INFO - 2197 UDK: 007:343
Primljeno/Received: 2018-03-02 Authors Review/ Pregledni rad

https://doi.org/ 10.32914/i.51.3-4.7

PREVENTIVE MEASURES AGAINST COMPUTER RELATED CRIMES: APPROACHING AN INDIVIDUAL

PREVENTIVNE MJERE PROTIV RAČUNALNOG KRIMINALA: PRIBLIŽAVANJE POJEDINCU

Roman V. Veresha
Academy of Advocacy, Kyiv, Ukraine
Akademija za odvjetništvo, Kijev, Ukrajina

Abstract
Cybercrime is a combination of information, financial and personal security threats. The purpose of this research is to target statistical data to allocate the most effective preventive measures against cybercrime that would contribute to the combat at the level of potential (or real) cyber victims and cyber criminals. Brining the so-called Cyberethics into the life of people will be preventive against cybercrimes, as it will add to their culture of cyberspace through educational and popular science projects (such-like program that was put into action in Nigeria stroke positively). With the rapid spread of cybercrime, preventive measures geared towards individuals such as anti-criminalization, anti-bullying and anti-phishing propaganda, the practice of shaping negative attitude towards crimes, and discovery of responsibility for committing cybercrimes gain in importance. Society improvement as a countermove to cut out criminal factors provoking a positive or neutral attitude to cybercrimes should be geared towards better living, as the higher is the standard the lower is the level of cybercrime. Taking individualized preventing measures to people prone to commit cybercrimes will prevent against such even before they take place (with cyber extortion and ransomware threats, such actions gain in relevance). For the fight against cybercrime, special programs are to level down victimization in the field of cybersecurity by fostering a shielding attitude in persons who can become victims. The path of designing such programs will lead to a drop cybercrime activity. Specific public authorities and non-governmental

Sažetak
Kibernetički kriminal je kombinacija informacijskih, financijskih i osobnih sigurnosnih prijetnji. Svrha ovog istraživanja je ciljati statističke podatke za dodjelu najučinkovitijih preventivnih mjera protiv *cyber* kriminala koje bi doprinijele borbi na razini potencijalnih (ili stvarnih) *cyber* žrtava i *cyber* kriminalaca. Uvođenjem tzv. *Cyber*-etike u život ljudi bit će preventiva protiv *cyber* kriminala, jer će doprinijeti njihovoj kulturi korištenja *cyber*-prostora kroz obrazovne i popularno-znanstvene projekte (takav program je pozitivno djelovao u Nigeriji). S naglim širenjem *cyber* kriminala, preventivne mjere usmjerene prema pojedincima kao što su anti-kriminalizacija, propaganda protiv zlostavljanja i anti-phishing, praksa oblikovanja negativnog stava prema zločinima i otkrivanje odgovornosti za počinjenje kibernetičkih kriminala dobivaju na važnosti. Poboljšanje društva kao protupotez za izostavljanje kriminalnih čimbenika koji izazivaju pozitivan ili neutralan stav prema kiberkriminalitetu treba biti usmjereno prema boljem životu, jer što je viši standard, to je niža razina cyber kriminala. Poduzimanje individualiziranih mjera za sprječavanje ljudi koji su skloni počiniti kibernetički kriminal spriječit će takve napade čak i prije nego što se dogode (s prijetnjama *cyber* iznuđivanja i *ransomwarea,* takve akcije dobivaju na važnosti). Za borbu protiv kibernetičkog kriminala, posebni programi su smanjivanje viktimizacije u području kibernetičke sigurnosti poticanjem zaštitnog stava osoba koje mogu postati žrtve. Put izrade takvih programa dovest će do pada aktivnosti *cyber* kriminala. U preventivnom

organizations should take part in the preventive process. All-encompassing preventive measures against cybercrime approaching individual at the international level will allow designing specific pilot programs for individualized prevention.

procesu trebaju sudjelovati posebna javna tijela i nevladine organizacije. Sveobuhvatne preventivne mjere protiv *cyber* kriminala koje se približavaju pojedincu na međunarodnoj razini omogućit će osmišljavanje specifičnih pilot-programa za individualiziranu prevenciju.

