LOOK
ACADEMIC PUBLISHERS
OPEN ACCESS

IEJME — MATHEMATICS EDUCATION
2016, VOL. 11, NO. 5, 1127-1134
Article number: mathedu.2016.0100

Criminological Analysis of Determinants of Cybercrime Technologies

Lola F. Tatarinova[a], Karimzhan N. Shakirov[b] and Danila V. Tatarinov[b]

[a]"Turan" University, KAZAKHSTAN; [b]Al-Farabi Kazakh National University, KAZAKHSTAN.

ABSTRACT

An important task, the government, particularly law enforcement officers and scientists, faces in the rapid development of information technologies, is to prevent crimes committed with their application. Comprehensive analysis of the criminological characteristics of computer crimes, which is the aim of this study, provides an opportunity to identify the motives of these crimes to determine the most effective ways to eliminate them, as well as to work out the best ways and investigation means of criminal cases in this category. One of the fundamental structural elements of the national security of any state in the period of cyberspace development is to protect all information resources and communication networks against criminal assault. A complete analysis of computer crimes requires the understanding of motivation of illegal intrusion into information systems in order to obtain the information, stored in them, as well as using the opportunities provided by these systems or disabling the whole system or its components. The statement above is confirmed by the global use of computer technologies, information and communication networks.

KEYWORDS
Criminology; cyber security; information technologies; cryptography; criminological methods

ARTICLE HISTORY
Received 15 September 2015
Revised 10 November 2015
Accepted 22 February 2016

Introduction

Cybersecurity is possible through the methods of criminology.

The innovation of the article is an attempt to adapt the methods of criminological analysis to cyberspace. K. Driscoll (2016) notes, that cyberspace is an integral part of the encrypted system. Thus, the knowledge of cryptography helps to identify and prevent cybercrimes.

An important tool for protection against computer crimes is cyberhygiene – the improvement of the Internet culture, an integral part of which is the possession of the complex procedures applied by cybercriminals. Many works are written on the “phishing” methodology (Murashbekov, 2015, Leukfeldt, 2015a, Leukfeldt, 2015b,

CORRESPONDENCE Danila V. Tatarinova ✉ danila_tatarinov@mail.ru

Leukfeldt, Kleemans & Stol, 2016), but much smaller number of works is devoted to the development of an adequate level of cyberculture (Cross, 2016), which should be developed from an early age.

Moreover, the analysis of the situation shows that the growth of computer crime is partly due to the increasing number of professional users (Murashbekov, 2015).

It is important to note that the development of mechanisms for the protection of computer, information and communication networks will be more effective at the international level than at the local, as this type of crime is transnational.

The data results on committing cybercrimes are visualized in diagrams in Figures 1 and 2.

The topicality of this article is due to the expansion tendency of the global network. By the time the Internet covers the entire planet, it will be necessary to master the complex of cybercrime prevention measures.

The practical value of this paper is in the proposed method of reducing the number of cybercrimes by improving the skills of criminology.

This paper makes a significant contribution to the world of science, as it indicates the actual problems, caused by the current globalist tendencies.

Purpose of the Study

The purpose of this study is to identify the criminological specificities of cyberspace crime.

Research Questions

The objectives of the study include:

- establishing the boundaries for cybercrimes;
- transfer of the means of cyberspace protection;
- cybercrime visualization, comparative and quantitative analysis;
- determining the criminological issues in cyberspace.

Methods

The methodological basis includes complex comparative analysis, statistical data analysis in the field of cybercrime, as well as an interdisciplinary analysis.

In addition, the research specifics are based on the criminological methods, such as studying documents and observation.

Results

The identification of criminological specifics of cyberspace crime helps to prevent crimes in the sphere of information technologies.

Establishing boundaries for cybercrimes bases both on the information space and the nature of the offense, clearly identifiable as such offline. This study determined the basic ways of cyberspace protection, which lie within the area of cryptography, the basics of which are necessary for the IT-specialists, interested in solving cybercrimes.

