REVISTA
SAN GREGORIO

http: 10.36097/rsan.v1i44.1580

Artículo Original

International Cyber Crime: Main Trends

Crime Cibernético Internacional: Principais Tendências

Author

Denis V. Puchkov

Candidate of Legal Sciences, Head of LOYS Law Office (Yekaterinburg), Email: d.puchkov@loys.law. https://orcid.org/0000-0002-4384-8461

Fecha de recibido: 2020-11-30
Fecha de aceptado para publicación: 2021-02-01
Fecha de publicación: 2021-03-25

Abstract

The subject of this article is global cybercrime. The relevance of the topic is increasing, as, globally, law enforcement agencies have noticed an increase in cyber crimes due to their use by organized individuals and criminal groups. The author comes to the conclusion that, in addition to the transformation of methods and techniques for committing cyber crimes, there is a change in the characteristics of cybercriminals themselves. In the article, the author notes that it is possible to observe major changes in the field of cyber threats against financial institutions and the emergence of new cybercriminal groups. Thus, even though there is consensus among most countries in the world as to the importance and relevance of combating cyber crime, which presupposes a constant and coordinated response, this problem in itself cannot be described within quantitative limits in the same way as various forms practical implementation. of cybercrime in the world cannot be described either.

Keywords: family life, private life, European Court of Human Rights, state, grounds for interference.

Resumen

O assunto deste artigo é o cibercrime global. A relevância do tema está aumentando, uma vez que, em nível global, as agências de aplicação da lei notaram um aumento nos crimes cibernéticos devido ao uso deles por indivíduos e grupos criminosos organizados. O autor chega à conclusão de que, além da transformação dos métodos e técnicas de cometimento de crimes cibernéticos, há uma mudança nas características dos próprios cibercriminosos. No artigo, o autor observa que é possível observar grandes mudanças no campo das ameaças cibernéticas contra as instituições financeiras e o surgimento de novos grupos cibercriminosos. Assim, mesmo que haja consenso entre a maioria dos países do mundo quanto à importância e relevância do combate ao crime cibernético, que pressupõe uma resposta constante e coordenada, este problema em si não pode ser descrito dentro de limites quantitativos da mesma forma que várias formas de implementação prática. do cibercrime no mundo não pode ser descrito também.

Palabras clave: vida familiar, vida privada, Tribunal Europeu dos Direitos do Homem, estado, motivos de interferência

Introduction

The use of the Internet and business networks is rising as cybercrime rises. Today organizations of all sizes rely more than ever on the company's networks, data and internet access. The internet's economic influence among "private customers and small start-up companies" is according to a study from the McKinsey Global Institute. Even the smallest businesses may be internationally affected by the Internet. What started as a dark network of scientists a few decades ago has evolved into an e-commerce business with a network of more than two billion people for $8 billion a year.

To date, the process of technical and technological development has transformed cybercrime into a fairly serious and widely branched business, thanks to which revenues are obtained compared to those obtained from drug trafficking (Chandra & Snowe, 2020). The ongoing process of attracting persons with special knowledge in such illegal actions in a rather specific area, to which cyber technologies and, in fact, hackers themselves, are involved, is becoming an integral part of the fight against organized criminal activity around the world.

The further rapid development of information and communication technologies (ICT), globalization, a sharp increase in data volumes and an increase in the number of different types of equipment connected to data transmission networks have an impact on daily life, the economy, and the general functioning of the state. On the one hand, this level of ICT development will contribute to an increase in the level of accessibility and usability of services, increase the transparency of citizens' participation in governance, and also reduce the costs of the public and private sectors. On the other hand, the increase in the importance of technical innovations is accompanied by an increase in the state's dependence on an already rooted electronic algorithm and hinders the consistent development of new technologies. In addition, the Internet is becoming more accessible; the number of users continues to grow, and the number of potential attack vectors, along with their complexity, is increasing with new technological solutions and services such as the Internet of Things and cloud computing (Aazam et al., 2014; Díaz et al., 2016; Tao et al., 2014; Zhou et al., 2013).