1. INTRODUCTION

Modern society evolves in the climate of rapidly developing information and communication technologies, so one of the main problems here is how to build a comprehensive legal system of information security measures /**1**/. Cybercrime tools are considered the Internet, e-mail and social networks, but the list gets longer year-by-year /**2**/. Thus, simpler life in social space brought new technologies on the stage that triggered some security problems and opened doors for cyber criminals to enter and attack cybersecurity with less effort /**3**/.

Now is a time when almost every person decides for one's self on the role of computer technologies in his (her) everyday life. On a casual basis, computer technologies took over the single aspect of it, so cyberspace become an inescapable, far-reaching and decisive factor that gave birth to a new reality that needs security as any other. Cybersecurity measures should take place outside (protection against offences committed by other countries and criminal groups against individual citizens) and within the national space (protection against offences committed by other citizens), especially given that global cybercrime development took progressive turn /**4**/.

Cybersecurity problems are now in the focus of researchers, especially some areas touched by the anti-cybercrime need: for example – computer-based crimes like cyber-attacks with a network involved, phishing, cyberstalking and copyright infringement /**5**/. For credit card fraud, we stand on that preventing against the spread of innovative online technologies to every door takes special programs to design that would encompass people on how such illegal activity may hit on them, reach them out with the main cybercrime trends and methods for combating cyber-fraud /**6**/. Cybercrime in the sphere of financial activity is another side of the problem. As long as the impact of cybercrime on the financial sector is significant, cybercrime takes a lot of money (it depends on the relationship between tangible and intangible factors). Multilevel analysis will show that huge amount of money spent by companies on cybersecurity will increase the cost of cybercrime in this area, entailing obstacles for those who combat this problem /**7**/. Investments in cyberspace protection from crime also takes green, as highlighted within the context of establishing the benefits and drawbacks of advanced anti-cybercrime technologies /**8**/.

Cybersecurity proved to be a priority sphere of corporate information security, since digital technologies rooted deeply into business, changing business ethics, models and types of employment (the number of remote employees, who connect to corporate networks remotely, continues to jump, etc.). This puts companies at high risk if they rely on digital technologies /**9**/. This problem is under the looking glass to protect private computers, storage media and information systems against cybercrime committed against availability of computer data or systems that are important to holders. Protection at this point requires some effective measures to undertake /**10**/. Cybercrime threat to companies is analyzed from the perspective of fraud matters. In the United States, for example, 13100000 people became victims of identity theft in 2013. This cost to more than 18000000000 dollars /**11**/. Cyberstalking is an exciting matter to discuss – it runs all sorts of threats or even real violent acts against a particular person or group that may go beyond the cyberspace. This kind of matter touches upon liability to penalties /**12**/. Cybercrime are associated with crimes targeting electronic payment systems and digital econ-

omy to finance terrorism. Another aspect of cyberspace protection is about protecting intellectual property rights and copyrights at the legislative level. Attractive is the possibility of police cooperation with other areas of science and practice for ensuring a safe cyberspace: as suggested, Finland could make computer forensics available /**13**/. They also speak about vigilance and awareness as informal confidential forms of control over crimes on the Internet. There is an assumption that such skills will contribute to cooperation between non-state organizations and criminal justice for ensuring cybersecurity /**14**/. Although cyberspace protection is a matter of global concern (when it comes to dangerous international operations), each country should mind harmful cyber-propaganda on their own territory, given that it leads to international crime /**15**/. Cyberterrorism is one of the most dangerous forms of cybercrime, as evidenced by numerous cyber-attacks that recently took place in the world and posed a threat to international security. As soon as it occurred, an emphasis was laid on establishing global international rules and methods for investigating cybercrime. At the moment, many international organizations focused their efforts against cybercrime, because national laws that are in power in individual countries cannot handle the issue /**16**/. Effective cyberterrorism defense (and cybercrime defense in general) needs criminal law resources to be combined with technical resources for investigating and qualifying crimes, so that measures against computer-based crimes like hacking, cyberterrorism, information warfare and whatever else could actually work /**17**/. In the climate of cyber war, international standards and global measures against cybercrime gain in importance /**18**/. Cyberwar launched in 2007, when Tallinn became a center for cybercrime investigation and a place where countermeasures to cyber war are developed /**19**/. Preventive measures against cybercrime occupy a central place in cybersecurity, most significantly those that are the most effective when it comes to approaching an particular individual /**20**/. This was highlighted in the research on prevention against cybercrimes with a sexual component committed against /**21**/. Individualized preventive measures proved to be effective in the research on cyberbullying /**22**/. The above-mentioned areas of research conducted in the field of cybersecurity, as well as the emergence and rapid development of certain types of cybercrime, prove that effective preventive measures, geared towards individuals, that run against cybercrime at the level of national and international security are needed. Therefore, the purpose of this research is to target statistical data to allocate the most effective preventive measures against cybercrime that would contribute to the combat at the level of potential (or real) cyber victims and cyber criminals.