The study carried out a quantitative and comparative analysis of cybercrimes, the visual results of which are shown in Figures 1 and 2. It should be noted that the motives of financial crimes are easy to determine, while determining the motives of online crimes against human rights and freedoms applies the same principles, as offline. Similar data were obtained based on the materials on Figure 2, which reveals gaps in the criminological knowledge of experts, because a third of cybercrime was found accidentally. In further studies, it is necessary to develop a set of measures to increase the competence of IT-forensics.

Moreover, determining criminological issues in cyberspace was carried out based on the qualitative criteria, such as specific areas in which a civil cybercrime (material or non-material) was committed.

Discussions and Conclusion

This part of the study includes the analysis of the cybercrimes, which are divided into the crimes against personal rights (such as harassment and lack of privacy of writing), crimes against financial security (unsafe e-payment) and crimes against the children's morality (bullying).

First of all, there is a list of points that makes the exploitation of the Internet safer, bonded with the cryptography. K. Driscoll (2016) systematically assures that there are some crypto key-management issues:

- (Inter) national cryptography laws – export, import, use, key management
- Two aspects of key-management – trust: whom do you trust? with what? to do what? logistics: Mechanisms to enforce the trust
- Creation of keys and their ownership/association,
- Key distribution and management,
- Allowing only the authorized users for a set time;
- Handling revocations;
- Distribution needs protection for private and secret keys, even if these keys are only used for authentication; popular authentication schemes need secret keys;
- Ordinary use,
- Extraordinary use,
- The need to access the encrypted "plaintext" – the main reason for the easiest and the most common method is to give government access to the keys (but still it can greatly complicate the key distribution and management),
- Just "use the X. SOg-based public key infrastructure (PKI)", but: full PKI is heavyweight and does not solve all the problems by itself.
- Mitigating most of these issues for avionics – no secrets are stored on aircraft, which simplifies the airborne side of link.

The way in which young people have integrated online and digital technology into their personal relationships and sexual development is an important emerging issue for researchers and policymakers. Over the past few years, news media in Australia, North America and other Western countries have reported their concern on the cases of sexting, where minors have used the digital cameras on mobile phones to take and distribute sexual images of themselves and/or others, in some cases falling foul of child abuse or child pornography laws (Lee, 2013).

S. Hopkins & J. Ostini (2015) rethink the relationships between technology and violence, as it must spread feminist theories in digital cultures and the problems of gender, sex and power online. Cybersafety campaigns tend to locate the problem with the victim rather than the perpetrator, assuming that in cyberspace, as in the physical world, women are responsible for reducing the risk of being attacked (rather than revealing the power relations that create the domestic and sexual violence in the first place).

According to M.K. Musa (2015), the borderless nature of Internet and its easy access to cyberspace has provided a low-cost but high-connectivity ways for criminals to reach victims. This resulted in a rise of crimes which make use of the Internet as a medium, such as frauds, child sexual exploitations and cyber stalking. Cyber stalking has been labelled to be the crime of the nineties, due to its nature, which uses the latest technological telecommunications as a mean to perpetrate such act. Cyber stalking, similarly to stalking, involves threatening or harassing behaviours by one individual against another, with the exception that this particular act makes full use of the Internet. It contradicts the D. Clairmont & K. Waters (2015) search, including Nova Scotia's position that regularly deals with sexual harassment cases.

Thus, lack of cybersecurity intervenes into personal life and has serious consequences. These illegal actions, in turn, can cause the disruption of critical infrastructure elements' work in any state and result in deaths, property damage or other socially dangerous consequences.

Given the current predictions about the increase in computer crime through IT, the degree of their high latency, as a result of which the investigation and solution of crimes in this area is often carried out long after the commission, it is worth noting, that it is necessary to develop the international standards for protecting information about messages, transmitted through the global information and communication networks.

However, there is an example, studied by C. Angus (2016), C. Chalmers et al. (2016), H. Al-Alosi (2016), where Australian police eliminates cyberbullying with the help of a school and its social elements.

