Criminological Aspects of Current Cyber Security

Submitted: 29 December 2021
Revised: `12 January 2022
Accepted: 18 January 2022

Andrejs Vilks*
https://orcid.org/0000-0002-5161-0760
Aldona Kipane**
https://orcid.org/0000-0001-6408-3456
Inga Kudeikina***
https://orcid.org/0000-0002-7895-4264
Karina Palkova****
https://orcid.org/0000-0002-6909-571X
Jānis Grasis*****
https://orcid.org/0000-0002-1394-9958

Article submitted to peer blind review
Licensed under a Creative Commons Attribution 4.0 International

DOI: https://doi.org/10.26512/lstr.v14i2.41411

Abstract

[Purpose] To analyze the criminological features of the sensitivity of security in the cyber space on the basis of theoretical and empirical bases.

[Methodology] In order to evaluate the criminological aspects of the phenomenon under study, theoretical guidelines, special literature, opinions of national and foreign specialists, research papers and periodicals are analyzed. The following scientific research methods have been used in the development of the study: content analysis, analytical, inductive and deductive approaches, as well as systematic analysis of documents, generalization and forecasting.

[Findings] The authors conclude that the cyber culture and behaviour of the society need to be improved. This would reduce the potential harm of an individual's interests and would raise an individual's understanding of cyber hygiene. An important direction of victimological prevention of cybercrime is a set of systematic and targeted measures to inform people on behaviour of a potential criminal, identifying him/her and personal protective measures and methods to avoid becoming a victim of cyber violations.

[Practical Implications] The materials of the article are of practical value for teachers engaged in the development of lectures, seminars, assignments for independent work.

Keywords: Victimology. Cyber Space. Cyber Threats. Cybercrime. Cyber Culture.

* Andrejs Vilks is a Full Doctor in Law, Professor at the Faculty of Law, Riga Stradins University, Riga, Republic of Latvia.
** Aldona Kipane is a Full Doctor in Law, Associate Professor at the Faculty of Law, Riga Stradins University, Riga, Republic of Latvia.
*** Inga Kudeikina is a Full Doctor in Law, Associate Professor at the Faculty of Law, Riga Stradins University, Riga, Republic of Latvia.
**** Karina Palkova is a PhD in Law, Associate Professor at the Faculty of Law, Riga Stradins University, Riga, Republic of Latvia.
***** Jānis Grasis is a Full Doctor in Law, Professor at the Faculty of Law, Riga Stradins University, Riga, Republic of Latvia.

INTRODUCTION

One of the successful preconditions for the development of a society is a condition or a situation where a person is not threatened, endangered and protected from unwanted events. A criminal offense is an important social problem that has a significant impact on the security of society and every individual (ŅESTEROVA et al., 2015). The modern world cannot be imagined without information and communication technology. Due to the spread of the Internet the opportunities of cybercrimes have increased. New technologies are more and more entering everyday life. They create new potential risks and security threats (VILKS, 2015a). Technology has become an enabler for criminality, leading to new crimes such as up skirting, and the rise in other offenses such as stalking. Fraud and cyber offenses now account for nearly half of all crime in England and Wales (Victim Strategy). The International Monetary Fund has estimated that the annual loss from cyber-attacks is 9% of global net income, or around € 100 billion (Estimating Cyber Risk…, 2018). US cybersecurity venture Cybersecurity Ventures, one of the most professional and skilled cyber defense companies, has estimated that the cost of cybercrime will increase by about 15 percent a year (MORGAN, 2020). Experts predict that the cost of cybercrime in 2021 could reach $ 6 trillion in 2021, and the cost of cybercrime in 2025 will reach $ 10.5 trillion a year. It is acknowledged that cybercrime will cost the world $ 11.4 million a year in 2021 (MORGAN, 2021). Cybercrime will become the third largest economy this year.

Crime has shifted to new forms in recent years. The activities of the criminal world are diversifying, the space of activity expands and the speed of commitment of a crime and of moving a criminal is increasing, the geographical localization is getting ignored. The spread of crime is rightly regarded as a serious threat to national security Undeniably, cybercrime is one of elements that has a significant impact on a state of an individual, group and national security. “Crime and security” is a broad construct, covering issues related to the diverse range of illegal goods and acts, offenders, victims/targets, places, technologies, and formal and informal agents of crime control (COCKBAIN and LAYCOCK, 2017). Cybercrime is a complex problem. Modern technologies radically change the society, its everyday life, they also create new risks that are difficult to predict. From the point of view of security theory, crime should be seen not only in the legal sense, but also in the social aspect as a form of social activity that reflects the nature of the relationship of cultural, economic, state and non-governmental institutions, the link between the political regime and the structure and dynamics of criminality (FRANJIĆ, 2020).

