays a very critical role in the development of the content for this thesis. The approach further provides an essential basis on which the literature for this review is gauged to determine its relevance and significance to the topic of targeting the escalation of cybercrime in Greece. It provides that the structuring of the routine activities in a particular society influences the kind of situations experienced by the constituents of that society and the changes thereof result in a shift in the circumstances that emerge (Cohen and Felson, 1979; Bennett, 1991). Additionally, people react according to the situations they are confronted with on a daily basis, which is inclusive of their involvement in the crime (Bernburg and Thorlindsson, 2001). Therefore, Routine Activity Theory (RAT) provides criminologists with a way of determining the crime rates in a society following the establishment of the influence of regular activities in that society (Cohen and Felson, 1979; Cohen et al., 1981).

The theory further establishes a connection between the macro-level structural model and the micro-level situational model, providing a much more in-depth explanation of why crime occurs (Felson and Cohen, 1980). The situational model postulates that the manifestation of a crime is a result of the convergence of the factors as mentioned earlier. The Routine Activity Theory and its connections to other methods of criminology, including the rational choice theory, which explains that people respond to situations depending on the facts provided (Felson, 2013). Furthermore, an understanding of the provisions of this theory provides investigators with the platform to explore the crime rates of individuals, not to mention their impacts on the crime rates of the entire society (Maxfield, 1987), for instance, Greece. It is very instrumental in its application as a crime prevention technique (Williams and Levi, 2017).

Instead of positioning technology as an entity separate from the broad society, the digital society concepts places it at the center of the larger social entity and recognizes technology as embedded in the organization in the form of media, networks, and digital technologies in our daily lives (Livingstone and Haddon, 2008). This includes its application in fields including but not limited to; victimization, perpetration of a crime, and justice (Stratton et al., 2017). The rate at which technology is transforming lives has caused the emergence of digital criminology attributed to the resolution of problems related to cybercrime activities (Stratton et al., 2017; Cruz-Cunha and Portela, 2015). A collection of literature available on the escalation of cybercrime in Greece has been analyzed in this thesis and sorted according to their relevance to promote the establishment of the solution that can be employed to curb this menace.

Previous studies note that international security, following the governance of cyberspace, is impacted adversely by the unchecked sovereign power of states as they are placed at the forefront in the development and opportunities exploited by cybercriminals (Fidler et al., 2013). The review of the available research promotes the development of the theory that the escalation of cybercrime activities, in European countries; specifically, Greece, is aided by the lack of rigid and concrete laws governing the detection and prosecution of cybercrimes (Rughiniş and Rughiniş, 2014). Therefore, it has been very effortless for cybercriminals to conduct their activities in the country with something g close to an assurance that they will never be caught. This has fueled an increase in the growth experienced by the cybercrime ecosystem as a firearm, illegal goods, people, and other commodities exchange hands over the web especially after the continuous growth of the Web 2.0. This research establishes the impacts of this escalation, even as efforts are made to devise substantial solutions to eliminate this vice.

METHODOLOGY

Research Method

All the literature involved in the development of this thesis is systematically selected to fulfill the requirements of this thesis and its concerns. A qualitative analysis has been conducted to establish the suitability of each source to the topic under discussion. Greece is virtually at a high risk of experiencing cyber-attacks following its passage and incorporation of broadband technologies, which has created a haven for cybercriminals to expand their activities (Papathanasiou et al., 2013).

Systematic literature review

Systematic literature reviews "are a form of research; they are (and the theoretical and ideological perspectives underlying these methods) a way of bringing together what is known from the re- search literature using explicit and accountable methods." (Gough, et al., 2012; p.1) The methods of a systematic literature review are evolved specifically for analyzing the effect of the existed findings; this fact incorporates the results of the research that applies experimental controlled designs. However, the perspective of the methods in systematic literature reviews are referred to every scientific department. Consequently it is possible that development is found in the systematic literature on the same level as in initial studies. (ibid.,2012)

