VARSTVOSLOVJE, Journal of Criminal Justice and Security
year 12
no. 4
pp. 378-396

Perception of Cyber Crime in Slovenia

Maja Dimc, Bojan Dobovšek

Purpose:

The purpose of this article is to present the results of the pilot research regarding the perception of cybercrime in Slovenia.

Design/Methodology/Approach:

The study focused on the research of the perception of cybercrime among the general public, as well as the members of the law enforcement agencies.

Findings:

The development of information and communication technologies critically influences all aspects of our lives, and consequently the characteristics of crime have adapted to the new form of operation in the virtual world. Cybercrime is the new way of breaking the law, and in order to implement successful preventive strategies it is of crucial importance to understand the perception of the general public, as well as the perception of the members of law enforcement agencies regarding cybercrime. The pilot study was performed on a smaller group of individuals (approximately half were the representatives of the general public, while the rest were the representatives of law enforcement agencies) in the form of in-depth interviews. The findings of the pilot research were alarming, since the majority of the interviewees greatly differentiate between certain forms of crime performed in the cyberspace as opposed to the same form of crime performed in real life i.e. the act of stealing, piracy in particular, is unacceptable in the real world and at the same time only natural in the virtual world. Furthermore, the pilot research displayed serious lack of awareness regarding different forms of cybercrime among the general public, as well as the members of law enforcement agencies, and consequently also poor understanding of legislation pertinent to cybercrime. Based on the results of the pilot research it is evident that it is of crucial importance to raise the awareness and understanding among the general public and increase the knowledge of the members of law enforcement agencies regarding cybercrime and its consequences in our everyday life.

Research limitations/implications:

The results are not generalizable due to the small group of interviewees. Consequently, future research will include a larger group of interviewees and will combine both in-depth interviews as well as questionnaires.

Practical implications:

The article represents a useful source of information for individuals working in this field as well as the general public. Furthermore, it represents the basis for further research of the field.

Originality/Value:

The article deals with the issue of the perception of cybercrime in Slovenia and exposes the critical issues related to the difference in the perception of a similar act of crime in the real life as opposed to the virtual world.

UDC: 343.3/.7:004(497.4)

Keywords: computer-related crime, cybercrime, information and communication technologies, Slovenia

1 INTRODUCTION

The development of information and communication technologies critically influences all aspects of our lives in both positive as well as negative ways. The internet has expanded at an average global rate of 380 % from 2000 to 2009, and has currently approximately 1.7 billion users (Schjolberg, 2010). Every day, the internet presents new opportunities for all fields imaginable, from business, research, education, law enforcement to entertainment and public discourse, it has become "a window to the world", surpassing the limitations of traditional boundaries of communication (Britz, 2009). However, the advantages of the internet have also presented boundless opportunities for illegal activities; namely traditional illegal activities have been "improved" and new forms of crime have emerged. Furthermore, the nature of cyberspace as that "place between places", international in scope and growing at a rapid pace contributed to the increased level of criminal behavior, which can be attributed to its virtual nature, namely the general public oftentimes perceives actions performed in the virtual world as merely virtual without considering the consequences in the real world (ibid.).

Furthermore, criminal activities performed in cyberspace are not bounded by the usual physical limitations and since location is of no importance, such criminal activities can be performed in different locations with different victims at the same time making the perpetrator almost impossible to uncover. The computer and the internet thus provide an additional "cloak of anonymity" to the perpetrators of such crimes and make criminal activities that much more appealing (Weber, 2006).

Cybercrime is a new way of breaking the law, and in order to implement successful preventive strategies it is of crucial importance to understand the perception of the general public, as well as the perception of the members of law enforcement agencies regarding cybercrime.

The presented pilot study was performed on a smaller group of individuals in the form of in-depth interviews. The findings of the pilot research were alarming on several levels, since the results not only displayed a serious lack of awareness regarding cybercrime, but also point to the fact that certain forms of illegal behavior have become socially acceptable when performed in the virtual world. Based on the results of the pilot research it is evident that it is of crucial importance to raise the awareness and understanding among the general public and increase

the knowledge of the members of law enforcement agencies regarding cybercrime and its consequences in our everyday life.

2 DEFINITION AND PERCEPTION OF CYBERCRIME

The phenomenon has to be defined in a broad manner in order to include the extensive diversity of criminal activities related to information communication technologies. Marjie T. Britz thus defines cybercrime as " abuses and misuses of computer systems or computers connected to the Internet, which result in direct and/or concomitant losses…criminal activity that has been facilitated via the Internet" (Britz, 2009).

UN Office on Drugs and Crime defines cybercrime as »conduct that entails the use of digital technologies in the commission of the offence; is directed at computing and communications technologies or involves the incidental use of computers with respect to the commission of other crimes« (UN Office on Drugs and Crime, 2005).

Understanding of the phenomenon influences consequent behavior; therefore, we attempted to gain an insight into the understanding and perception of cybercrime by the general public through our conversations with the interviewees.