Important document in the field of cyber security is Regulation (Eu) 2019/881 of the European Parliament and Of the Council on Enisa (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (2019). This document defines cybersecurity as the action to be taken to protect network and information systems, their users and other persons exposed to cyber threats. Cyber threats, on the other hand, are any possible circumstances, events or activities that

could cause damage or disruption or otherwise adversely affect networks and information systems, their users and others.

At present, cybercrimes are the fastest – growing criminal offence compared to others. The situation is made more complex by increasing of the transnational character of crime (TUMALAVIČIUS et al., 2016). According to experts' forecasts, cybercrime will exceed the entire drug market in 2021 and the damage is going to be six trillion all over the world. An Indian criminologist, Professor K. Jaishankar (2011) reasonably points out that cybercrimes are no longer simply a hacker attack or an attack on the system, but it is an attack on people (VILKS, 2018). Attacks in a virtual environment or cyberspace take place every day; they are targeting public authorities, enterprises and citizens. In the Global Risks Report (2017), the cyber risks are named among five greater risks alongside terrorist attacks, illegal migration flow, nature disasters and extreme weather conditions. Having analysed the most visited websites, the company "Menlo Security" found out that 42% of sites are at risk of meeting cyber threats. Cyber criminality has a variety of negative consequences for victims and society as a whole. A victim of a cybercrime has not only material damage, but also a traumatic experience that in the short term and the long-term causes or may cause a variety of physical and mental health disorders or their risks. The consequences of cybercrime are also significant for the society, including in financial terms. It has been identified that cyber-attacks cost 400 billion Euros each year to the global economy (Reform of Cyber Security…, 2021).

The unlimited space of the cyber space and the lack of borders make it difficult to monitor it. Cyber space is an abstract environment where communication takes place on a computer network, it is global and captures virtually the whole world, it has no physical boarders. The authors point out that it is difficult to determine the true extent of cybercrime and to what extent traditional criminals have moved to the cyberspace. Borders are not an obstacle for a criminal in cyber space, there is no difference between large and small countries. The broad availability of cyberspace facilitates the possibility of harming an individual, group, society or the state.

The Cyber Security Strategy of Latvia 2014-2018 (2021) states that cyberspace is an interactive environment that includes users, networks, computing technology, software, processes, information in transit or storage, applications, services, and systems that are connected directly or indirectly to the Internet, telecommunications or computer networks, and where its users interact. Professor S. Brenner (2001) writes that cyberspace is an environment that exists along with the real world, but independently of it. It exists in human imagination but does not contain material substance. It is a new space whose origins are to be found in the real world, but which goes beyond that reality. Modern society, its life and its social relationships are deeply influenced by virtual space, and this is the reason why the world's information technology specialists and representatives of various branches of science focus on solving the problems of cyber security (LIMBA et al., 2017). Not without a reason in another source, this environment is also described as the fifth of the common environmental system. It requires co-

ordination, co-operation and legal actions among countries, as in the land, sea, air and space environment (SCHOLBERG and GHERNAOUTI-HELIE, 2011).

CYBER SECURITY AS A SECURITY DIMENSION

"Security" is an old expression and the exact meaning of it "feeling save" is of vital importance from ancient times till today. Through all the centuries security has been considered to be an inherent part of fullness and completeness (LANKAUSKIENĖ and TVARONAVIČIENĖ, 2012). Security is a complex concept and is linked to many spheres of individual's, group and social life. It is a concept that has several levels. There are considered at least two levels in philosophical retrospective: micro level or personal security, and macro level or social and national security. If there are any objective or subjective reasons that threaten the macro level, they also endanger the micro level. At the same time, the insignificant role of security assessment at the micro level can serve as a catalyst to reduce the security level at the macro level (SMIRNOV et al., 2018). Security is not a constant phenomenon, but a phenomenon that needs to be built and maintained, adapted to changing risks and needs of the individual, and should be developed and supported regularly through innovative approaches. Science-based methods and approaches and recommendations should be followed when developing new models for the control and prevention of criminal activities. In particular, the principles of development of crime prevention and control programs should be mentioned (TUMALAVIČIUS et al., 2017).