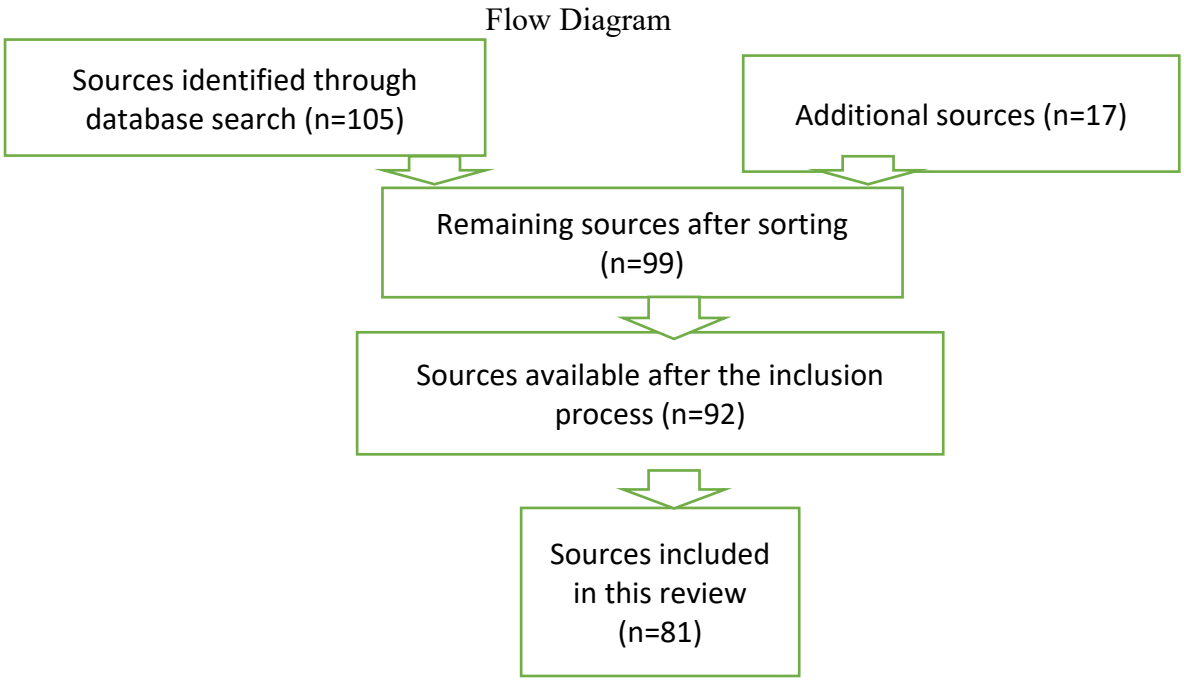
Inclusion and Exclusion criteria

The literature included in this review has been subjected to a comprehensive inclusion and exclusion criteria. As such, it is established that its significance to the thesis has a direct impact on its quality, not to mention its impact on the relevance thereof. All the articles are peer-reviewed and each study is carefully investigated, and a conclusion determining its relation to the requirements of the topic concluded to establish its suitability. The results of this process can be taken from the facts presented in this thesis in which is collected using both qualitative and quantitative tools, not to mention the review of other discussions and other documents.

As for the exclusion criteria in this thesis, the existed literature of the subject under investigation is limited so many sources about cybercrime were excluded. The topic analyzes cybercrime in correlation with the rise of the phenomenon Greece so the

sources were focusing mostly on this context. The language of the selected sources was in English so every other source was excluded.

Flow Diagram



Databases and Keywords

Sorting through an increased volume of research required the use of several keywords in the different databases that facilitated the determination of the correct sources of information for this thesis. These keywords are used in Google Scholar , the Google search engine and, Malmö University's electronic library and they include "cyber," "cybercrime," "cybercrime in Greece" "cyber security in EU," "digital criminology," "criminology." Cybercrime is a common hindrance to the adoption and implementation of communication and information technologies, especially in modern society.

Advantages and Limitations of the Method

Qualitative analysis allows for an in-depth dive into the research topic to establish, behaviors and attitudes. It is preferred for its record of both ranks and counts, and the additional information regarding the reason for a specific response. However, even though it eliminates the existence of presumptions and pre-judgments, qualitative analysis is significantly dependent on the skills of the researcher and only allows for the analysis of a reduced sample.

Ethical Considerations

It is paramount that research respects the outlined regulations regarding the subjects under investigation. In the case of this literature review, it affects different categories of subjects, hospitals, schools, industries, and agencies that are synonymous with people. Therefore, the most significant ethical consideration of this review is that which reflects its effects on humans. Its benefits should be such that they exceed the extent of the risk for which it is conducted. However, since this is only a literature review in which no classified information and documents, consents, and permission is needed from the research subjects, so no ethical approval is required from Malmö University. It presents an analysis of previous research regarding the topic under investigation. To promote the ease of locating the information included herein, a reference list is provided.

Previous Research

An increased volume of research and studies have been performed on this topic whose results are discussed herein. Most of it has been focused on the prevention, detection, and control of cybercrimes in Greece (Rughiniş and Rughiniş, 2014). Even

though numerous studies have been conducted on the topic of cybercrime globally, not many of them have specifically been focused on the escalation of cybercrime in Greece.

CYBERCRIME IN GREECE

Papanikolaou et al., (2014a), input that Greece has especially been impacted by the modern trends in the development of the networks that enhance socialization. The ubiquity observed in a technologically advanced society is presented by mobile devices, computers, and smartphones. Following the advancements of the web 2.0 and other social networking platforms, cybercriminals identify a new perspective inclusive of new and better aspects that can be exploited (Papanikolaou et al., 2014b; Vaxevanakis, Zahariadis and Vogiatzis, 2003).

Greece has experienced attacks and the exposure of its public sector by both ambitious and upcoming cybercriminals (Papanikolaou et al., 2014a). Shreds of evidence recently discovered correlates state actors with cybercriminals which effectively promotes the perpetration of hostile acts, including the denial of services attacks (DoS), and industrial espionage with plausible deniability (Papanikolaou et al., 2014b; Grabosky and Smith, 2001). Studies suggest that for a unified and strengthened effort in the fight against cybercrime, it is convenient that countries all over the world enhance prevailing strategic direction (Pease, 2001). It is critical to note that studies stipulate that when individuals and organizations experience attacks, most of them do not even notice and, therefore, no report of the attacks are made like in the case of Greece. As a result, the development of Cybex ensued, a program similar to NATO (Fidler et al., 2013), allowing its users to mitigate cybercrime through the development and implementation of effective mechanisms. It constitutes a three-year program that entails the selection of representatives by member countries who then educate public servants and other officers on factors such as what cybercrime is, the techniques used by cybercriminals to perpetuate it, and the fines and punishments (Li, 2017). It also provides a reference to the justice system of Greece and the penalties attached to cybercrime activities as stipulated in the Greek Criminal Code.