2. METHODS

Methodological basis of this research is the analysis of specific statistical data on cybercrime for 2010-2017: dynamics, cost, case-specific history and categories of people vulnerable to becoming victims. These data are relevant to specific countries (USA, Nigeria, China, Norway, etc.), but put onto display the general cybercrime and anti-cybercrime trends

Thus, statistics show that cybercrime cost tends to increase from year to year. People spend more and more money on designing new technologies against this phenomenon, but this strategy does not pay off, as evidenced by statistics. Statistical data show that in 2007, the US government allocated 7.5 billion dollars to combat cybercrime, when in 2016 this sum was 28 billion dollars /**23**/. Cybercrime brings more and more income year-by-year, so it costs more for the state and business (Cybercrime Costs More Than You Think). This becomes clear from Table 1.

Table 1. Cybercrime Cost Caused to Business in the USA

Year	Cost (USD, billion)
2010	3.8
2011	5.9
2012	6.2
2013	9.1
2014	9.7
2015	11

Other world statistics for 2017-1018 were also analyzed, so we managed to allocate countries with the most and the least developed cybercrime activity /**23**/ (Table 2). From these data, it becomes obvious that cybercrime activity depends not only on the technological achievements of the country, but also on the socio-economic background: the higher is the standard of living the lower is the level of cybercrime.

Table 2. Countries with Highest and Lowest Rates of Cybercrime

Most infected countries	Least infected countries
China: 57.2% of computers infected	Finland – 20.32% of computers infected
Taiwan: 49.15% of computers infected	Norway – 20.51% of computers infected
Turkey: 42.52% of computers infected	Sweden – 20.8% of computers infected

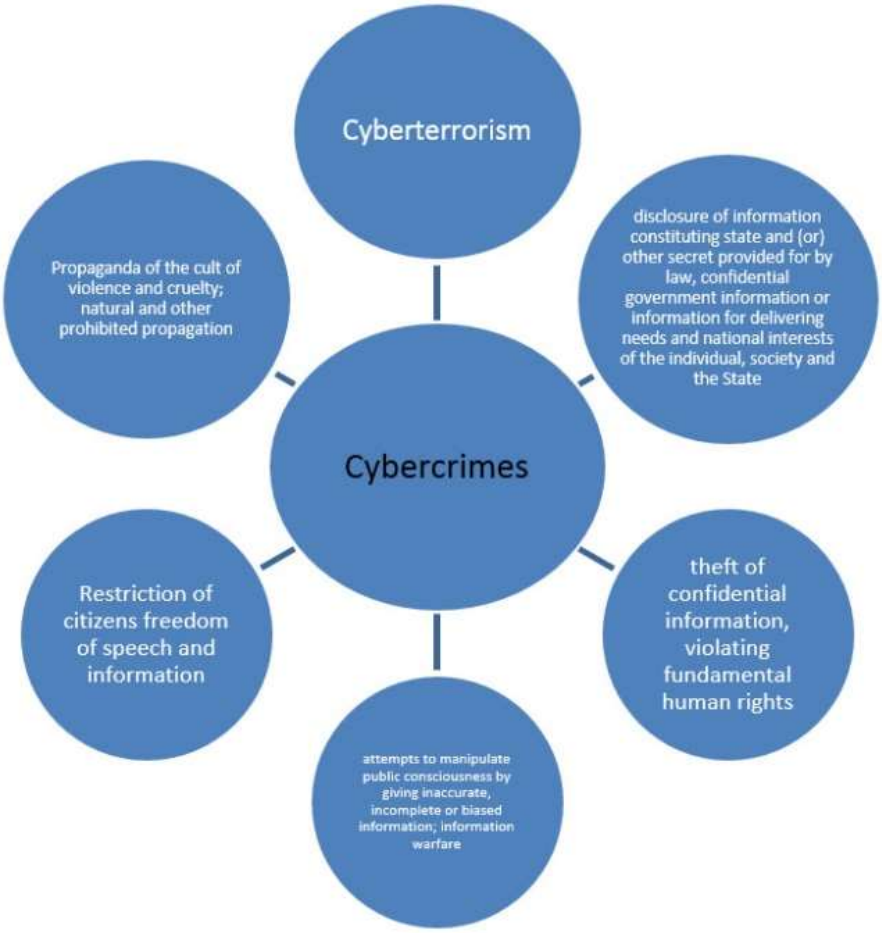
Methodological basis also includes special programs against victimization and criminal intentions to commit cybercrimes: for example – a special preventive program against cybercrime was designed in Nigeria and concerned specifically minors. For its effectiveness investigation, 218 secondary school students were selected. Data analysis shown that the action program for preventing from computer-based crimes adds to student awareness on preventive measures /**24**/. There are also programs to be for determining conditions on which the cost jumps, as well as dynamic capabilities and business models used in cybercrime. These items are verified and investigated from the perspective of scale and nature of a commitment that took place in the cyberspace. Shaping a better understanding of how such illegal activities are performed will boost the law enforcement agencies and security services in identifying cybercrime trends and maximizing the effect of limited resources used against this phenomenon /**6**/. This factored into allocation of the most effective measures against cybercrime that run both at the national and international levels.