Safety is one of the fundamental needs of a human being. For an individual, safety is the freedom from potential or existing harm, loss in the various areas of social life. The levels of an individual's relationships, in which his/her feeling of safety is gradually developing, the safety circles are the individual himself/herself; family and close relations; society; state and international environment (Report on Population Development…, 2021). People's perception of the concept "Safety" can be divided into four groups: safety as an internal state; safety as a perception of their protection; safety as a necessity; interpersonal safety (trust-based relationships) (MIHAILOVA, 2015).

In the information age cybercrime is a symbol of online insecurity and risk (WALL, 2007). According to the opinions of representatives of the criminological security theory, criminological security is a subjective state of a person, society and the state in protecting the rights, freedoms and legitimate interests from criminal offences and protection from such threats, as well as an individual's feeling of safety from threats and harm (SYMONENKO, 2007). Insecurity in cyberspace may impact the reliability of the use of information and communication technologies and thus prevent the development of a modern and innovative society (Cyber Security Strategy…, 2021). The origins of cyber threats are linked to the misuse of information and communication technologies and the use of them can be both an end in itself and an instrument that can be used by a wide range of users (CAVELTY, 2008). According to CERT.lv data,

part of the leakages experienced in the global cyberspace in 2017 has occurred due to insufficient user awareness on the use of cloud services and the level of security. Every month information on the average 90,000 to 100,000 vulnerable unique IP addresses have been gathered (Public Report on CERT.LV…, 2017).

Nowadays cyber security is one of the greatest challenges in the individual, community, national and global context. Cyber security is a global phenomenon. As such, it has to deal with all levels, from the international arena to regional, national and local levels. The threats may be the same, but the response may vary (ANDREASSON, 2011). The authors acknowledge that determining the state of security in cyberspace is a particularly complex issue; it is difficult to assess what is safe in a virtual environment. The rapid development and variability of technology should be taken into consideration, and the criminal environment adapts to these changes. H. Nissenbaum (2005) argues that cyber security, although it includes the technical safety of computers, goes far beyond its substance. The border separating it, where the technical overlapping of computers and cyber security end, is to be searched for in the way that the particular enterprise, officials or individuals give value to aspects such as privacy, confidentiality, anonymity. In her opinion, technical data security is focused on protecting individuals from all kinds of threats, including those that violate privacy or try to stop the freedom of an individual. One must agree that cyber security is not just the security of information technology, but also includes organisational, personal and physical security measures. Cyber security can be explained as a security state and conditions in cyberspace, when the protection of the vital interests of the individual, society and the state is ensured.

THREATS OF CYBER SECURITY AND THEIR PERCEPTION

Every year, the number of the Internet users is increasing in Latvia. Data from the Latvian Internet Association show that 82% of the population is available on the Internet in 2017, 1 457 800 are active users, 848 800 users use the Internet by the telephone, 446 800 users use the Internet and 79% of users use the Internet daily (Industry in Numbers, 2017). Since 2010, the number of the Internet users has increased by 16 percentage points. According to gemius Audience data, in 2020, the average number of Internet users in Latvia from all platforms combined (i.e., from computers, mobile phones and tablets) was 1,400,000 users or Real Users. On average, 1,176,000 users used computers to browse the Internet and 1,107,000 used mobile devices (Latvians of all ages…, 2021).

Everyone in the information society is in a permanent unorganized flow of information. In Latvia the average Internet user is 25-44 years old. In the studies conducted in recent years it has been spoken about the gap between generations, based on the different skills of members of society of different generations in constructing social habits, and their different opportunities to access technologies (DANIELA, 2018). The proportion of the Internet users significantly varies within age groups. Youth (children and young people) is one of the most rapidly growing groups of the Internet users. According to the Youth

Law (2011), young people are persons from 13 to 25 years of age. It has to be admitted that social networks have had a significant impact on children and young people. This is a social group that is very passionate about communication on social networks. At the same time, it should be noted that taking into account the psychological and age characteristics this age group is subject to the greatest risks. An immature psyche can increase the chances for a child or young person to become both a cyber-abuser and a victim.

The introduction of information and communication technologies into daily lives of children and young people creates a situation that researchers consider unique: children's experience is often incomprehensible for adults. Today's children and young people are increasingly connected to the new technologies. They reveal their identity and interact with each other in the virtual space with surprising naturalness, with greater intensity expressing intimacy (TAPSCOTT, 2008). Sociological research confirms that in the welfare society, in the first decade of the 21st century the user of technology was on average 6-13 years old, while in the second decade, one is already talking about the digital literacy of children of 3-4 years old (RUBENE, 2018). Socializing through social networks has become a favourite hobby. It is increasingly integrated in everyday activities, especially for those individuals who are "digital natives" and "born digital" – individuals who grow up and live in the digital environment. N.L. Fraim (2006) points out that socializing on the Internet is "electronic interaction" by defining cyber socialisation as "computer-based interaction with known or unknown individuals for exploration, entertainment, friendship or relationship, subject to loneliness and sexual deprivation".