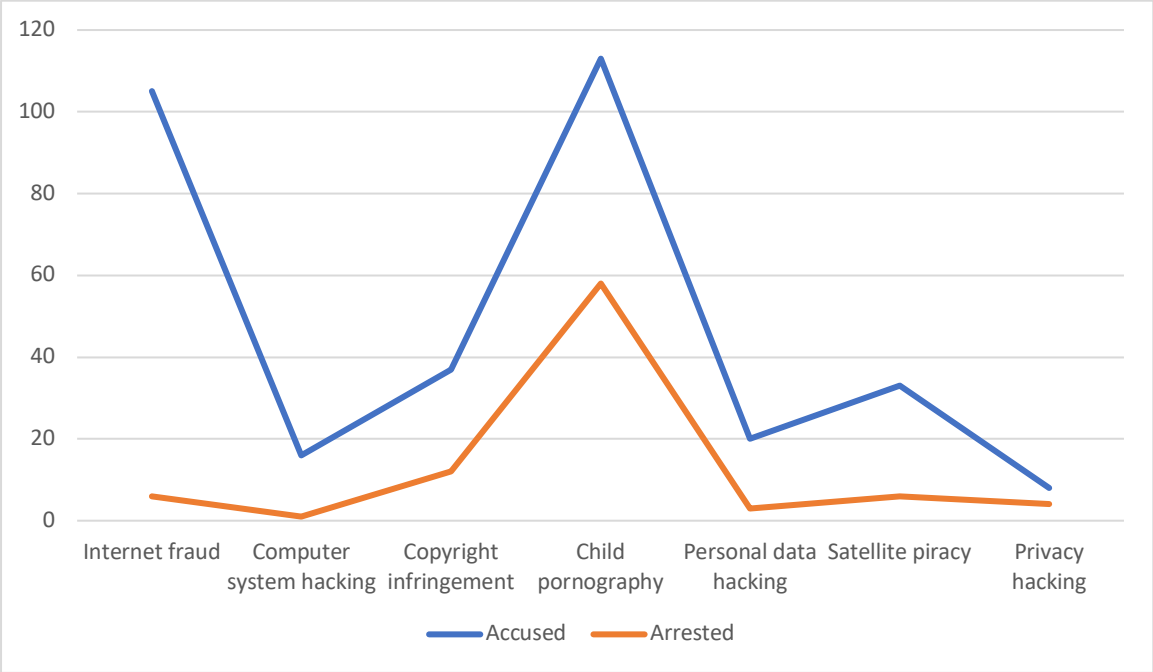
For instance, phishing, which involves the capturing of an individual's financial information with the intent of manipulating their financial and online banking data illegally (Pratt et al., 2010; Gupta et al., 2017); pharming has been popular for a long

Social Network	Number of Crimes
Ados	5
Facebook	327
Twitter	2
Badoo	2
Windows Live	1
Zoo	5
Total	**342**

time and is used to divert the traffic of a legitimate website to another used by cybercriminals (Obied and Alhajj, 2009); key logging has to be the most common form of illegal activity perpetrated by cybercriminals. The table above shows cybercrime cases associated with the use of Facebook and other social networking platforms in Greece in 2011 (Papanikolaou et al., 2014a).

Cybercrime adopted a whole new approach and employed the use of different techniques in Greece following the adoption of the broadband technologies (Vlachos et al., 2011; Polykalas and Vlachos, 2006). It follows that a society that continually undergoes the evolving stages of embracing technological advancements is a catalyst to the application of the information and communication technology (ICT) growths (Vlachos et al., 2011; Polykalas and Vlachos, 2006). However, cybercrime poses a hindrance to the employment of these technologies by the modern society. When voluntary cases by public sector servants and employees in Greece were submitted for analysis in a study to determine the shifts in the content when it came to cybercrime activities, the results are indicative of the remarkable rise in the activities perpetrated by cybercriminals. It can be deduced from the findings that Greek users are much more concerned about cybercrime activities that take a primary relation to the newly introduced social networking, including cyberbullying, cyber-extortions, and schemes of financial fraud (Vlachos et al., 2011; Krambia Kapardis and Papastergiou, 2016). The escalation of these activities in Greece is attributed to the growth and development

of the social networks in which people store information, including that regarding their private and financial statuses. This can be seen from the graph below (Papanikolaou et al., 2014a)



The rate at which the complexity, diversification, and expansion of the strategies and practices used in cybercrime pose a significant risk in the assessment, detection, and establishment of sustainable solutions in terms of policies meant to prevent these crimes (Sabillon et al., 2016). This has proven to be a hindrance to the investigation of the magnitude of the embedded risk presented by these activities, including the prevention techniques to protect individuals, organizations, and corporations alike. The field of criminology is consequently presented with the task of conducting research extensively to enable the determination of the most effective regulations and policies in attempts to outdo the cybercriminals (ibid., 2016; Thomas and Loader, 2000; Krambia Kapardis and Papastergiou, 2016; Williams and Levi, 2017). This is especially critical for some industries such as the healthcare and the financial sectors.