Moreover, researches on media-cyberbullying (Arntfield, 2015) have consistently overlooked the role of victims in online offending, as well as the victim behavior. The M. Arntfield's (2015) study provides an interdisciplinary review of existing researches and proposes a new basis for cybervictimology – the traditional victimology in the context of cyber activities. One of the main criteria of "traditional" bullying is its repetition, so the routine activities of victims in social media environments are key facilitators in the bullying process; they serve as advanced indicators of victimization in a space where anti-social behavior is comparatively tolerated by the absence of suitable guardianship. M. Hughes (2015) conceives that the national plan can partly liquidate the cyberbullying.

M. Williams & O. Pearson (2016) note that a national media campaign on legal protection, available to the victims of cyber-hate, should be launched during the hate crime awareness week. This part of battle is also noticed by D. Cross (2016).

E.R. Leukfeldt, E.R. Kleemans & W.P. Stol (2016) assumes that social ties still play an important role in the origin and growth of the majority of networks. Forums, however, also play a significant role in a number of networks, for example, to find suitable co-offenders or to get into contact with enablers. Criminals with access to forums are able to increase criminal capabilities of their network relatively quickly. Forums would seem to make it easier for loners or small groups to find suitable co-offenders and, potentially, to allow such networks to grow quickly. Forums are also used to acquire knowledge and skills. In the digital era, forums are replacing prisons as the 'university for cybercriminals'. Loners experimenting out of curiosity with all sorts of legal or illegal technical tools can end up in criminal networks through forums. More insight is therefore needed into what prompts individual criminals to become active on forums.

Increasing knowledge about these elements will ensure that we are able to better understand what cybercriminal networks are really like, and what countermeasures can be taken. This is not only of academic interest; it also provides law enforcement with an insight into which counter-strategies work best. It goes without saying that an international network of experts will offer different opportunities and challenges for law enforcement agencies than locally rooted networks of criminal all-rounders (Leukfeldt, 2015a).

Researchers (2015b) also compare (low-tech) phishing attacks and (high-tech) malware attacks. Both types of attacks have, for example, almost the same crime script. Furthermore, both groups of criminals are happy with anything they can get and do not discriminate between the rich and poor. There are also differences.

Firstly, regarding the effect of online visibility, almost none of the variables had any effect on phishing victimization.

The victims of malwares, however, tell a different story. There is a clear connection between spending time online and victimization. There are two types of activities, which ensure a higher chance of becoming a victim, namely downloading and online gaming. The second difference can be found within online accessibility. Again, none of the variables mattered when it came to phishing. The malware analysis, however, shows that users with certain (popular and widely used) operating systems and web browsers do have an increased risk of victimization.

M. Alazab & R. Broadhurst (2015) guess that spam pose a global challenge because this remains a major vector for the dissemination of malfare. It can also be the initial contact point for cybercriminals, such as the operators of a fraudulent scheme, who use emails to contact and solicit prospective victims for money (as in advance see frauds) or to commit identity theft by deceiving recipients of such mail into sharing personal, bank, and financial account information.

J. Kerstens and J. Jansen's (2016) findings demonstrate that the overlap between financial cybercrime victimization and perpetration is partially explained by retaliation, low self-control and on-line disinhibition, suggesting that state-dependency and individual heterogeneity explanations should be supplemented by explanations funded in the dynamics of the on-line environment.

Accounting that the above international regulations on cybercrime are rather contradictory including contradictions in determination of cybercrime, it may cause criminal liability avoidance only due to the state where a cybercrime was committed and the state where the guilty person was apprehended are oriented at different international treaties on cybercrime (including growing significance of mobile devices as the main means of Internet access may cause wider use of those devices by criminals), conceives O.B. Murashbekov (2015).

According to R. Taivo (2015), social networking refers to the use of the Internet to connect with people generally and build a network of friends, professional colleagues, business associates, and so forth. Obviously, wideness of communicative elements involves wideness of potential cybervictims. A.C. Moise (2015) lists these spheres as Government information networks, telecommunication networks, navigation systems for maritime and air transport, water control systems, energetic systems, financial systems, or other functions of vital importance for the society.

But the solution to this problem is not so simple, as the development of common standards for new areas is made difficult by technical differences, existing between states with both fundamental and applied nature.