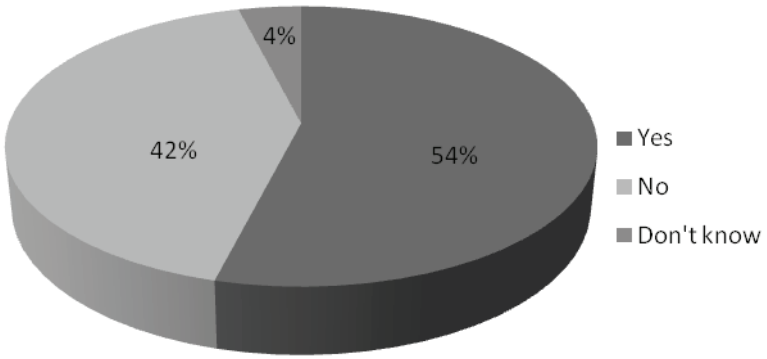
For the purposes of the presented pilot study we performed in-depth interviews on a smaller group of individuals; we attempted to gain an input from the representatives of the general public, as well as the representatives of law enforcement. Therefore, approximately half of the interviewees work in the field of law enforcement, while the other half are representatives of the general public. Age of interviewees ranges from 20 to 48 years for age, with an average age of 31 years. Educational level of the interviewees ranges from finished high school up to master degree; for the purpose of analysis we divided the educational level into two ranges, namely lower educational level which includes interviewees with completed high school degree (35 %) and higher educational level which includes interviewees with obtained undergraduate and graduate degree (65 %).

2.1 Definition and Understanding of Cybercrime

Cybercrime proved to be difficult to define as 23 % of the interviewees did not even attempt to define the term, 83 % of these with lower educational level. However, several interviewees proved to have a good understanding of the term with definitions such as "all illegal activities performed with the use of the internet" and "all illegal activities performed with the use of computer technologies".

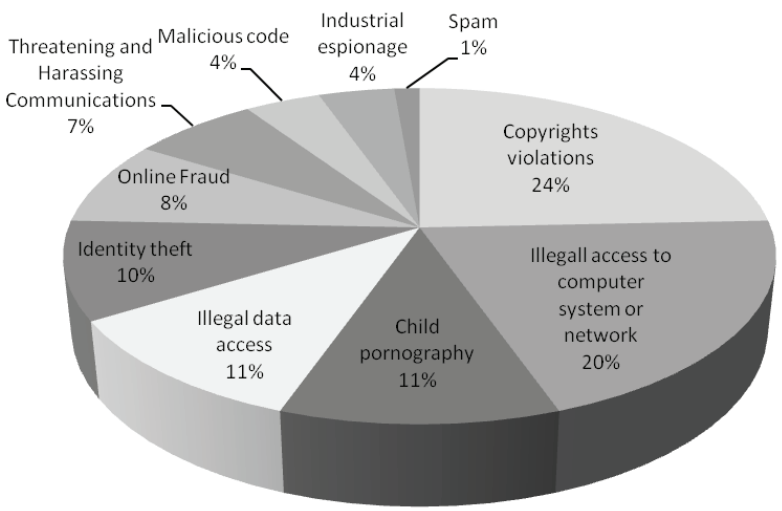
When it comes to the borderline between legal and illegal use of the internet, 27 % of the interviewees believed that the general public has a clear understanding of where legal use of the information communication technologies ends and illegal use begins. It is quite alarming that 65 % of the interviewees believed that the general public is not able to define this borderline, particularly due to the fact that 30 % of these interviewees work in the field of law enforcement. The remaining 8 %

of the interviewees believed that the definition of this borderline is not adequately clear in the eyes of the general public and is clearly understood only when related to a particular field, the interviewees pointed out the field of copyrights.



Graph 1: Is the borderline between legal and illegal use of the Internet clear?

The majority of the interviewees (54 %) believed that the perpetrators of cybercrime have to be extremely proficient in the field of information communication technologies; however, they also pointed out that the level of proficiency is dependent on the type of cybercrime (information system hacking requires a high level of proficiency as opposed to fraud or child pornography proliferation).



Graph 2: Types of cybercrime

The type of cybercrime the interviewees mentioned most often was the violation of copyrights (24 %). It is evident that the interviewees are aware of

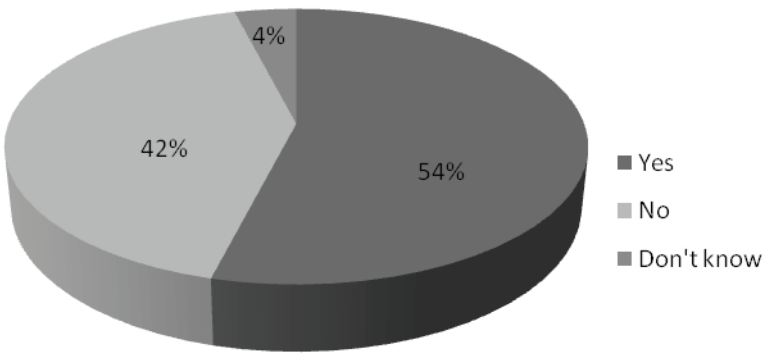
the illegal aspect of online piracy and the problems of copyright infringements, which is the reason why this type is stated most often. When discussing the issue of cybercrime, the image that most often stands out is the image of a hacker. Consequently, illegal access to computer system or network is in second place with 20 %. The interviewees mentioned illegal data access and child pornography in 11 % of their answers, closely followed by identity theft (10 %) and online fraud (8 %) in which case Nigerian letters were mentioned most often. It is quite interesting that spam was mentioned only in 1 % of the answers, which points to the fact that the interviewees do not perceive this type of activity as illegal.

2.2 Cybercrime Perceptions

The questionnaire continued with questions touching the issues related to general misconceptions of the activities that constitute cybercrime. Namely, we attempted to gain an insight into the actual perception of any form of cybercrime in the eyes of the interviewees. The first question "Have you ever committed any form of cybercrime?" laid the grounds for the consequent questions. We purposely chose the consequent questions to deal with more "simple" forms of cybercrime in order to analyze the perception of the borderline between legal and illegal activities and point out the general misconceptions.