When research has been conducted on the impacts of cybercrime on the industries contained in a country, it is established in these industries, as mentioned above, experience the most detrimental effects. This is simply because they involve the use and storage of confidential and volatile information whose destruction or acquisition by unauthorized hands could entirely destroy these organizations; hence the ease of victimization (Ngo and Paternoster, 2011; Furnell, 2002).

Another aspect of cybercrime that is very prevalent in Greece is online child exploitation, which represents a constantly growing phenomenon on an international basis. This results from the lack of focus by the government to improve the social sectors. As such, research proposes that the detection of the cybercrimes that focus on children, when done early enough, could promote the decline in their prevalence (Floros et al., 2013; Livingstone and Smith, 2014; Fragkou, 2018). A particular analysis by Scherrer and Ballegooij (2017), indicates that on a daily basis, the number of children that encounter exploitation and abuse while online. Research shows that the prevalence of child exploitation in the form of emotional, physical, and sexual abuse, exceeds the perception levels of the society, even as many render it unforgivable (Scherrer and Ballegooij, 2017; Fragkou, 2018).

Primary educators must be imparted with the knowledge regarding the prevention and detection of child exploitation cybercrimes (Glasner, 2010; Berson, 2003; Davies, 2004; Livingstone and Haddon, 2008). The Internet has presented the world with new learning and developmental opportunities. These include children who can increase the scope of their experiences in addition to gaining new knowledge (Floros et al., 2013). However, it goes without saying that children often present an easy target for cybercriminals because they are perceived as being defenseless (Glasner, 2010; Cockbain and Brayley, 2012). This has also promoted malicious practices such as child trafficking exposing young children to a myriad of risk factors, especially diseases (O'Connell Davidson, 2011). The precarious activities that these children are forced to engage in are unfathomable (Livingstone and Smith, 2014).

The structuring and partitions of the Internet are such that children appear defenseless against virtual exploitation (Armagh, 2001). Regardless of the availability of laws and regulations governing the safe use of the Internet by children in different countries, there still exists a gap in the level of education and awareness of children about online safety (Davies, 2004; Kierkegaard, 2008). Research inputs that over the past decades since the introduction of the Internet, the age at which children begin to access the Internet has alarmingly declined while the number of children accessing resources online continues to skyrocket (Kierkegaard, 2008). It is indicated in most studies regarding the use of the Internet by children that school includes the one environment in which they can safely access it.

This follows the benefits accrued to classroom supervision, the availability of monitoring and filtering software, and the regulations enhancing acceptable-use that

parents, children, and teachers agree to follow (Laud et al., 2013). Even though there is a deficiency in the presence of a foolproof technological approach that can be applied to entirely protect children accessing the Internet, teaching them discrimination and selective techniques promotes their safety (Laud et al., 2013).

RESULTS

1. The Impacts of the Escalation of Cybercrimes on Law Enforcement and other Agencies in their attempts to Devise Sustainable Preventive Measures

The theoretical antecedents of a digital society present the bodies and agencies involved in the criminology of computing and cybercrimes with an expanded, innovative, and informative crime and justice framework (Miethe and Meier, 1990). Concerning the escalation of cybercrimes in countries inclusive of Greece, research indicates that there has inadequate focus put on the Internet of things, social web, and big data, by the computing and cybercrime research and theories (Miethe and Meier, 1990; Thakur et al., 2016; Yar, 2005). These paramount technological shifts have shown an apparent rift between the perceptions of the law enforcement, and other agencies fighting against cybercrime, and the actual impacts of technology, not just as a tool facilitating common crimes, but as a critical causal element in the investigation of criminal activities (Wikström, 2004). It can be applied to the comprehensive understanding and exploration of the cybercrimes to promote the establishment of sustainable solutions concerning its detection, prevention, and control.

The cybercrime industry in Greece has especially escalated following the understaffing of government agencies mandates with cyber security, their lack of equipment that could match that used by the perpetrators, and the tons of workload they have to pile through to address these issues (Papanikolaou et al., 2014a; Papathanasiou et al., 2013). Attempts have, however, been put in motion regarding the upgrade of government agencies to increase the quality of their outcomes when it comes to fighting cybercrimes. In this analysis of the scope of cybercrime in Greece, it is established that attackers are especially interested in the exploitation of the still-evolving constituents of the security practices regarding online social and wireless networking in the exploitation and defrauding of organizations as well as individuals (Papanikolaou et al., 2014b; Vaxevanakis, Zahariadis and Vogiatzis, 2003). When empirical studies have

been conducted on this topic, borrowing from the most aged to the most recent attempts on the theoretical improvements on the social engineering methodologies, people are established as the weakest link (Papanikolaou et al., 2014a; Furnell, 2005). This has promoted the conclusion that the sophistication, severity, and complexity of future cybercrimes will be such that they will be more challenging to prevent, detect, or even control.