Based on the analysis, authors present a diagram (Figure 1), showing the main types of computer crimes.

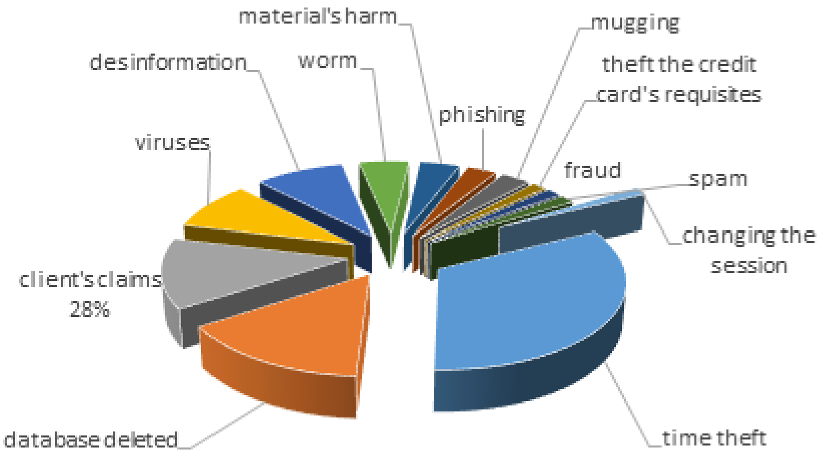

Figure 1. The main computer's crimes

Another factor, influencing the increase in criminality of the crimes in question, is the existence of legal, legislative and enforcement issues in the field of prevention and fight against crimes in the sphere of computer technologies.

The significant determinants of computer crimes are the gaps in the activities of inquiry and preliminary investigation. This is due to the lack of law enforcement professionals competent in the field of computer technology, as well as the rapid development of the latter, which often are expensive to purchase with the state budget, as opposed to the opportunities of criminal organizations.

However, computer crimes are still recorded, as mostly they are found in the investigation of other crimes. Figure 2 below shows which cases often reveal computer-related crimes.

Thus, the results of this study are quite controversial, as even a society that has come to the legislative regulation of cybercrime, according to D. Clairmont & K. Waters (2015), tends to excuse certain types of civil rights violation (as harassment and sexting), due to the inability to determine them in cyberspace. Perhaps this is partly due to the complexity of determining of the fact of the crime.

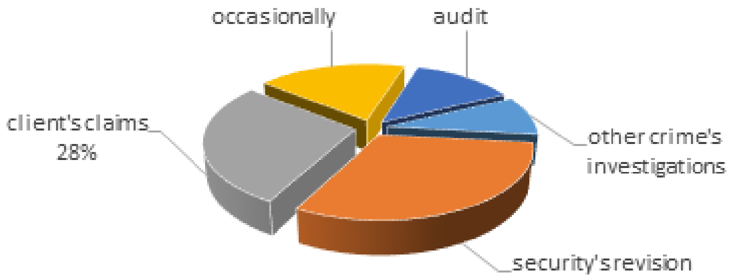

Figure 2. Computer crimes' revealing

This study takes an important place in the structure of human knowledge, as it contains the results of a multidisciplinary analysis, at the moment not conducted thoroughly in any related disciplines.

Implications and Recommendations

The scientific value of the article is a comprehensive analysis of possible cooperation between criminology and cybersecurity.

This study opens up the possibility of studying the multidimensional issues of cybersecurity and further liability for committing cybercrime. Practical application of the article may be implemented in the revision of the liability as a result of the cybercrime commission or and implementation into legislation.

The analysis of the causes for the emergence and development of crime in the field of computer technology and computer information leads to the following conclusion: the cross-border nature of the global information and communication networks allows computer criminals to bypass existing state borders, increasing the activity of international organized criminal groups.

Therefore, it is necessary to reinforce in the consciousness of the whole society the existing aspects of computer crime (improving cyberculture), as well as the rapid personnel policy expansion of law enforcement bodies, aimed at improving the level of expertise among employees, involved in the investigation of cases, related to computer crimes.