Preventive measures were designed following the binding provisions of the international legal acts defining the main areas where cybersecurity is needed. These acts are the International Convention for the Suppression of the Financing of Terrorism (adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999); Okinawa Charter on Global Information Society of 22.07.2000; the UN Millennium Declaration of 8.09.2000; Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions; the United Nations Convention against Transnational Organized Crime (adopted by General Assembly resolution 55/25 of 15 November 2000); The Council of Europe Convention on Cybercrime of 23.11.2001; Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature

committed through computer systems of 28.01.2003; the UN Declaration of Principles Building the Information Society: a global challenge in the new Millennium (dated December 12, 2003).

3. RESULTS

Cybercrime refers to all forms of crime related to computer networks, digital technologies, software, etc /**25**/. In general, cybercrime is a certain type of illegal activity performed by individuals or legal entities using information technology (cyber technology) to achieve a criminal goal. In this case, computer data are not always subject to change. Although this type of crime is relatively new in the criminal world, cybercrime reduced to theft, fraud, copyright infringement, and alike. The main kinds of cybercrime are outlined in Figure 1.



These offences can take place during crimes against confidentiality, integrity, general availability of computer systems and data (illegal access to data and systems; interference with the functioning of a computer by damaging and/or destroying computer or computer-related components; illegal production and sale of such systems, programs or data). They may pop out during crimes committed using a computer or similar device (fraud, theft, etc.), crimes related to content prohibited by law (racism, child pornography, etc.); crimes against copyrights and other related rights, etc.

Since a criminal takes his hands on information contained on certain media, as well as on media itself, cybercrime is classified as cybercrime if certain objects involved (Figure 2).

Preventive measures against any kind of crime are usually divided into common, special and individualized. They are linked to one another, but still have certain peculiarities. We recognize individualized measures (measures geared towards individuals) the most important, since they allow projecting a direct influence on potential (or real) cybercriminals, as well as persons who are likely to become victims of such crime. Statistical data prove that individualized measures are needed to prevent cybercrime, as the greatest number of cybercrimes take place at home, in the Internet cafes and schools using personal gadgets (about 81%) /**20**/.

Individualized counter-measures imply that cybercrime prevention will focus on certain individuals who have already committed crimes against cybersecurity or are prone to commit them. Besides, we believe that these measures should outreach individuals who might become victims of cybercrime because they were raised in a certain way and fostered necessary traits.