2. How has Escalation of Cybercrime in Greece influenced the Health Care, Education, and Banking and Finance Sectors in the Past Decades

Several studies has focused on the emotional, physical, and sexual abuse of children through the emotional, physical, and sexual acts of exploitation (Cyr et al., 2013; Nesteruk and Marks, 2011). This alters the psychological and physical well-being of the child, which consequently tampers with their ability to perform in school. Therefore, the Greek and European legislation programs regarding the perpetration of such heinous acts against children provide a protective veil against the cyber exploitation of children (Davidson et al., 2011; Young and Widom, 2014; Rughiniş and Rughiniş, 2014). Following the escalation of such practices, Greece devised anti-trafficking laws whose awareness involves the use of specialists and experts and other stakeholders concerned with the children's welfare (Koumpoulas, 2015).

From the findings, it is evident that consumers are concerned about the security of their banking information, not to mention the protection of their privacy. It is now clear that cybercriminals are adamant when it comes to the exploitation of loopholes existing in newly launched and implemented systems whose protection practices are yet to gain root (Giovanis et al., 2012; Riek et al., 2015; More and Nalawade, 2015). Greece has adopted the internet banking services which necessitate the investigation of the influence of the extended Technology Acceptance Model (TAM) inclusive of the privacy risk evaluation, and the concepts of the Innovation Diffusion Theory (IDT) (Giovanis et al., 2012; More and Nalawade, 2015; Pantelidis, 2014). It makes it critical that the factors influencing the perceptions of Greek users and the differences in consumer attitudes are evaluated regarding the implementation of the new technology (Giovanis et al., 2012; Riek et al., 2015). As such, the relationship between the compatibility and the behavioral intentions of consumers are mediated by the privacy

and security risks perceived by the consumers and TAM (Giovanis et al., 2012; Riefenstahl, 2015).

Hospitals and other health care organizations have been hit with cases of cyber-attacks which have caused severe damages in their reputations so much so that some of them never recover (Mougiakakou et al., 2011). When an individual's information regarding finances has been accessed by cybercriminals, they have been extorted and made to pay lump sums to regain control of their accounts, which is never a guarantee. It is pivotal that these organizations, even as they strive to keep pace with the advancements taking place in the field of technology, device protection strategies to protect their networks against such attacks (Furnell, 2002; Mougiakakou et al., 2011). An increase in the levels of awareness, seeing as how humans present the weakest link to these perpetrators, by promoting best practices goes a long way in the enhancement of security (Ngo and Paternoster, 2011; Chawki, 2005).

3. How the Adoption and Implementation of New Technological Upgrades influenced the Escalation of Cybercrimes in Greece

An analysis of the presentations of the literature included in this thesis indicates that a number of factors influence the escalation of cybercrime activities in Greece. Firstly, the country's embrace of the broadband technologies which allowed the exploitation of the information and communication networks by cybercriminals (Alexiou et al., 2005). Secondly, the adoption of emerging social networking platforms, mainly social media sites. These have been a hotbed of cybercrime activities because of the several loopholes existing before preventive policies and practices can take effect (Grabosky and Smith, 2001). Lastly, the desire to join other nations as they migrate towards the attainment of a new social status as fueled by the advancements in technology. These developments allow these criminals to employ complicated and diverse techniques in the manipulation of information networks. A large number of resources show that in as much as research is pivotal; in the establishment of a sustainable solution, it should be supplemented by education and creating awareness to improve the quality of the outcomes.

The increase in the number of illegal tools that cyber criminals can apply to carry out their activities has promoted the escalation of cybercrime (Antoniadou and Kokkinos, 2015). This has allowed them an extremely wide spectrum in which they can

manipulate different industries, organizations, and individuals alike (Fisher, 2008). They employ the use of specific software that allows them to monitor and record keystrokes secretly to harvest personal data to facilitate espionage and fraud vendettas (Fisher, 2008); and the distributed denial of service which constitutes the burdening of computer resources with tasks inundating enough to make them unavailable to authorized users. This has promoted the growth and further expansion of the cybercrime industry, in addition to the inadequacy of the agencies mandated with the protection against it.

DISCUSSION

Cybercrime activities are a threat to all the aspects of the economy of Greece, as they are to the entire world (Ulsch, 2014). Reports are published and broadcast on a daily basis about attacks that are taking place throughout the globe. The diversifications that are taking place in the cybercrime industry are such that the criminology department of the law enforcement sector is at a loss for preventive policies and strategies (Saini et al., 2012). Greece has been on the map following its constant embrace and adoption of new technological approaches, especially in the social networking arena, the banking and finance sector, and the acceptance of implementing broadband technologies as have other European nations (Pantelidis, 2014). Although a lot of benefits can be reaped from upgrading into a modern society, it is essential to note that it also increases the vulnerabilities to attacks and exploitations by cybercriminals (Theocharidou and Gritzalis, 2009).

Even when programs, regulative and legislative, have been put in place to protect against cybercrime activities, cybercriminals have always used a complex and sophisticated software to bypass security protocols (Theocharidou and Gritzalis, 2009). Greece had experienced several cases of cybercrime incidences since 2011 when it embraced broadband technologies on a large scale (Papanikolaou et al., 2014a). Research attributes this to the inadequacy of an understanding of practices meant for the protection against such instances (Archick, 2004). The escalation of cybercrime in Greece has forced the criminology department and other agencies concerned with privacy protection to indulge in extensive research to promote an understanding of how cybercriminals work, their strategies and techniques, and to devise counteractive

measures to undo their damages (MOD, 2011). These agencies must cause an increase in awareness of these activities so that the masses are knowledgeable about the detection, prevention, and control of these activities despite their category (Thomas and Loader, 2000).