Accordingly, the authors can talk about cyber addiction – human addiction to the environment created by modern technology. The view of Russian specialist V. Pleshakov (2012) is to be supported that the Internet has become an urgent need in the human life: The Internet "must always be available". The modern man *Homo Sapiens* turns into a unique new form of *Homo Cyberus* (a cyber-socializing person). The danger is that in reality there is not always a clear boundary between the virtual environment and the physical environment. S. Greenfield (2008) points out that virtual communication and the fascination with social networks lead to personality and brain degradation. Social networks are dangerous, because when they are used, people often divide their lives into two parts: "in the real virtual reality and "quasi-life" (false life) reality where reality becomes blurred". At the same time, it has been identified in the studies that parents are often unaware of the potential risks related to the use of technology. It refers to a short circuit, fire or virus that can damage the device itself. However, there is a lack of information and awareness about the risks to children. This should be seen as a signal for improving the pedagogical competence of parents (RUBENE, 2018).

According to the studies conducted by "Kaspersky Lab" and "iconKids& Youth" in 2016, children are growing up online while spending their lives in it (Kaspersky Lab: Kids…, 2021). Four children out of ten use their smartphone even at meals; in the age group from 8 to 10 years old, 23% of children's parents admitted that a child was going to bed with a mobile phone, but with child's age

the volume of use is increasing, namely from 11 to 13 years – 41% and 64% in the age group from 14 to 16. According to UN International Telecommunication Union data, in 2017, the proportion of young people (15-24 years old) who use the Internet is significantly higher (71%) than the overall proportion of the population (48%) (ICT Figures and Facts, 2017). In 104 countries more than 80% of young people can be reached online. In developed countries 94% of young people use the Internet, in developing countries – 67% and in low-income countries – 30%. Most of the young people (9 out of 10) who do not use the Internet live in Africa, Asia and the Pacific Ocean states.

THEORETICAL AND VICTIMOLOGICAL ASPECTS OF PREVENTION OF CYBERCRIME

Prevention of crime (also known as crime control or restriction) is a complex set of methods and tools aimed at preventing criminal offenses in the country or in one of its regions. The modern world is characterized by an increase in the diversity of manifestations of deviance – types of behaviour that violate norms established by the state (law) or worked out by society (morality). There is a blurring boundary between "deviant" and "normal" behaviour. At the same time, there is a "crisis of punishment" – the ineffectiveness of traditional forms of social control over criminal (generally deviant) behaviour. In these conditions, the development of strategy and tactics of social control over crime is gaining in importance (MATVEJEVS, 2018). Of course, it is more effective to take action before the problem arises, rather than responding to a criminal offense. Reasonable crime prevention is recognized as a practical method for direct control of crime. It involves analysing criminal attack methods and designing specific actions within the environments of potential victims to reduce criminal opportunities and manage the crime risk (MULUGETA and MEKURIAW, 2017). Preventive measures are implemented at national, regional and local level.

Prevention of crime is understood as a system of multi-level legal coercion measures. It has to be admitted that crime prevention may only be effective in a comprehensive and coherent way, transforming the social environment, and transforming the personality of a criminal, by neutralizing criminal manifestations. In general, crime prevention refers to a series of strategies implemented by companies, community, government, individuals and non-governmental organizations to influence the various environmental, cultural, economic and social factors affecting the risk of crime and victimization (WINTERDYK, 2017). Preventive measures should focus on the wider areas of social life: social security; employment; education; leisure activities; urban planning and so on.

It has been considered that crime can be better prevented by special programs that are jointly implemented by law enforcement agencies, other public authorities, local authorities and the public. Thus, successful crime prevention

may be possible through community partnership and participation. A well-planned crime prevention strategy not only prevents crime and victimization, but also promotes public safety and sustainable development of the country.

Developing crime prevention programs, in order to make the activities effective the development stages should be followed. The first step is to identify and precisely define the problem. This is one of the main prerequisites for the usefulness and purposefulness of the program. The second step is to identify the objectives and tasks of the program. The third step is the selection of preventive measures. To this end, all possible and appropriate preventive measures to address a particular problem are analysed, taking into account their potential for effectiveness. The fourth stage is the determination of execution and management structure of the program (TUMALAVIČIUS et al., 2017).