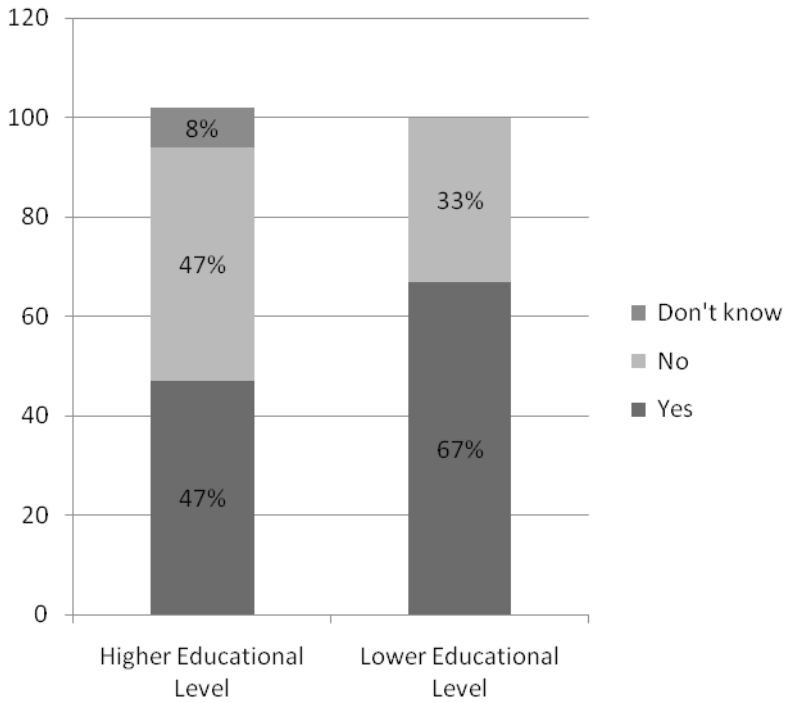
The majority of the interviewees (54 %) admitted to committing a certain type of cybercrime at some point in their life, 42 % of the interviewees stated they have never committed any type of cybercrime, and 4 % of the interviewees stated they do not know whether they have or have not committed cybercrime in the past.

Graph 3: Have you ever committed any form of cybercrime?



In order to obtain a closer look at the answers, we also analyzed the answers as they relate to the educational level of the interviewees and found that the percentage of the interviewees with higher educational level that committed cybercrime (47 %) was the same to the percentage of the interviewees that did not commit any form of cybercrime (47 %). However, in the case of the interviewees with lower educational level, the percentage of the interviewees that committed cybercrime in the past (67

%) was considerably higher than the percentage of the interviewees that have not committed any form of cybercrime (33 %).



Graph 4: Have you ever committed any form of cybercrime? (educational level)

Furthermore, we also reviewed the answers as they relate to the interviewee's field of operation; for this purpose we divided the interviewees into "general public" and "law enforcement officers". Among the affirmative answers, 64 % constituted the answers of the representatives of the general public, and 36 % constituted the answers of law enforcement officers. The fact that such a percentage of the persons whose professional life is dedicated to law enforcement is alarming to say the least and representative of the fact that cybercrime and its consequences are widely misunderstood and marginalized.

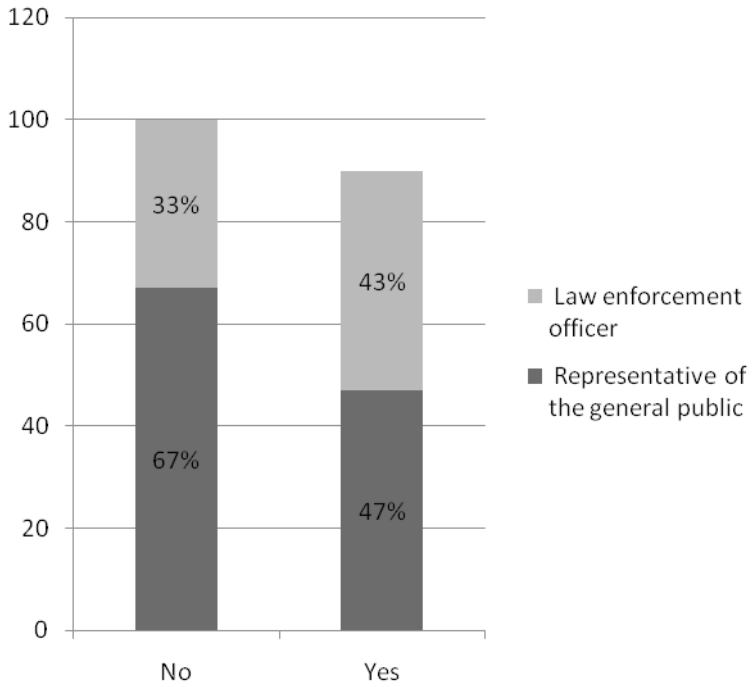
As mentioned previously, the interview continued with questions related to certain more widely accessible types of cybercrime, namely the types where the borderline between legal and illegal activities could easily be breached. The questions are inter-related; consequently, the analysis is performed on all questions as they relate to one another.

Only 28 % of the interviewees have purchased all the software currently installed on their computers. The majority of these interviewees also downloaded software from the internet; they either downloaded freeware or have paid for the particular software. However, 17 % of the interviewees stated that they have purchased all their software, and have also downloaded some software, but not

all of their downloaded software is freeware, which clearly points to the fact that they have lost the perception of property when it comes to property in electronic format.

An alarming percentage of the interviewees (72 %) have not purchased all their software or have downloaded software other than freeware and additionally alarming is the fact that 33 % of these were law enforcement officers.

Graph 5: Have you paid for all installed software other than freeware?