The most effective preventive measures against cybercrimes are the following:

— forecasting possible dangerous cybercrimes for prevention purposes by researching through the use of official statistical and empirical data;
— setting sights on the most dangerous spheres that use information technologies as tools in (terrorism, fascism and the alike);
— anchoring an international legal framework containing rules and tools for statistical analysis of cybercrime in global and national dimensions;
— shaping global (international) strategy to combat cybercrime, and formulating international agreements on cooperation for ensuring international security;
— developing conceptual apparatus to define the relationship between people and organizations in the network, following the line of philosophy and psychology;
— boosting informational and educational activities performed by population in some countries to ensure national security;
— detecting external and internal threats to cybersecurity on cue and neutralizing them within the criminal justice framework

There are no individualized counter-measures proposed for the fight against cybercrime. Although one can claim that above measures are geared towards specific individual at the core (so they seem to be rather individualized), actual individualized measures are undertaken in a way different form that the common and special measures are.

For example, one may go with designing special government programs for improving the well-being of citizens through well-paid jobs and a flexible system of incentives and benefits. This should improve the standard of living of some individuals, and, therefore, reduce the risk of them participating in criminal activities for better living. Besides, it seems necessary to foster in individuals habits of being careful about avoiding danger or risk, and undertake preventive measures not to become victims of cybercrime. This first applies to young people, because this particular segment of the population is more prone to committing cybercrime. This requires special programs and measures to introduce that would push young people towards legitimate behavior, and respect for

fundamental rights, freedoms and legitimate interests /**20**/.

One should also keep in mind the danger posed by cyberbullying and phishing (fraudulent attempt to obtain from trustful or inattentive users personal data of those using online auctions, translation or currency exchange services, online stores). Therefore, special programs should also kill or weaken the effect of victimization factors associated with cybercrime.

In general, above factors will have a positive effect at the individual level, but the list is not full.

We introduce the following most effective individualized preventive measures:

1) cyberculture improvement among people, especially children and teens, through educational and popular science projects that are to foster in people a high culture of behavior in cyberspace. Both government and non-government organizations can implement such programs aimed at creating the so-called "Cyberethics". Such a preventive measure is proved to be needed once such-like program stroke positively in Nigeria with 218 student participants. In the long run, it could boost cybercrime prevention /**24**/.
2) putting hands on common cybercrime phenomena and processes, namely launching anti-bullying and anti-phishing propaganda, shaping a negative attitude towards criminal acts, and discovering responsibility for committing cybercrimes. This pack of measures should be put into play by the relevant government bodies (law enforcement and judicial agencies). These measures should be to allocate the main cybercrime determinants, develop effective regulatory and legal means against its growth, and explain the most common and most dangerous illegal actions against cybersecurity. According to statistical data, cyberbullying is becoming more widespread, especially in social networks: Facebook – more than 80% of cases, while other 20% are attributed to other social networks (Instagram, Twitter, etc.) /**22**/. At this point, these measures are needed desperately;
3) waging an aggressive recovery campaign for killing criminogenic factors that provoke a positive or neutral attitude towards cybercrime. These measures should also be undertaken by the relevant government bodies (law enforcement and judicial agencies) operating to improve the standards of living. Statistical data on countries with high and low rates of cybercrime were very informative when demonstrating cybercrime growth dependence on media and cyber technologies, as well as on the overall level of life in the country: the highest rates were recorded in China (57.2%) and Taiwan (49.15%), while the lowest – in Norway (20.51%) and Finland (20.32%) (Mason John, 2018). This speaks well to the effectiveness of this measure;
4) using individualized prevention strategies to people inclined to commit crimes against cybersecurity. This preventive measure is linked to the performance of specific government bodies searching for such persons. At this point, special criteria are requirable to identify people inclined to commit cybercrimes before they direct all their efforts to commit them. The urgency of such measure is evident from the fact that the number if phishing cases increased by 36% in a period from 2016 to 2017, and then 4 000 crimes are committed on a daily basis. Besides, about 230 000 malicious programs appear every day /**23**/.
5) designing special government and non-government programs for reducing cyber-victimization by shaping the ability to resist in individuals who can easily become victims of cybercrime. The measure is guided by criteria of being a victim, and effective (as much as possible) leverages intended to reduce the propensity to become victims of cybercrime. Such programs should be designed with contributions from special government bodies and non-governmental organizations. Such programs are needed, since 78% of people are aware of risks that arise when opening unfamiliar programs or letters, but still do it. Besides, such a measure will come in

handy for private entrepreneurs, since 43% of cyber-attacks target small business /**23**/.