Cybercrime as a form of crime is a dynamic social, legal and technological phenomenon. The criminal world is constantly copying in the new social conditions and in human activities. Technology is cumulative and there is no way to turn back in time. The people have to therefore develop the skills, the structures and the regulations, which will allow to anticipate the threats and the evolutions of both technologies and markets better and more quickly. This will allow to pilot and enhance change, applying new technologies to present and future needs, in an ethical and responsible way (BARTSCH and FREY, 2018). The intense development of cybercrime determines that the fight against this type of crime is also rapidly developing. In this context, two major directions are recognized regarding the fight against cybercrime: the development and improvement of international and national laws and development of the structures of the institutional system that take concrete measures to prevent and combat cybercrime (VILKS, 2015b).

Regarding the cybercrime, the authors can refer to three types of crime prevention strategy described in criminological literature (TONRY and FARRINGTON, 1995):

1. Primary prevention – it requires the use of various tools and measures in cyber space to promote, strengthen or enhance user skills in the use of social networking on the Internet; awareness of the risks in this environment; improve the level of education of the user; to provide systematic information on potential risks. For example, the circulation of illegal information, child pornography threats, dangers of the Internet.

2. Secondary prevention – cybercrime prevention (criminological) policy has to be developed with the aim to target preventive measures to specific risk groups, both offenders and potential victims. In developing crime prevention programs, it is necessary to follow certain stages ensuring the effectiveness of prevention and control activities. Problem identification and formulation are to be distinguished as the first stage (TUMALAVIČIUS at el., 2018).

3. Tertiary prevention aims at re-socializing of a cybercriminal and rehabilitating of a victim. Special "recovery" programs for cybercriminals and victims should be developed.

It is important to take into account the peculiarities of the virtual environment, the impact on potential risks, the spreading of information and the

problem of content control, the diverse criminal and potential victim range. For example, providing of parental control, content filters, active security control, no access to chats are proposed asones of the prevention measures to reduce the availability of malicious content. In the prevention of cybercrime, it is necessary to constantly search for new forms and methods, both keeping from the committing offense and through using various measures. The authors believe that in comparison to the physical environment, the personality of a victim himself/herself and his/her activities in cyberspace are an essential aspect in the cybercrime mechanism. F.M. Llinares (2012) tells that the role of a victim in cyberspace is much more decisive than in the physical one. According to the view expressed by the professor, a victim sets the risk limits to which he/she will be subjected. In this respect, the Routine Activity theory can be used to explain the mechanism of criminal behaviour. According to this theory, a cybercrime takes place in interacting of three elements in cyberspace and in time: a motivated criminal; an appropriate victim, who is related to the motive and communicative environment of a criminal; and lack of adequate protection (or guarding).

The study of the victimological aspects indicates that while an individual personally has not encountered security problems in the electronic environment, ease of use is the most important requirement and precaution is forgotten. Victims do often not find or understand that they have become victims of a cybercrime. A fairly large proportion of victims of such cases do not report, they fear, and/or feel blame for it. It is hard for an unaware person to understand that information published on the Internet can no longer be made unprecedented. Its copies will remain somewhere, and it is not known who and when will use them (MURĀNE, 2015). Similar victimological problems are indicated for companies. According to data from the Global Economic Crime Survey (2016), most companies are still not adequately prepared for – or even understand the risks faced: only 37% of organisations have a cyber-incident response plan. Though most people believe that cyber security is something important, research on the relationship between attitudes and behaviour (maintaining privacy, providing security) online shows that the person's actual behaviour is not in line with his/her attitude (LEUKFELDT, 2017). For example, the interesting results of the study conducted by "Kaspersky Lab" and "B28 International" in March 2015 showed the interesting differences in gender attitudes towards online threats. "Women who use the Internet are less worried about online threats, 27% of European men agreed to have the opportunity to become a victim of cybercrime, while women are 18%. In Europe, 9% of men and 12% of women do not use security systems on their devices" (Women are less Concerned…, 2021).

It is reasonable to recognize that a significant number of users have a poor understanding of cyber space potential, safe working in this environment and protection measures that the authors can call cyber security awareness. Persons lack experience, skills to identify and assess risk levels, anticipate and prevent harm. The authors state that the positive personality guideline is the ability to critically and adequately assess the situation and choose the right behavioural

model. Therefore, it is important that people work online safely and securely, such as intelligently sharing information, avoiding potentially dangerous websites, and so on. This is an important area of victimology, which needs to be improved in the country, reducing the risks of negligence and reckless behaviour among the population. Another important area is to strengthen parent education and responsibility for and with their children. Parents as natural guardians of a child represent the first level of education because there is no doubt that parents primarily affect the formation a child's legal consciousness and moral principles (KUDEIKINA, 2018).