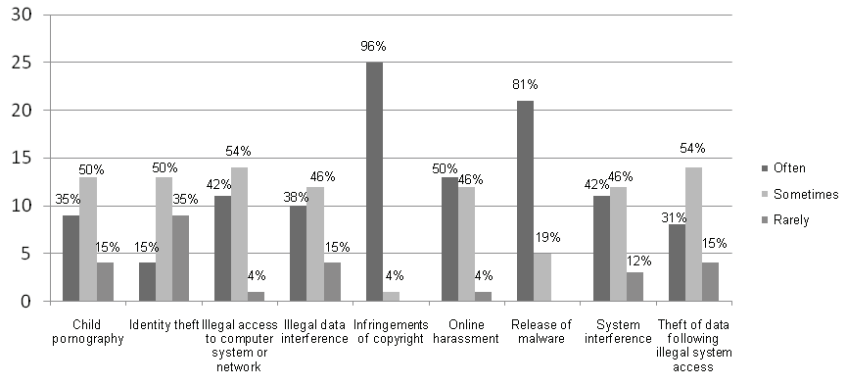


Furthermore, only 19 % of the interviewees purchased all the movies and music in their collections, which could point to the fact that the general public views the contents available on the internet to be "free of charge" or the property of everybody. Clearly, the perception of property in the electronic format greatly differentiates from the perception of property in the real world.

2.3 Perception Regarding Cybercrime Occurrence in Slovenia

Peception of the general public regarding the occurrence of a particular type of crime can have an important influence on the actions of the general public and can also result in a more proactive approach toward the fight against the particular type of crime. However, as we have seen, the general public has a slightly different attitude toward crime when performed in the virtual world.

The interviewees were asked to determine how often, or rarely, a particular type of cybercrime occurs in Slovenia.



Graph 6: Perception of cybercrime occurrence in Slovenia

The types of cybercrime that stand out are:

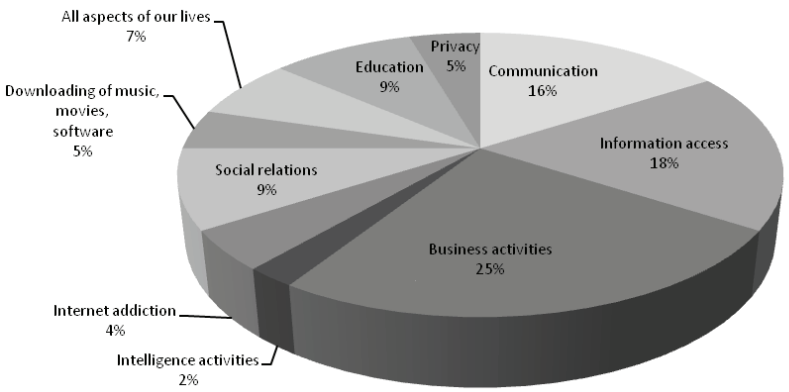
- infringements of copyright, since 96 % of the interviewees stated that this type of crime occurs often or very often. In retrospective, we find that this type of cybercrime was mentioned most often when the interviewees were asked to list a couple of types of cybercrime;
- release of malware, in this case 81 % of the interviewees belived that this type of cybercrime occurs often and 19 % belived that it occurs sometimes. It is interesting that only 4 % of interviewees previously mentioned this type of crime. However, we can attribute the high percentage to the fact that most likely the majority of the interviewees has had an encounter with one of the types of malicious code (computer virus, worm, trojan, etc.);
- online harassment, in this case 50 % of the interviewees believed that online harassment occurs often and 4 % belived that it occurs rarely;
- child pornography, in this case 35 % of the inteviewees belived it occurs often, while 50 % believed it occurs sometimes, and 15 % belived it occurs rarely. However, according to the statistical data the number of illegal activities related to the creation, dissemination and possession of child pornography has been continuously increasing in the past three years (Spletno oko, 2009).

Overall, we can conclude that the interviewees perceived the occurrence of any type of cybercrime to be on a regular basis. However, it is interesting that the occurrence of identity theft has been identified by the majority of the interviewees to occur only sometimes or even rarely, despite several larger identity theft cases in the last year. It is possible that the interviewees do not have a clear understanding of what constitutes identity theft and this issue would undoubtedly be interesting to include in future research.

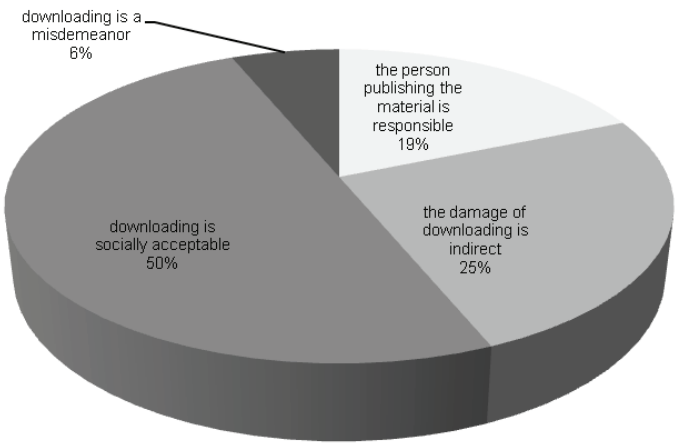
3 INFORMATION SOCIETY - CONSEQUENCES

All of the interviewees agreed that the development of information communication technologies critically influences our lives and 7 % of the interviewees were convinced that these influences spread throughout all aspects of our lives. Business activities, the development of e-business in particular, were pointed out in 25 % of the cases, followed by easier and faster information access (18 %), and easier and faster communication (16 %) due to the development of online telephony. It is interesting that only 5 % of the interviewees mentioned the field of privacy, which might display the fact that the general public is either not aware of the influence of the development of information communication technologies on the level of our privacy or that privacy is perceived differently when in the virtual world. In either case, the issue will undoubtedly be included in further research.