Since cybercriminals do their business not only within one country, international cooperation for combating cybercrime is a matter of importance. This requires modern legal acts that would take into account the specific features of national legislation and specific role programs for individualized prevention of cybercrime.

4. DISCUSSION

Most of analyzed papers on cybersecurity problems are devoted only to certain aspects in this area, while those devoted to individualized preventive measures against these criminal practices are out of the range. Although everyone underlines hat cyber threats are more advanced and destructive nowadays, no specific measures were introduced to create obstacles for criminals and facilitate the exposure of cybercrime.

It is rightly said that technology by itself cannot guarantee security in the sphere of information exchange within cyberspace. Therefore, the major role in ensuring cybersecurity is occupied by individualized prevention of cybercrime, cutting down the very root of it (when an idea of committing such a crime arises). Without new individualized measures for preventing from cybercrime and boosted criminal legislation (both national and international), the most important and vulnerable areas of cybersecurity cannot be protected.

There is one research introducing some measures that, in their opinion, are against or contribute to the fight against cybercrime, although not all of them are so effective. In particular, vigilance and awareness as an informal method of preventing cybercrime raises certain doubts /**14**/, since they can be a preventive tool only for specific targets, but will not work with potential (or real) criminals. Some suggest trust in contrast to regulation, but despite the significant drawbacks of state techno-regulation has, trust without state regulation will not give a desired effect /**26**/. At the same time, cyberspace protection takes not only the latest technological resources, but also great investment, since cybersecurity costs are constantly growing. If the goal is to reduce expenditures, investing in technological development of cybersecurity is not enough. At this point, state criminal policy should be focused on cyberspace protection from criminal encroachments using different means /**8**/, special programs for individualized prevention included.

When it comes to combating and preventing cybercrime, one holds to the regulation of personal content provision to individuals, as there is a real threat in cyberspace associated with the protection of personal data and intellectual property in the digital market. At the same time, rules securing the right to provide personal information for processing may violate the fundamental rights, freedoms and interests of a person sending it. Therefore, approaching cybernetics in combination with criminology achievements is an effective path to take when shaping the legal response to cybercrime /**27**/.

Cybercrime and its impact on information security, as well as specific measures against the phenomena that would approach at the individual level, were not considered at the level as fairish as needed . In particular, no specific actions to ensure cybersecurity were identified when studying the problem of countering cybercrime in business relying on information technologies (Internet resources), although this sphere is one those that are the most threatened by cyberattacks. It is worthwhile to agree with the probable positive impact that training sessions can have on shaping a defensive behavior from cybercrime among computer users – this will help to reduce victimization among these individuals /**28**/. This should also apply to home computers, as they are also often at risk of cybercrime /**29**/.

Another fact speaking for need of the most effective individualized measures against cybercrime is that this type of crime dominates among crimes against a person. Women are particularly vulnerable to such offences, although this is difficult to accept, as they equally encroach upon both men and minors /**30**/. These crimes also put public in danger by putting victimization on rise among people, especially teenagers, through intimidation /**31**/. This, in turn, creates a rather serious threat to modern society.

Another problem here is the elaboration of criminal measures aimed at ensuring cybersecurity of minors /**32**/. Taking into consideration the fact of how important is to ensure normal development of minors and their safety at all levels, this problem should be solved as quickly as possible. Thus, studies throw light on a right thing when illuminate the problem of protecting children from sexual corruption and exploitation (Kosovo case), characterized by such problem aspects as difficulty in identifying such crimes and their investigation. This problem can be solved only on condition that appropriate international and national legislation is established /**33**/. Designing special programs (such as that done in Nigeria) aimed specifically at combating cybercrime and its influence on minors is one of the most effective directions in this area /**24**/. Such programs should be designed with regard to national characteristics of each country, but since this problem is of an international character, we need a certain international program to be designed as a role model for national programs.

5. CONCLUSIONS

The above statistical data prove that we need individualized preventive measures against cybercrime. Although the overwhelming majority of data characterize the situation that takes place in some particular countries (the USA, Nigeria, China, Norway), they show general cybercrime and anti-cybercrime trends that are now gaining steam in the world.