The fewer people will have the ability to become a victim of cybercrime, the fewer cybercrime will be. The ability and skills of citizens to protect themselves and their loved ones, to build their personal security and safety must be promoted. A child is especially to be protected, following the provisions of the Law on the Protection of the Children's rights, the child as a physically and intellectually immature person that needs special protection and care. D. Finkelhor (2008) has found that three specific types of characteristics increase the potential for victimization:

1) Target vulnerability. The victims' physical weakness or psychological distress renders them incapable of resisting or deterring crime and makes them easy targets.

2) Target gratifiability. Some victims have some quality, possession or attribute that an offender wants to obtain, use, have access to, or manipulate.

3) Target antagonism. Some characteristics increase risk because they arouse anger, jealousy, or destructive impulses in potential offenders.

There are two areas of victimological aspects of cybercrime prevention:

1. General or general social – it includes a wide range of economic, social, cultural, educating and legal activities that actively target not only the victimity of particular persons, but also the formation of criminal tendencies in the society.

2. Special (criminological) – a set of measures carried out by the state, law enforcement agencies and public organizations with persons who, in certain circumstances, have the ability to become victims. An important task of law enforcement institutions is the identification of a potential victim and a systemic, purposeful upbringing work with them (ZĪLE, 2002).

To reduce the risk of children becoming victims online, EU-wide education initiatives and standardized EU-level prevention and awareness-raising campaigns are crucial for online education. Such initiatives should seek to include younger children (Internet Organized Crime…, 2018). Cyber culture, behaviour in the cyber space should be improved in the society. This would reduce the potential harm of the individual's interests and the individual's understanding of cyber-hygiene, similar to the notion of personal hygiene. It is a tool for the proper protection and maintenance of information technology systems and devices and the implementation of best practices in cyber security (Review of Cyber Hygiene…, 2016). The authors can describe it as a set of practices, regular precautions taken by users to protect data, to protect against any harms regarding their interests and external attacks. Diverse explanatory measures among the population have a positive impact. Warning information

included in various informational materials and recommendations for action in cyberspace increases the attitude of citizens towards cyber security measures, possible actions of a criminal and their harmful consequences, as well as develops and broadens an individual's critical attitude towards both his/her actions and actions of others in a virtual environment.

CONCLUSION

It is important to predict the development tendencies of the criminal situation in the future. Cyber risk forecasting is required. Criminological forecast shows that next year, unlike other criminal offenses, cybercrime will continue to increase, negatively affecting the global cyber security situation. The world now faces new threats that are more diverse, less visible and less predictable. This is confirmed by new criminal offenses in the area of cybercrime. Such a rapid life makes it necessary to search for new effective solutions to reduce the vulnerability of an individual in cyberspace. One of the most urgent tasks in Latvia is to improve the awareness of the population about the cyber threats and the basis of cyber security.

An informed, educated and trained individual forms the basis of an individual's cyber security. Public education involves identifying risks, identifying the potential consequences and the ability to use security measures. A cyber security culture should be promoted. Cyber security measures should be regularly promoted to society. The alarming effect is a broad explanatory work through mass media. An important direction of victimological prevention of cybercrime is a systematic and targeted set of measures to inform people about the behaviour of a potential criminal, his/her exposure and personal protective measures and methods to avoid becoming a victim of cybercrime.

REFERENCES

ANDREASSON, K. J. (2011). *Cybersecurity: Public sector threats and responses*. Boca Raton: Taylor & Francis Group, LLC.

BARTSCH, M., & FREY, S. (2018). *Cybersecurity best practices.* Retrieved from: https://www.amazon.com/Cybersecurity-Best-Practices-Cyberresilienz-Unternehmen/dp/3658216549. Access date: 04 September 2021.

BRENNER, S. (2001). *Is there such a thing as a virtual crime?* Retrieved from: https://lawcat.berkeley.edu/record/1126844. Access date: 17 September 2021.

CAVELTY, M. D. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. London: Routledge.

COCKBAIN, E., & LAYCOCK, G. (2017). Crime science. *Oxford Research Encyclopedia of Criminology and Criminal Justice.* Retrieved from: http://criminology.oxfordre.com/view/10.1093/acrefore/978019026407

9.001.0001/acrefore-9780190264079-e-4. Access date: 02 September 2021.