At the same time, there are grounds for understanding that due to the increasing influence of information technologies on NBIC convergence, the procedure for transforming the technological mode for a person and society as a whole will be an extremely fast process as to its historical standards. Humanity can expect greater progress in the study of the laws of social structures since the increasing autonomy of individuals will inevitably lead to the emergence of new communities, ethical criteria and social norms. Such forecasts are based on the capabilities of technologies ranging from research projects to date to the expected forecasts of current scientific long-term strategies.

The radicality of cyber technologies as new technologies is determined by whether they create a new type of functioning or only facilitate the implementation of already formed institutions. The scale of the use of new technology is associated with how many agents perform the types of activities it provides; what are the roles and place in the social system of these institutions that determine the transformation of the existing technological mode. According to studies, "the replacement of technological paradigms requires, as a rule, appropriate modifications in institutional and social systems, which not only alleviate social tension but also contribute to the massive introduction of technologies of the latest technological mode corresponding to its lifestyle and type of consumption." At the same time, it becomes obvious that the implementation of the latest opportunities for civilizational development, which are opening up due to the convergence of bio-, nano-, info- or cognitive technologies, will almost inevitably lead to radical social, cultural and ideological changes. This also applies to the revision of traditional ideas about basic, fundamental concepts such as mind, life, man, existence, and nature.

Today, humanity has to understand that in the real world, there are no clear boundaries between various phenomena previously considered dichotomous. In the light of modern developments that are associated with the formation of cyber technologies, the traditional criteria for distinguishing the living from the non-living are losing their meaning; the boundaries between man as a living being endowed with consciousness and a human-sized programmable technical system are smoothly blurring; our ideas about death and birth, about the facets of "humanity" are being modified, being tied in many respects to the essence of cyberspace.

Rise of cybercrime

The main threat to cybercrime and its growth is currently manifested in the significant development of the skills of cybercriminals and their increased ability to conduct organized attacks. At the same time, an important part of the registration of crimes is the collection and processing of digital evidence, which are new challenges to the procedural and digital forensic capabilities of the police. It is significant that national cybersecurity depends to a certain extent on actors operating in cyberspace

with their different skills, goals and motivations. It is often difficult to distinguish between criminals and decent users of the global Internet or to determine their criminal ties with national or international organizations (R. I. Dremliuga et al., 2017). However, the activity of states capable of cyberattacks is growing. For example, states have increasingly begun to engage cyberspace actors involved in cyber espionage, which aims to "crack" specific computers connected to the Internet, as well as hack closed networks in order to collect information about both national security and economic data for entire countries.

At the global level, law enforcement agencies have noted an increase in cybercrimes due to the use by individuals and organized criminal groups, the main purpose of which is to generate significant profit, and new opportunities for committing cybercrimes. According to analysts, over 80% of such crimes were committed by various methods and means of organized crime using the capabilities of the existing cybercrime "black market", for example, the development of malicious programs, including computer viruses, unauthorized management of botnets, and collection of personal and financial data, their subsequent sale and receipt of significant monetary assets for classified information (Clough, 2015).

In addition to the transformation of the direct methods and techniques targeted at committing cybercrimes, there is also a change in the characteristics of the cybercriminals themselves. At the initial stage of the development of cyber technologies, these were people who had special knowledge and skills; they were driven by the desire to search for something new. At present, these are people pursuing certain criminal goals, often selfish and aimed at especially large thefts and, accordingly, forming criminal communities. At the same time, a certain hierarchy is formed among such specialists, ranging from those who received a ready-made algorithm that ensures the implementation of a certain order of actions and uses it, and up to persons who have very deep knowledge in this rather specific area, or a kind of cybercrime elite. It is important to note that committing simple cybercrimes does not imply certain complex skills or knowledge when using complex methods. These ready-made algorithms have contributed to the emergence of a subculture of young people (R. Dremliuga, 2014) who engage in financial fraud using computers according to ready-made criminal schemes (Donegan, 2019). Moreover, many of them began to engage in this type of crime as early as adolescence (Osipenko, 2004).