Graph 7: Development of ICT - fields of influence



Due to the fact that contemporary communication is largely performed in the virtual world, we decided to include a question regarding net ethics, rules of behavior in the virtual world, and found that 50 % of the interviewees were familiar with the term. However, only 54 % of these interviewees respect the rules of net ethics, 31 % occasionally respect these rules, and 15 % of the interviewees do not respect the rules of net ethics even though they are familiar with them. Since the other 50 % of the interviewees have never even heard of the term, we can conclude that the majority of online communication does not follow the rules of net ethics.



Graph 8: Difference between downloading and stealing

In the attempt to touch on the issue of the borderline between legal and illegal online activities, we included a question regarding the difference between stealing a movie in a store and illegal movie downloading. The majority of the interviewees (65 %) believed that there is a major difference and the reason stated most often is the fact that downloading is socially acceptable. Interesting is also the perception that the responsibility lies in the person publishing the material, namely the person that made the material available, which was stated by 19 % of the interviewees.

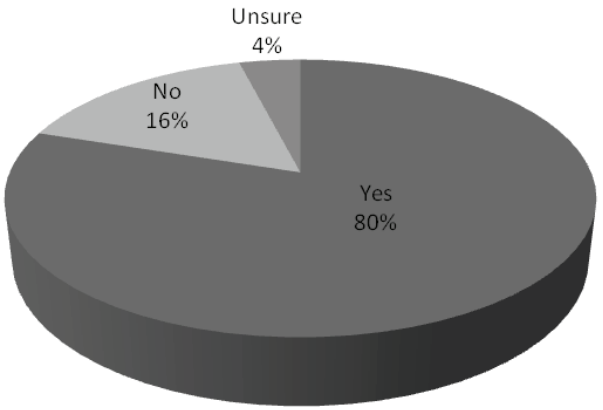
4 CYBERSPACE – SAFETY AND SECURITY

Due to the fact that we spend an increasingly larger amount of our lives in cyberspace, it is important to touch on the issues of the perception of safety and security. The amount of time spent on the internet per day was divided into four groups and 76 % of the interviewees stated that they spend up to 3 hours per day on the internet, 12 % of the interviewees spend from 3 to 6 hours, 8 % 6 to 10 hours, and 4 % 10 to 12 hours. It should be pointed out that the last two groups consisted of the individuals whose professional career includes online work resulting in the high online access numbers.

4.1 Perception of Safety and Understanding of Security Measures

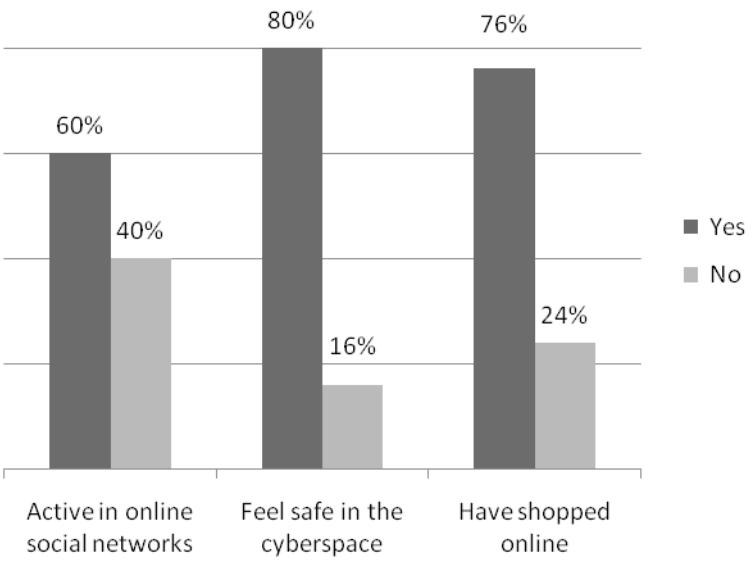
Despite the increasing number of cybercrime cases all over the world and also in Slovenia, the majority of interviewees (80 %) stated that they feel safe in the cyberspace.

Graph 9: Do you feel safe in the cyberspace?



An important indicator of the perception of safety during online activities is the percentage of people engaging in online shopping; 76 % of the interviewees stated to have had shopped online, which corresponds to the large percentage of interviewees believing in the safety of online activities. However, it is interesting that all of the interviewees who stated that they do not feel safe in the cyberspace have, despite this negative feeling, performed online purchases, and additionally, 75 % of these interviewees spend over 3 hours per day in the cyberspace.

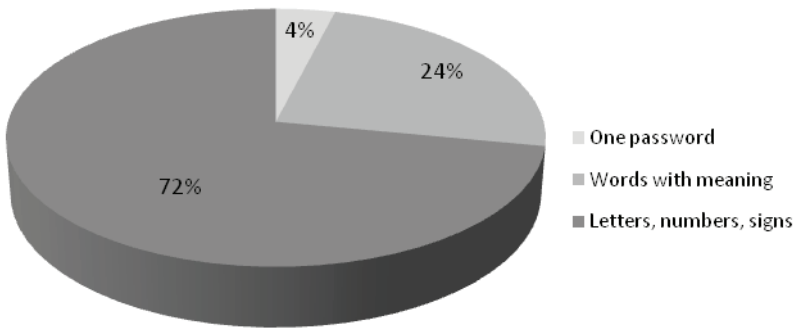
Graph 10: The feeling of safety in the cyberspace



Furthermore, 60 % of the interviewees are active in online social networks such as facebook, twitter, netlog, myspace etc. and 20 % of these are actually

the interviewees that expressed the opinion that they do not feel safe online. Furthermore, among the interviewees that participate in online social networks, 26 % of the interviewees participate in two or more different social networks. Interesting is also the fact that 93 % of the interviewees who participate in online social networks use their actual name as opposed to using a nickname, which again corresponds with the fact that 80 % of the interviewees feel safe in the cyberspace.