Cyber Security Strategy of Latvia 2014-2018. (2021). Retrieved from: www.unodc.org. Access date: 21 September 2021.

DANIELA, L. (2018). *Innovations, technologies and research in education*. Newcastle upon Tyne: Cambridge Scholars Publishing.

Estimating Cyber Risk for the Financial Sector. (2018). Retrieved from: https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/. Access date: 13 September 2021.

FINKELHOR, D. (2008). *Childhood victimization: Violence, crime, and abuse in the lives of young people*. New York: Oxford University.

FRAIM, L. N. (2006). *Cyber socialization: What's missing in my life?* Retrieved from: https://www.diva- portal.org/smash/get/diva2:1128959/FULLTEXT01.pdf. Access date: 07 September 2021.

FRANJIĆ, S. (2020). *Cybercrime is very dangerous form of criminal behavior and cybersecurity*. Retrieved from: https://ijournalse.org/index.php/ESJ/article/view/233. Access date: 23 September 2021.

Global Economic Crime Survey. (2016). Retrieved from: https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf. Access date: 05 September 2021.

GREENFIELD, S. (2008). *ID: The quest for identity in the 21st century*. London: Scepter. Marchenoka.

ICT Figures and Facts. (2017). Retrieved from: www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf. Access date: 27 September 2021.

Industry in Numbers. (2017). Retrieved from: www.lia.lv/statistika. Access date: 18 September 2021.

Internet Organized Crime Threat Assessment. (2018). Retrieved from: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. Access date: 09 September 2021.

JAISHANKAR, K. (2011). *Cyber criminology: Exploring Internet crimes and criminal behavior*. Boca Raton: Taylor & Francis Group, LLC.

Kaspersky Lab: Kids spend more of their lives online as they grow up. (2021). Retrieved from: www.kaspersky.com/about/press-releases/2016_kaspersky-lab-kids-spend-more-of-their-lives-online-as-they-grow-up. Access date: 12 September 2021.

KUDEIKINA, I. (2018). *Problems associated with the parents' failure to execute their care responsibilities from the viewpoint of juvenile delinquency*.

Retrieved from: https://sgemsocial.org/ssgemlib/spip.php?article6539&lang=en. Access date: 05 September 2021.

LANKAUSKIENĖ, T., & TVARONAVIČIENĖ, M. (2012). Security and sustainable development: approaches and dimensions in the globalization context. *Journal of Security and Sustainability Issues,* 1(4), 287-297.

Latvians of all ages used the Internet more last year. (2021). Retrieved from: https://eng.lsm.lv/article/society/society/latvians-of-all-ages-used-the-internet-more-last-year.a389537/. Access date: 11 September 2021.

LEUKFELDT, R. (2017). *Research the human factor in cybercrime and cubersecurity*. The Hague: Eleven International Publishing.

LIMBA, T., AGAFONOV, K., PAUKŠTĖ, L., DAMKUS, M., & PLĖTA, T. (2017). Peculiarities of cyber security management in the process of internet voting implementation. *Entrepreneurship and Sustainability Issues,* 5(2), 368-402.

MATVEJEVS, A. (2018). Effective crime control as guarantor of public security. *Journal of Security and Sustainability Issues,* 7(3), 417-426.

MIHAILOVA, S. (2015). *Internal security – One of the essential factors of sense of security*. Riga: RSU.

MORGAN, S. (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Retrieved from: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. Access date: 23 September 2021.

MORGAN, S. (2021). *Cybercrime Vs. COVID-19: Which will inflict more financial harm?* Retrieved from: https://cybersecurityventures.com/cybercrime-vs-covid-19-which-will-inflict-more-financial-harm/. Access date: 07 September 2021.

MULUGETA, E., & MEKURIAW, D. (2017). Community policing: Practice, roles, challenges and prospects in crime prevention in East Gojjam administrative zone. *Social Crimonol,* 5, 1-13.

MURĀNE, I. (2015). *Information security awareness system for everyday computer users.* Riga: University of Latvia.

ŅESTEROVA, M., TEIVĀNS-TREINOVSKIS, J., & IVANČIKS, J. (2015). Security and public safety: Impact of gender on prisoners' justice perception. *Journal of Security and Sustainability Issues,* 4(4), 403-413.

NISSENBAUM, H. (2005). Computer security meets national security. *Ethics and Information Technology*, 7(2), 61-73.

PLESHAKOV, V. (2012). *Human cybersocialization: From Homo Sapienssie to Homo Cyberusia.* Moscow: Prometej.