Individualized preventive measures against cybercrime involve the creation of the so-called Cyberethics implying cyberculture improvement among people, especially children and teens, through educational and popular science projects. Such programs can be implemented by both governmental and non-governmental organizations. Such a preventive measure is proved to be needed once such-like program stroke positively in Nigeria. In the long run, it will boost cybercrime prevention

Aside from that, we need to put our hands on the most common phenomena and processes related to cybercrime: namely – to go for anti-criminalization, anti-bullying and anti-phishing propaganda, to shape negative attitude towards crimes, and discover responsibility for committing cybercrimes (identifying cybercrime determinants and developing regulatory tools against cybercrime). Such a measure is needed, as evidenced from statistical data on the progression of cyberbullying activity in social networks (Facebook – more than 80% of cases, while other 20% are attributed to other social networks (Instagram, Twitter, etc.). Society should be improved. Be that, we killing criminogenic factors that provoke a positive or neutral attitude towards cybercrime. These measures should also be undertaken by the relevant government bodies (law enforcement and judicial agencies) operating to improve the standards of living in social, economic, and political spheres. Statistical data were very informative when demonstrating that cybercrime growth depends not only on media and cyber technologies, but also on the overall level of life in the country: the highest rates were recorded in China (57.2%) and Taiwan (49.15%), while the lowest – in Norway (20.51%) and Finland (20.32%) /**23**/.

Individualized prevention is requirable among people who are more likely to commit crimes against cybersecurity. At this point, special criteria are needed to identify such persons. This will allow preventing such crimes before they take place. Special government (mainly law enforcement) bodies should undertake this measure. Such a measure proved to be relevant once the threat from phishing grew (by 36% in 2017), as well as the number of malicious programs (by about 230.000 per day).

Special programs must be designed for reducing cyber-victimization by shaping the ability to resist in individuals who can easily become victims of cybercrime (78% of people are aware of the risks that arise when opening unfamiliar programs or letters, but they still do it). Specific public authorities and non-governmental organizations should take part in designing these programs.

Undertaking these individualized measures as a single set to prevent cybercrime can significantly reduce the rates of cybercrime at the national level. At the international level, this will allow designing specific pilot programs for individualized cybercrime prevention.

Notes

/1/ Safa N. S., Solms Von R., Furnell S. (2016). Information security policy compliance model in organizations, *Computers & Security* Volume 56, pp. 70-82.

/2/ Paul P., Aithal P. S. (2018). *Cyber Crime: Challenges*, Issues, Recommendation and Suggestion in Indian Context.

/3/ Solak D., Topaloglu M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students, *Procedia-Social and Behavioral Sciences* Volume 182, pp. 590-595.

/4/ Choucri N., Madnick S., Ferwerda J. (2014). Institutions for cyber security: International responses and global imperatives, *Information Technology for Development* Volume 20, Issue 2, pp. 96-121.

/5/ Sun J. R., Shih M. L., Hwang M. S. (2015). A Survey of Digital Evidences Forensic and Cybercrime Investigation Procedure, *IJ Network Security* Volume 17, Issue 5, pp. 497-509.

/6/ Kraemer-Mbula E., Tang P., Rush H. (2013). The cybercrime ecosystem: Online innovation in the shadows?, *Technological Forecasting and Social Change* Volume 80, Issue 3, pp. 541-555.

/7/ Lagazio M., Sherif N., Cushman M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector, *Computers & Security* Volume 45, pp. 58-74.

/8/ Bernik I. (2014). Cybercrime: The Cost of Investments into Protection, *Varstvoslovje: Journal of Criminal Justice & Security* Volume 16, Issue 2.

/9/ Boone A. (2017). Cyber-security must be a C-suite priority, *Computer Fraud & Security* Volume 2017, Issue 2, pp. 13-15.

/10/ Mills A. J., Watson R. T., Pitt L., Kietzmann J. (2016). Wearing safe: Physical and informational security in the age of the wearable device, *Business Horizons* Volume 59, Issue 6, pp. 615-622.

/11/ McMahon R., Bressler M. S., Bressler L. (2016). New global cybercrime calls for high-tech cyber-cops, *Journal of Legal, Ethical and Regulatory Issues* Volume 19, Issue 1, pp. 26.

/12/ DeMatteo D., Wagage S., Fairfax-Columbo J. (2017). Cyberstalking: are we on the same (web) page? A comparison of statutes, case law, and public perception, *Journal of aggression, conflict and peace research* Volume 9, Issue 2, pp. 83-94.