In addition to the question regarding the feeling of safety we touched the issue of security, namely we focused on the question of how individuals protect themselves during their online activities. We were particularly interested in the way the interviewees create their password, how often they change it and the manner in which they protect their computer system. We found that 4 % of the interviewees use only one password for all of their online activities, 24 % of the interviewees use words with meaning, and the remaining 72 % of the interviewees use a combination of letters, numbers and occasionally signs to create their passwords.



Graph 11: How do you create your passwords?

Furthermore, a third of the interviewees change their password on a regular basis and all of them belong to the group of interviewees with the safest manner of creating password (combination of letters, number, signs). The second third of the interviewees only rarely change their passwords and the last third of the interviewees never change their password.

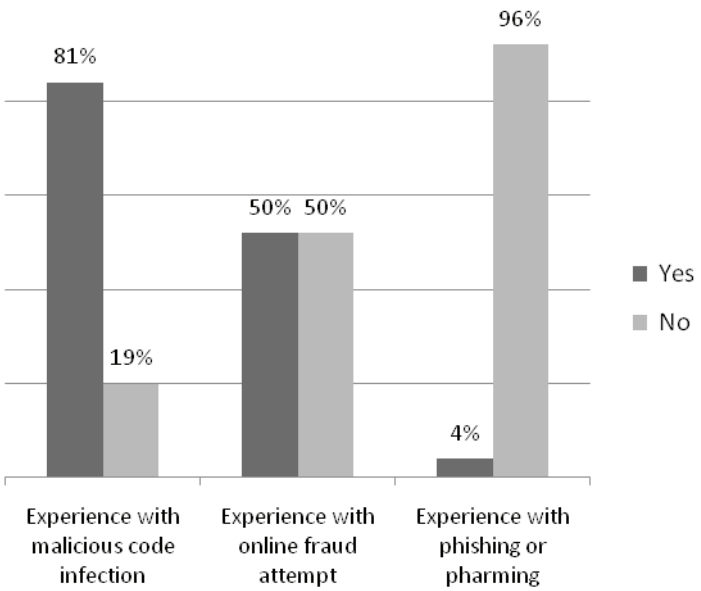
In relation to assuring the safety and security of their computer systems, the large majority of the interviewees are taking at least some steps to protect themselves from illegal access attempts and other types of misuse of devices and only 8 % of the interviewees are not protecting their computer system at all.

4.2 Cybercrime Experiences

The majority of the interviewees (81 %) have had an experience with cybercrime, and generally these experiences are related to encounters with malicious programming code infecting their computer systems. Furthermore, 50 % of the interviewees have had an experience with an attempt of online fraud; the majority of these attempts

where the classical attempts of funds transfer fraud (Nigerian letters, etc.) either soliciting via e-mail or pop-up windows. The majority of the interviewees (88 %) have never had an experience with phishing or pharming; however, only 22 % of these interviewees are actually familiar with the terms phishing and pharming and were able to correctly define them.

Graph 12: Cybercrime Experiences



Almost all interviewees, with the exception of one, were lucky during their activities online, and despite the fact that they have had encounters with cybercrime, they never experienced any monetary loses, which might contribute to their feeling of safety while online.

5 LEGISLATION, PREVENTION AND PROSECUTION

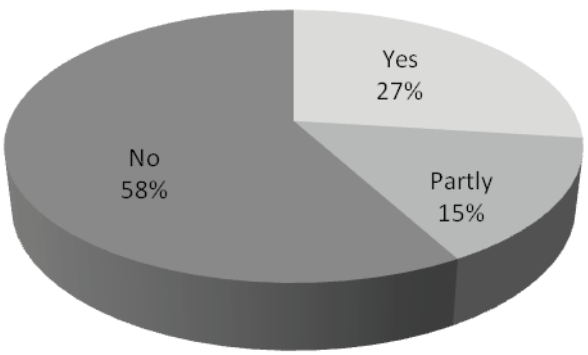
The Council of Europe adopted the Convention on Cybercrime in 2001 (Council of Europe, 2001); it was ratified by the majority of the European countries by 2004. Convention on Cybercrime represents the cornerstone of European cooperation in the field of cybercrime, and is dedicated to creating common legislation in all countries of the EU and other countries that ratified this convention. In 2003 the additional protocol to the convention on cybercrime was adopted dealing with the criminalization of acts of racist and xenophobic nature committed through the computer systems.

Slovenia signed the Convention in June of 2002. Consequently, the Law on the ratification of Convention in Cybercrime and additional protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic

nature committed through computer systems was adopted in 2004, thus integrating the convention in the Slovenian legislation.

5.1 Understanding of Legislation Related to Cybercrime

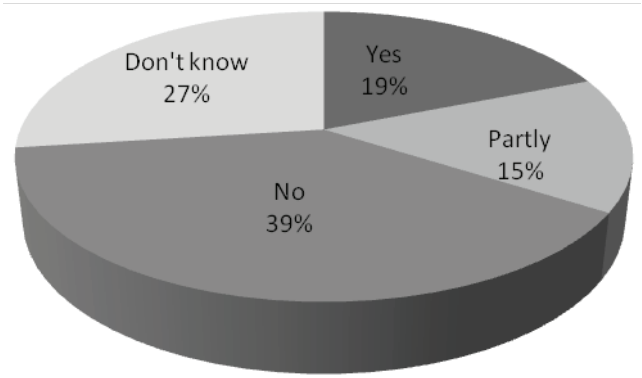
The percentage of the interviewees that are at least somewhat familiar with the legislation related to cybercrime constitutes only 27 % of the interviewees and 71 % of them were law enforcement officers. A partial understanding of the legislation related to cybercrime was expressed by 15 % of the interviewees. The majority of the interviewees (58 %) are not familiar with the legislation in the field of cybercrime. Consequently, the largest amount of the interviewees did not know whether the legislation in this field is appropriate.