The stated complex of measures to be implemented at the state level will not only consider the causes and conditions of committing computer crimes, but also take conceptual measures for their prevention and elimination.

The benefits of the proposed investigation method are based on combining methods of one sphere (Criminology) with other spheres (cyberspace), allowing to accurately describe the surrounding reality and to prevent the appearance of crimes in cyberspace.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Lola F. Tatarinova is PhD, Associate professor of Department of Jurisprudence and International Law, "Turan" University, Almaty, Kazakhstan.

Karimzhan N. Shakirov is Doctor of Jurisprudence, Professor of International Law, Al-Farabi Kazakh National University, Almaty, Kazakhstan.

Danila V. Tatarinov is PhD, Associate professor of International Law, Al-Farabi Kazakh National University, Almaty, Kazakhstan.

References

Al-Alosi, H. (2016) The role of bystanders in cyberbullying. *Precedent NSW Conference in the Sydney, 132,* 20-24.

Alazab, M. & Broadhurst, R. (2015) The Role of Spam in Cybercrime: Data from the Australian Cybercrime Pilot Observatory. *Cybercrime Risks and Responses. Palgrave Macmillan*, 103-120.

Angus, C. (2016) Cyberbullying of children. *Parliament of NSW Government,* 1-22.

Arntfield, M. (2015) Toward a Cybervictimology: Cyberbullying, Routine Activities Theory, and the Anti-Sociality of Social Media. *Canadian Journal of Communication, 40(3),* 138-144.

Chalmers, C., Campbell, M., Spears, B., Butler, D., Cross, D., Slee, P. & Kift, S. (2016) School policies on bullying and cyberbullying: perspectives across three Australian states. *Educational Research, 58,* 91-92.

Clairmont, D., & Waters, K. (2015*) The Nova Scotia Restorative Justice Program*. Dalhousie: Dalhousie University. 104p.

Cross, D. (2016) Longitudinal impact of the Cyber Friendly Schools program on adolescents' cyberbullying behavior. *Aggressive behavior, 42(2),* 166-180.

Driscoll, K. (2016) Cyber safety and security for Reduced Crew Operations. *Integrated Communications Navigation and Surveillance*, 1-21. .

Hopkins S. & Ostini J. (2015) Digitized Domestic Violence: Technology Abuse is a Feminist Issue. *Media, Technology*, 23-25.

Hughes, M. (2015) Facing Cyberbullying: *A National Implementation Plan*. The London Anti-Bullying Coalition, 1-28.

Kerstens J. & Jansen J. (2016) The Victim–Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's On-Line Victimization and Perpetration. *Deviant Behavior, 37(5),* 585-600.

Lee, M. (2015) Sexting among young people: Perceptions and practices. *Trends & Issues in Crime and Criminal Justice, 508*, 1-35.

Leukfeldt, E .R. (2015a) Organised Cybercrime and Social Opportunity Structures. A Proposal for Future Research Directions. *European Review of Organised Crime, 2*, 91-103.

Leukfeldt, E. R. (2015b) Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *arXiv preprint arXiv,* 1506.00769

Leukfeldt, E. R., Kleemans, E. R. & Stol, W. P. (2016) Cybercriminal Networks, Social Ties and Online Forums. *British Journal of Criminology, 9*, 35-44.

Moise, A. C. (2015) Some Considerations on the Phenomenon of Cyberterrorism. *Law Annals Titu Maiorescu, 5,* 146.

Murashbekov, O. B. (2015) Methods for Cybercrime Fighting Improvement in Developed Countries. *The Journal of Internet Banking and Commerce, 5*, 24-29.

Musa, M. K. (2015) *Cyber Stalking: Social Issues of Harassment on Internet.* Direct access: idosi.org/aejaes/jaes15(tesms)15/2.pdf

Taivo, R. (2015) Cyber Behavior. *Encyclopedia of Information Science and Technology, 3rd Edition, Hershey*, 638-646.

Williams M., & Pearson O. (2016) Hate Crime and Bullying in the Age of Social Media. Current Perspectives. *Hate Crime Awareness Week, 35,* 25-26.