Public Report on CERT.LV Task Execution. (2017). Retrieved from: https://cert.lv/uploads/CERT-LV_gada_2017_publ_galaversija.pdf. Access date: 05 September 2021.

Reform of Cyber Security in Europe. (2021). Retrieved from: www.consilium.europa.eu. Access date: 22 September 2021.

Regulation (Eu) 2019/881 of the European Parliament and Of the Council on Enisa (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation. (2019). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=LV. Access date: 04 September 2021.

Report on Population Development in Latvia 2002/2003. (2021). Retrieved from: http://providus.lv/article_files/920/original/UNDP2003_ful_lv.pdf?1326366357. Access date: 05 September 2021.

Review of Cyber Hygiene practices. (2016). Retrieved from: https://www.enisa.europa.eu/publications/cyber-hygiene/at.../fullReport. Access date: 13 September 2021.

RUBENE, Z. (2018). *Digital childhood: Some reflection from the point of view of philosophy of education, in Daniela. Innovations, technologies and research in education.* Cambridge: Scholars Publishing.

SCHOLBERG, S., & GHERNAOUTI-HELIE, S. A. (2011). *Global treaty on cybersecurity and cybercrime*. Retrieved from: http://pircenter.org/media/content/files/9/13480907190.pdf. Access date: 18 September 2021.

SMIRNOV, A., LAVRINENKO, O., & TUMALAVIČIUS, V. (2018). Analysis of social-economic security of administrative areas in Latvian municipalities. *Journal of Security and Sustainability Issues,* 7(4), 817-829.

SYMONENKO, D. A. (2007). *Criminological security and its provision by the internal affairs bodies*. Retrieved from: https://search.rsl.ru/ru/record/01003061264. Access date: 28 September 2021.

TAPSCOTT, D. (2008). *Grown up digital: How the Net generation is changing your world*. Retrieved from: https://www.amazon.com/Grown-Up-Digital-Generation-Changing/dp/0071508635. Access date: 09 September 2021.

The Global Risks Report. (2017). Retrieved from: http://www3.weforum.org/docs/GRR17_Report_web.pdf. Access date: 05 September 2021.

TONRY, M., & FARRINGTON, D. P. (1995). *Strategic approaches to crime prevention*.
Retrieved from: https://pdfs.semanticscholar.org/82c3/00f77c242a1dd77af552e647ae233679054d.pdf. Access date: 11 September 2021.

TUMALAVIČIUS, V., IVANČIKS, J., & KARPISHCHENKO, O. (2016). Issues of society security: Public safety under globalization conditions in Lithuania. *Journal of Security and Sustainability Issue,* 4(9), 545-573.

TUMALAVIČIUS, V., NIKOLAYEVSKYY, V., & ENDZIŅŠ, A. (2017). Issues of state and society security (Part II): Management of control over individual criminal processes. *Journal of Security and Sustainability Issues,* 6(4), 605-618.

TUMALAVIČIUS, V., VEIKŠA, I., NAČISČIONIS, J., ZAHARS, V., & DRASKOVIC, V. (2018). Issue of the state and society security: Ensuring public security in the fight against crime. *Journal of Security and Sustainability Issues,* 6(3), 401-418.

VILKS, A. (2015a). *Criminological aspects of modern technologies*. Riga: Valsts Policijas Koledža.

VILKS, A. (2015b). *Modern technologies – New risks and security threats*. Retrieved
from: https://www.rsu.lv/sites/default/files/imce/Dokumenti/izdevumi/socrates_2_2015.pdf. Access date: 18 September 2021.

VILKS, A. (2018). *Cybercrime and sexual exploitation of children in e-environment in the context of strengthening urban and rural security*. Retrieved from: https://www.shs-conferences.org/articles/shsconf/abs/2019/09/shsconf_shw2019_01010/shsconf_shw2019_01010.html. Access date: 19 September 2021.

WALL, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.

WINTERDYK, J. A. (2017). *Crime prevention: International perspectives, issues, and trends*. Boca Raton: Taylor & Francis Group, LLC.

Women are less Concerned about Cyber Threats. (2021). Retrieved from: https://skaties.lv/zinas/zinatne-un-tehnologijas/tehnologijas/kaspersky-lab-sievietes-ir-mazak-nobazijusas-par-kiberdraudiem/. Access date: 16 September 2021.

Youth Law. (2011). Retrieved from: https://www.youthpolicy.org/national/Latvia_2011_Updated_Youth_Law.pdf. Access date: 14 September 2021.

ZĪLE, J. (2002). *A victim from crime science perspective*. Latvia: Vēstnesis.