/13/ Leppänen A., Kankaanranta T. (2017). Cybercrime investigation in Finland, *Journal of Scandinavian Studies in Criminology and Crime Prevention* Volume 18, Issue 2, pp. 157-175.

/14/ Silva K. K. (2018). Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting? *International Review of Law, Computers & Technology* Volume 32, Issue 1, pp. 21-36.

/15/ Couzigou I. (2018). Securing cyber space: the obligation of States to prevent harmful international cyber operations, *International Review of Law, Computers & Technology* Volume 32, Issue 1, pp. 37-57.

/16/ Tehrani P. M., Manap N. A., Taji H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime, *Computer Law & Security Review* Volume 29, Issue 3, pp. 207-215.

/17/ Taylor R. W., Fritsch E. J., Liederbach J., Saylor M. R., Tafoya W. L. (2019), Cyber Crime and Cyber Terrorism.

/18/ Robinson M., Jones K., Janicke H. (2015). Cyber warfare: Issues and challenges, *Computers & security* Volume 49, pp. 70-94.

/19/ Kaiser R. (2015), The birth of cyberwar, *Political Geography* Volume 46, pp. 11-20.

/20/ Omodunbi B. A, Odiase P. O., Olaniyan O. M., Esan A. O. (2016). Cybercrimes in Nigeria: Analysis, detection and prevention, *Journal of Engineering and Technology* Volume 1, Issue 1, pp. 37-42.

/21/ Wurtele S. K. (2017). Preventing cyber sexual solicitation of adolescents, *Prevention of Child Maltreatment. St. Louis, MO: STM Learning, Inc*.

/22/ Chandrashekhar A. M., Muktha G. S., Anjana D. K. (2016). Cyberstalking and Cyberbullying: Effects and prevention measures, *Imperial journal of interdisciplinary research* Volume 2, Issue 3, pp. 95-102.

/23/ Mason J. (2018). *Cyber Security Statistics.* Electronic resource: https://thebestvpn.com/cyber-security-statistics-2018/

/24/ Adewale A. P., Adedayo I. O., Raymond Ch. K-K. (2015). Impact of a participatory cyber crime prevention programme on secondary school students' attainment in crime prevention concepts in civic education and social studies, *Education and Information Technologies* Volume 20, Issue 3, pp. 505–518

/25/ Aggarwal P., Arora P., Ghai R. (2014). Review on cyber crime and security, *International Journal of Research in Engineering and Applied Sciences* Volume 2, Issue 1, pp. 48-51.

/26/ Berg van den B., Keymolen E. (2017). Regulating security on the Internet: control versus trust, *International Review of Law, Computers & Technology* Volume 31, Issue 2, pp. 188-205.

/27/ Somer T., Hallaq B., Watson T. (2016), Utilising Journey Mapping and Crime Scripting to Combat Cybercrime and Cyber Warfare At-

tacks, *Journal of Information Warfare* Volume 15, Issue 4, pp. 39-VI.

/28/ Mahmud I., Ramayah T., Nayeem M. M. H., Islam S. M., Gan P. L. (2017). Modelling Cyber-Crime Protection Behaviour among Computer Users in the Context of Bangladesh, In *Design Solutions for User-Centric Information Systems*, IGI Global, pp. 253-273.

/29/ White G. L. (2015). Education and prevention relationships on security incidents for home computers, *Journal of Computer Information Systems* Volume 55, Issue 3, pp. 29-37.

/30/ Kabir N. (2018). Cyber Crime a New Form of Violence Against Women: From the Case Study of Bangladesh.

/31/ Yu S. (2014). Fear of cyber crime among college students in the United States: An exploratory study, *International Journal of Cyber Criminology* Volume 8, Issue 1.

/32/ Näsi M., Oksanen A., Keipi T., Räsänen P. (2015). Cybercrime victimization among young people: a multi-nation study, *Journal of Scandinavian Studies in Criminology and Crime Prevention* Volume 16, Issue 2, pp. 203-210.

/33/ Dushi D. (2018). Challenges of protecting children from sexual abuse and exploitation on the internet: the case of Kosovo, *International Review of Law, Computers & Technology* Volume 32, Issue 1

I