Graph 13: Are you familiar with legislation in the field of cybercrime?

36 % of the interviewees that are at least somewhat familiar with the legislation in the field of cybercrime stated that the legislation in this field is appropriate, 19 % stated that it is partially appropriate and that some changes would be necessary particularly in the field of prosecution, 27 % of the interviewees believed that the legislation is not appropriate and 18 % of the interviewees admitted that their familiarity with the legislation in this field is not extensive enough to be able to make a decision.

Graph 14: Are law enforcement representatives appropriately trained?

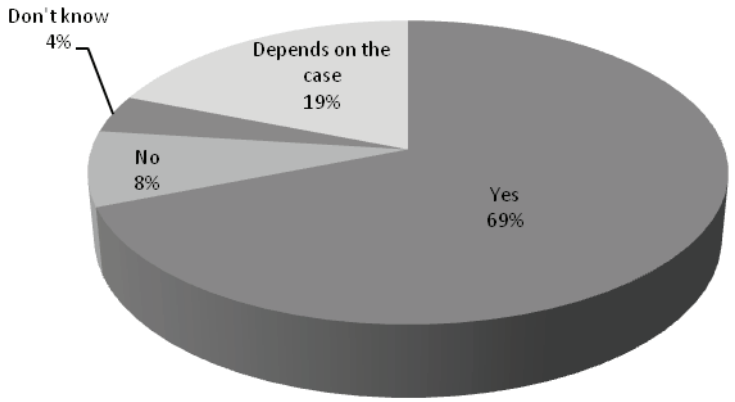


With regard to the level of expertise of the law enforcement officers working in this field, the majority of the interviewees (39 %) believe their level of expertise is not sufficient. On the other hand 19 % of the interviewees believed that they are appropriately trained, but the problem lies in their numbers as there are, according to certain interviewees, too few of such experts working in the public sector, and 15 % of the interviewees stated that in their opinion the law enforcement officers working in this field are not appropriately trained to "keep up with the cybercriminals". The remaining 27 % of the interviewees could not determinate whether the level of expertise is appropriate or not.

5.2 Understanding of Prosecution Process

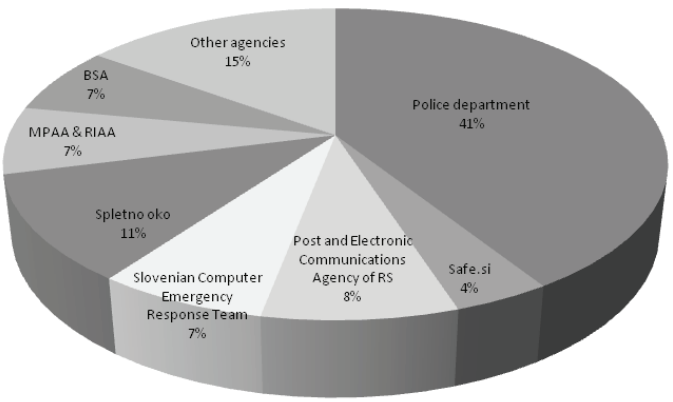
In order to gain an insight into the understanding of the interviewees regarding the prosecution process we discussed with the interviewees the actions they would take in case of an encounter with cybercrime. The majority of the interviewees (69 %) would immediately report an encounter with cybercrime.

Graph 15: Would you report an encounter with cybercrime?



The interviewees that would report cybercrime encounters, would report the case to appropriate law enforcement agencies (94 %), human rights ombudsman (4 %), and, in case of a more serious type of cybercrime, also the media (2 %). A group of interviewees (19 %) stated that they would report an encounter with cybercrime depending on the type and seriousness of cybercrime experience; these interviewees would also report the case to law enforcement agencies, the information commissioner, and some of them would also contact computer forensics and market inspectorate of RS. It is interesting that 50 % of the interviewees that would not report an encounter with cybercrime would do so, because they do not know who they could report it to. Furthermore, these interviewees would not take any other actions to protect themselves in the future.

The majority of the interviewees (62 %) were able to state at least one organization that deals with the issue of cybercrime; however, several of these interviewees only stated the police department.



Graph 16: Agencies in the field of cybercrime

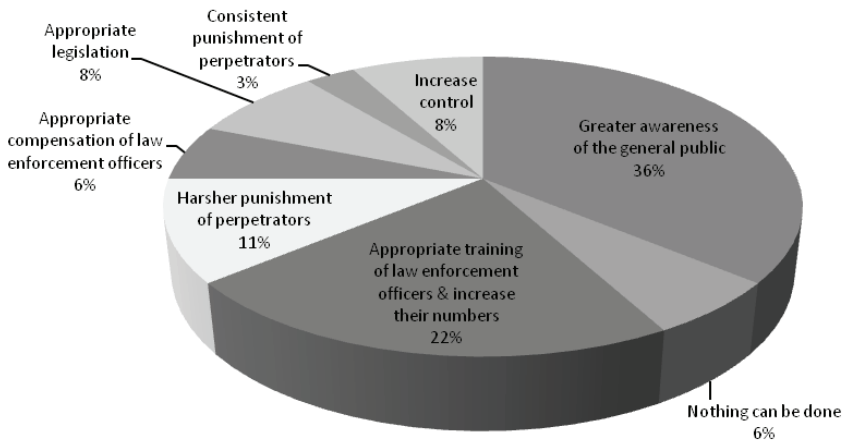
According to the answers of the interviewees, we can safely assume that their awareness regarding the agencies operating in the field of cybercrime is seriously lacking. The interviewees that have heard of the agencies dealing with different types of cybercrime were able to define the type of crime they would report to a specific agency (for example SI-CERT Slovenia Computer Emergency Response Team for illegal system access, Spletno oko for cases of child pornography and hate speech, etc.); however they represent only approximately 10 % of all interviewees, which is a reason for concern as it points out the low level of awareness.