LIMITATIONS

One of the most significant limitations encountered in this literature review is the vast volume of materials available in connection to the topic of research. This gives the researcher a hard time sorting out the vast volume of literature to determine the one that is best suited for this topic; sorting according to relevance. Cybercrime, even when constrained to one nation, is a very extensive topic that has evoked increased interest in researchers attempting to post its comprehensive understanding. The expanse of potential victims is immense as well, which increases the scope of the research.

CONCLUSION

The impacts of cybercrime pose such a detrimental aftermath that their occurrence should be avoided and prevented at all costs. It stagnates the delivery and reception of goods and services by altering the normalcy of the programs involved (Saini et al., 2012). When some of the industries have come under the influence of the promulgation of cybercrime activities, the effects have been so significant so that their recovery was considerably impaired. The health care and the banking and finance sectors constitute some of the most sensitive spots if hit by cybercriminals. The information stored therein is susceptible if it were to fall in the wrong hands. As such, the leadership of these organizations needs to enhance the security of such information by maintaining an upgraded technological approach. According to the Association for Information Service Industries (2001), this involves an understanding and up-to-date analysis of the trends used by cybercriminals so that they can adjust their security systems accordingly (Ulsch, 2014).

The escalation of cybercrimes in Greece comprises the increase in child exploitation through the web, including sexual abuse and manipulation (Griffiths, 2000). This affects the nature and extent to which children can perform in school. The

psychological, physical, emotional, and sexual well-being of a child is of significant importance (Fragkou, 2018). Their protection against exploitation has taken a new outlook with nations, such as the European, coordinating programs that enhance the safety of children as they access the Internet (Christodoulaki and Fragopoulou, 2010; Hasebrink et al., 2009). In consideration to the bigger picture, it is the mandate of the criminology department, with the help of other welfare agencies and organizations, in Greece to work towards the containment of cybercrime activities affecting corporations, organizations, and individuals alike (Shackelford and Andres, 2010; Gogoni et al., 2015). Cyber security and the protection of the citizens' privacy are depending on them both physically and in the virtual approach of crime prevention (Aas, 2007).

REFERENCES

Aas, K.F. (2007) Beyond the desert of the real: Crime control in a virtual(ised) reality. In Jewkes Y (ed.) *Crime Online*: 160-177. Portland, Oregon: Willan Publishing.

Alazab, A., Abawajy, J., Hobbs, M., Layton, R. and Khraisat, A. (2013) Crime toolkits: the productisation of cybercrime. In *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 1626-1632). IEEE.

Alexiou, A., Bouras, C., Igglesis, V., Kapoulas, V., Paraskevas, M., Tsiatsos, T. and Papagiannopoulos, J., (2005) The broadband status in the region of Western Greece: overview and recommendations. *Broadband Europe*.

Antoniadou, N. and Kokkinos, C.M. (2015) A review of research on cyber-bullying in Greece. *International Journal of Adolescence and Youth*, *20*(2), pp.185-201.

Archick, K. (2004) Cybercrime: The Council of Europe Convention, CRS Report for Congress. In *Order Code RS21208, Congress Research Service* (Vol. 22).

Armagh, D.S., (2001) Virtual child pornography: Criminal conduct or protected speech. *Cardozo Law Review* 23(6): 1993-2010

Association for Information Service Industries, (2001) International Branch. "International trends in measures against cybercrime and the establishment of information security." *JISA Bulletin* 63. 77–90.

Bennett, R. (1991) Routine activities: A cross-national assessment of a criminological perspective. *Social Forces 70*, 147–63.

Bernburg, J. G. and Thorlindsson, T. (2001). Routine activities in social context: A closer look at the role of opportunity in deviant behavior. *Justice Quarterly 18*, 543–67.

Berson, I.R. (2003) Grooming cybervictims: The psychosocial effects of online exploitation for youth. *Journal of School Violence*, *2*(1), pp.5-18.

Chawki, M. (2005) A critical look at the regulation of cybercrime. *IV (4) The ICFAI Journal of Cyberlaw*.

Christodoulaki, M. and Fragopoulou, P. (2010) SafeLine: reporting illegal internet content. *Information Management & Computer Security*, *18*(1), pp.54-65.

Cockbain, E., & Brayley, H., (2012) Child sexual exploitation and youth offending: A research note. *European Journal of Criminology*, *9*(6), 689-700.

Cohen, L.E. and Felson, M., (1979) Social change and crime rate trends: A routine activity approach. *American sociological review*, pp.588-608.

Cohen, L.E., Kluegel, J.R. and Land, K.C., (1981) Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, pp.505-524.

Cruz-Cunha, M.M. and Portela, I.M., (2015) *Handbook of research on digital crime, cyberspace security, and information assurance*. Information Science Reference.

Curtis, G., Dolan, R., Elan, S., Ivey, N., Minkus, C., Solsten, E., Spiegel, T., Steen, T., Federal Research Division and United States of America, (2009) Cybercrime: An Annotated Bibliography of Select Foreign-Language Academic Literature.

Cyr, C., Michel, G., and Dumais, M. (2013) Child maltreatment as a global phenomenon: From trauma to prevention. *International Journal of Psychology, 48*(2), 141-148.

Davidson, J., Grove-Hills, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T. and Webster, S., (2011) Online abuse: Literature review and policy context. *Project Report) European online grooming project*.

Davies, L., (2004) The difference between child abuse and child protection could be you: Creating a community network of protective adults. *Child Abuse Review*, *13*, 426- 432.

Felson, M. and Cohen, L.E., (1980) Human ecology and crime: A routine activity approach. *Human Ecology*, *8*(4), pp.389-406.

Felson, M., (2013) Routine activity approach. In *Environmental criminology and crime analysis* (pp. 92-99). Willan.

Fidler, D.P., Pregent, R. and Vandurme, A., (2013) NATO, Cyber defense, and international law. . *John's J. Int'l & Comp. L.*, *4*, p.1.

Fisher, J. (2008) The UK's faster payment project: avoiding a bonanza for cybercrime fraudsters. *Journal of Financial Crime*, *15*(2), pp.155-164.

Floros, G.D., Siomos, K.E., Fisoun, V., Dafouli, E. and Geroukalis, D. (2013) Adolescent online cyberbullying in Greece: The impact of parental online security practices, bonding, and online impulsiveness. *Journal of School Health*, *83*(6), pp.445-453.

Fragkou, A. (2018) Greek Primary Educators' Perceptions of Strategies for Mitigating Cyber Child Exploitation. (*Doctoral dissertation, Walden University*).

Furnell, S., (2002) *Cybercrime: Vandalizing the information society*. London: Addison Wesley.

Furnell, S.M. (2005) Considering the security challenges in consumer-oriented eCommerce. In *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.* (pp. 534-539). IEEE.

Giovanis, A.N., Binioris, S. and Polychronopoulos, G. (2012) An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece. *EuroMed Journal of Business*, *7*(1), pp.24-53.

Glasner, A. T. (2010) On the front lines: Educating teachers about bullying and prevention methods. *Journal of Social Sciences*, *6*(4), 537-545.

Gobran, A. (2015) Cyber terrorrism threats (*Doctoral dissertation, Utica College*).

Gogoni, P., Athanasaki, E. and Venni, E. (2015) Social Pedagogical Reflexes of Greek Society during the Economic Crisis Period: Indicative Social Pedagogical Actions. *International Journal of Social Pedagogy*, *4*(1), pp.248-273.

Gough, David A., David Gough, Sandy Oliver, and James Thomas., (2012) *An Introduction to Systematic Reviews. Systematic Reviews.* London: SAGE.

Grabosky, P. and Smith, R. (2001) Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (ed.) *Crime and the internet*. London: Routledge.

Griffiths, M. (2000) *Sex on the Internet: Issues, concerns and implications* Goteborg. U.S.: UNESCO International Clearinghouse on Children and Violence on the Screen.

Gupta, B.B., Tewari, A., Jain, A.K. and Agrawal, D.P. (2017) Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), pp.3629-3654.

Harichandran, V.S., Breitinger, F., Baggili, I. and Marrington, A., (2016) Cyber forensics needs analysis survey: Revisiting the domain's needs a decade later. *Computers & Security*, *57*, pp.1-13.

Hasebrink, U., Livingstone, S., Haddon, L. and Olafsson, K., (2009) *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*. EU Kids Online.

Kierkegaard, S. (2008) Cybering, online grooming and ageplay. *Computer Law & Security Review*, *24*(1), pp.41-55.

Koumpoulas, P. (2015) *Questionnaire of the United Nations' special rapporteur for child, trafficking, child prostitution and child pornography. Ministry of Foreign Affairs of Greece*.

Krambia Kapardis, M. and Papastergiou, K. (2016) Fraud victimization in Greece: room for improvement in prevention and detection. *Journal of Financial Crime*, *23*(2), pp.481-500.

Laud, A., Gizani, S., Maragkou, S., Welbury, R. and Papagiannoulis, L. (2013) Child protection training, experience, and personal views of dentists in the prefecture of Attica, Greece. *International journal of paediatric dentistry*, *23*(1), pp.64-71.

Li, J.X. (2017) Cyber crime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Sciences*, *12*(2), pp.196-207.

Livingstone, S. and Haddon, L. (2008) Risky experiences for children online: Charting European research on children and the internet. *Children & society*, *22*(4), pp.314-323.

Livingstone, S. and Smith, P.K. (2014) Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, *55*(6), pp.635-654.

Maxfield, M.G., (1987) Lifestyle and routine activity theories of crime: Empirical studies of victimization, delinquency, and offender decision-making. *Journal of Quantitative Criminology*, *3*(4), pp.275-282.

Miethe, T. and Meier, R., (1990) Opportunity, choice and criminal victimization: A test of a theoretical model. *Journal of Research in Crime and Delinquency 27*, 243–66.

MOD, U. (2011) The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. *UK Gov*.

More, D.M.M. and Nalawade, M.P.J.D.K., (2015) Online banking and cyber-attacks: the current scenario. *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper*.