5.3 Reflections Regarding Prevention

Among the necessary steps that would aid in the prevention of the increase of cybercrime cases, the majority of the interviewees (36 %) stated that increasing the

level of awareness of the general public is of the utmost importance. As the analysis of this pilot research displayed, the general public seems to be acutely unaware not only of the different types of cybercrime they could inadvertently be exposed to, but also of the actions they should take or agencies they should contact in case they become a victim of a cybercrime perpetrator.

Graph 17: Necessary steps to prevent the increase of cybercrime cases



Furthermore, several interviewees (22 %) pointed out the necessity of providing appropriate training of the law enforcement officers working in the field of cybercrime and the fact that their numbers should be increased. This statement links with the opinion that monetary compensation of professionals working for the government in the field of cybercrime should be increased (6 %). In order for a professional to be successful in any area of information and communication technologies, it is of imperative importance that such a professional is continuously increasing his/her knowledge. Professionals working in the field of cybercrime must have a combination of technical and also legal expertise, consequently the demand for such employees is also high in the business sector; the compensation in the public sector, unfortunately, oftentimes cannot compete.

The majority of the interviewees (73 %) also expressed the opinion that the role of law enforcement agencies is crucial for successful prevention and protection against cybercrime; however, some of the interviewees compare it with the "Don Quixote's battle with windmills", since they believe that the perpetrators are always "a step ahead of the investigators" due to their greater knowledge and experience. Furthermore, some of the interviewees believed that law enforcement agencies should be more interconnected both nationally and internationally.

6 CONCLUSION

Information communication technologies are an important part of our lives, influencing the way we study, work, communicate, socialize; however, with all the advantages, naturally, come the disadvantages. The extent of personal information individuals exchange and publish on the Internet is increasing rapidly, particularly with the increasing popularity of social networks. Consequently, the level of privacy has significantly decreased and is at an all time low, we could conclude that we live in a society of control, since control in the contemporary information society is "not merely visual, it has transferred to the world of the digital signal" (Kovačič, 2003). The possibilities offered by easier data access, smooth communications, and effective control are increasingly more often abused by the perpetrators of cybercrime. The awareness of the general public is of crucial importance for successful prevention and protection against cybercrime and therefore, the pilot study attempted to gain an insight into the perceptions and reflections of the interviewees regarding cybercrime and its consequences. The findings are alarming, since they point to the fact that certain types of cybercrime are so widely performed that they have become socially acceptable (i.e. piracy). In general, we could conclude that traditional crime has been desensitized when performed in the virtual world and individuals are oftentimes not aware of the real-life consequences. However, encouraging is the fact that a large majority of the interviewees would report an encounter with cybercrime, despite the fact that many of them believe law enforcement officers are not appropriately trained in this field, which, nevertheless, displays a certain level of trust in the law enforcement agencies. The results of the pilot research displayed that both, the general public and the members of law enforcement agencies are not familiar with different forms of cybercrime and are, additionally, not familiar with the legislation dealing with the field of cybercrime. Based on the results of the pilot research it is evident that it is of crucial importance to raise the awareness and understanding among the general public and increase the knowledge of the members of law enforcement agencies regarding cybercrime and its consequences in our everyday life. In order to further research the understanding and perception of the field of cybercrime in Slovenia, a more extensive research will be performed in the future.

REFERENCES

Britz, M. T. (2009). *Computer Forensics and Cyber Crime*. New Jersey: Pearson Education.

Council of Europe. (2001). *Convention on Cybercrime.* Retrieved September 01, 2010, from http://conventions.coe.int/Treaty/en/Treaties/html/185.htm

Kovačič, M. (2003). *Privacy and the Internet*. Ljubljana: Mirovni inštitut, Inštitut za sodobne mirovne in politične študije.

Schjolberg, S. (2010). *A Cyberspace Treaty: a United Nations Convention or Protocol on Cybersecurity and Cybercrime*. Retrieved August 10, 2010, from http://www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf

Spletno oko. (2009). *Najtemnejša plat interneta: otroška pornografija.* Retrieved September 01, 2010 from http://www.spletnooko.si/index.php?fl=1&nt=9&offset=21&m2w=Novice&sid=66

UN Office on Drugs and Crime. (2005). *The Eleventh United Nations Congress on Crime Prevention and Criminal Justice.* Retrieved August 12, 2010, from http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf

Weber, J. (2006). *The Cloak of Anonymity.* Retrieved October 28, 2010, from http://business.timesonline.co.uk/tol/business/industry_sectors/media/article709214.ece

About the Authors:

Maja Dimc, M.Sc., in addition to working as an IT analyst at the Ministry of Defense of RS, Maja Dimc is also teaching Business Information Systems at the International School for Social and Business Studies, and Cybercrime at the University of Maribor, Faculty of Criminal Justice and Security. Contact info: maja.dimc@gmail.com.

Bojan Dobovšek, Ph.D., Vice Dean and Associate Professor of Criminal Investigation at the University of Maribor, Faculty of Criminal Justice and Security. Bojan Dobovšek received his PhD in political sciences from the Faculty of Social Sciences of the University of Ljubljana. His areas of research are organized crime and corruption. Contact info: bojan.dobovsek@fvv.uni-mb.si.