Mougiakakou, S.G., Kyriacou, E., Perakis, K., Papadopoulos, H., Androulidakis, A., Konnis, G., Tranfaglia, R., Pecchia, L., Bracale, U., Pattichis, C. and Koutsouris, D., (2011) A feasibility study for the provision of electronic

healthcare tools and services in areas of Greece, Cyprus and Italy. *Biomedical engineering online*, *10*(1), p.49.

Nesteruk, O., and Marks, L. D. (2011) Parenting in immigration: experiences of mothers and fathers from Eastern Europe raising children in the United States. *Journal of Comparative Family Studies, 42*(6), 809-825.

Newman, G. and Clarke, R., (2002) *Etailing: New opportunities for crime, new opportunities for prevention*. Produced for the Foresight Crime Prevention Panel by the Jill Dando Institute of Crime Science, UCL.

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

Obied, A. and Alhajj, R. (2009) Fraudulent and malicious sites on the web. *Applied intelligence*, *30*(2), pp.112-120.

O'Connell Davidson, J. (2011) Moving children? Child trafficking, child migration, and child rights. *Critical social policy*, *31*(3), pp.454-477.

Pantelidis, K. (2014) E-banking: a comparison study between Greek and foreign financial institutions, perspectives, weaknesses and innovations. (*Master Theses University of Macedonia*)

Papanikolaou, A., Vlachos, V., Papathanasiou, A., Chaikalis, K., Dimou, M. and Karadimou, M. (2014a) A survey of cyber crime in Greece. *Telfor Journal*, *6*(2), pp.86-91.

Papanikolaou, A., Vlachos, V., Papathanasiou, A., Chaikalis, K., Dimou, M., and Karadimou, M., (2014b) *Cyber-crime in Greece: How bad is it? In 2013 21st Telecommunications Forum Telfor (TELFOR) (pp. 1-4). IEEE.*

Papathanasiou, A., Papanikolaou, A., Vlachos, V., Chaikalis, K., Dimou, M., Karadimou, M. and Katsoula, V. (2013) Legal and social aspects of cybercrime in Greece. In *International Conference on e-Democracy* (pp. 153-164). Springer, Cham.

Pease, K. (2001) Crime futures and foresight: Challenging criminal behavior in the information age. In D. Wall (ed.) *Crime and the internet*. London: Routledge.

Polykalas, S.E. and Vlachos, K.G. (2006) Broadband penetration and broadband competition: evidence and analysis in the EU market. *info*, *8*(6), pp.15-30.

Pratt, T.C., Holtfreter, K. and Reisig, M.D. (2010) Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), pp.267-296.

Riefenstahl, L., (2015) Hacktivism and Whistleblowing in the Era of Forced Transparency? *Cybercrime Risks and Responses: Eastern and Western Perspectives*, p.85.

Riek, M., Bohme, R. and Moore, T. (2015) Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), pp.261-273.

Rughiniş, C. and Rughiniş, R. (2014) Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. *computers & security*, *43*, pp.111-125.

Sabillon, R., Cano, J., Cavaller Reyes, V. and Serra Ruiz, J. (2016) Cybercrime and cybercriminals: a comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4 (6)*.

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

Scherrer, A. and Ballegooij, W.V. (2017) Combating sexual abuse of children Directive 2011/93/EU European Implementation Assessment. *European Parliament Research Service.*

Shackelford, S.J. and Andres, R.B., (2010) State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Geo. J. Int'l L.*, *42*, p.971.

Stratton, G., Powell, A. and Cameron, R. (2017) Crime and justice in digital society: towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), pp.17-33.

Thakur, K., Ali, M.L., Jiang, N. and Qiu, M. (2016) April. Impact of cyber-attacks on critical infrastructure. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 183-186). IEEE.

Theocharidou, M. and Gritzalis, D. (2009) Situational Crime Prevention and Insider Threat: Countermeasures and Ethical Considerations. In *Proc. of the 8th International Computer Ethics Conference* (pp. 808-820).

Thomas, D. and Loader, B., (2000) Introduction – Cybercrime: Law enforcement, security and surveillance in the information age. In D. Thomas and B. Loader (eds) *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

TNS Opinion & Social (2012) Cyber Security Report: Euro barometer Special Surveys, Report 390. *European Union.* 1-45.

Ulsch, M. (2014) *Cyber threat!: how to manage the growing risk of cyber attacks*. John Wiley & Sons.

Vaxevanakis, K., Zahariadis, T. and Vogiatzis, N. (2003) A review on wireless home network technologies. *ACM SIGMOBILE Mobile Computing and Communications Review*, *7*(2), pp.59-68.

Vlachos, V., Minou, M., Assimakopouos, V. and Toska, A. (2011) The landscape of cybercrime in Greece. *Information Management & Computer Security*, *19*(2), pp.113-123.

Wikström, P.O.H. (2004) Crime as alternative: Towards a cross-level situational action theory of crime causation. *Beyond empiricism: Institutions and intentions in the study of crime*, *13*, pp.1-37.

Williams, M.L. and Levi, M. (2017) Cybercrime prevention. *Handbook of crime prevention and community safety*, *454*.

Yar, M. (2005) The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), pp.407-427.

Young, J. C., & Widom, C. S. (2014) Long-term effects of child abuse and neglect on emotion processing in adulthood. *International Journal of Child Abuse & Neglect, 38*(1), 1369-1381.