New challenges

The hardware and software infrastructure continues to develop rapidly and the number of users of the shadow Internet networks, or DarkNet, is growing (Chaudhry, 2017; Mirea et al., 2019; Norgaard et al., 2018; Van Buskirk et al., 2016; Wood, 2009). This is the basis for an increase in the volume of crime related to the sexual exploitation of young people and children. At the same time, organized cybercrime has discovered a new criminal "Klondike" in the last two years, associated with the search, professional processing, and distribution of self-generated indecent content. The content authors are the children themselves. In addition, the volume of video content related to child abuse and other types of paedophile perversion is growing. An international transcontinental network is being formed connecting DarkNet, anonymous payment systems and encrypted traffic protocols, serving the paedophilia and child abuse market. Asian, Latin American and partly African countries act as content providers; North America and the EU countries are its consumers, and the states of Eastern Europe and the post-Soviet space are operators and part owners of this market.

Many of the main cyber threats remained in 2017-2018, unchanged comparing with previous periods (Guiney, 2020). This, in particular, applies to ransomware, petty theft using malicious software, the use of banking Trojans, etc. At the same time, the previously listed types of simple cybercrime, which is a kind of "street" one, did not dissolve in high-tech crime, but continue to grow in volume and get younger in age. It seems that this trend will continue for several more years until the criminal market in these segments reaches the equilibrium level.

Cybercriminals today are mostly focused solely on quick financial gain. In addition to causing direct financial losses, their activities can damage brands and lead to both fines from regulators and legal proceedings. Criminals effectively interact and share information with each other. The tools used by organized crime include anonymous marketplaces and "card" forums (where credit and debit card data and personal data are traded).

The trend of recent years has become the facts of corporate crimes, especially in the financial sector, where cybercrimes were not exclusive, but one of the criminal tools along with corruption and the use of social engineering methods. Hacker attacks have become more complex and professional in nature; they not only began to be directed at individual users but also set themselves large industrial systems as targets. Based on the results of research by Juniper Research company, even with the current level of cyber-attacks, the global economy could suffer total losses from the activities of cybercriminals in the amount of up to $ 2.1 trillion in the period until 2019.

It should be noted that most of the cyber-attacks registered in 2016-2017 are neither sophisticated nor advanced and refer to a kind of “street cybercrime” that exploits the blatant illiteracy of individual and corporate users. At the same time, in some areas, cybercriminals demonstrate the highest software, technical and organizational level using highly innovative approaches and tools. So, for the first time in a long period, they managed to successfully attack the international system of fast bank transfers SWIFT, as well as the NFC of several issuers. In addition, the volume of fraudulent activities related to ATM servicing and criminal disruption of the traffic of e-commerce payment systems continues to increase, primarily related to air tickets, car rental and payments for travel packages. For example, in 2017, Kaspersky Lab experts uncovered attacks on ATMs that used a new malware for remote control of ATMs and malware for attacks against ATMs called Cutlet Maker, which was openly sold on the Darknet market for several thousand dollars (with attached step-by-step user manual included).

In 2015-2018, most countries saw a marked increase in the number of cyberattacks against private and business networks. In most attacks, cybercriminals used already well-known tools and services to hack gadgets and networks. The largest number of attacks were carried out using password ransomware programs, spyware, and programs that compromise secure payment systems protocols. The most visible threat from malware is the use of password ransomware. The damage from these programs has eclipsed even the use of banking Trojans. The use of password ransomware programs causes approximately the same damage to both business and private users. Currently, there are two fundamentally different approaches to using ransomware. While young cybercriminals use ransomware as self-sufficient, small hacker groups combine the use of ransomware with a different type of software. As a rule, in such cases, ransomware is used to gain access to personal accounts, followed by the introduction of spyware, and then "software" that allows them to redirect payments.

Currently, we can see great changes in the field of cyber threats against financial institutions and the emergence of new cybercriminal groups. Attackers are increasingly targeting accounts of the financial service user. Personal data is the primary target of large-scale malicious attacks, and frequent data leaks provide cybercriminals with valuable information that they use to manipulate bank card numbers or attacks using a fake identity. Attacks on user accounts can lead to other serious problems, including further leaks of customer information and loss of their trust, so minimizing negative consequences is more important than ever for both business and financial services customers.

Cybercrime and cybersecurity are issues that can hardly be separated in an interconnected environment. The fact that the UN General Assembly resolution on cybersecurity considers cybercrime as one of the main problems only underlines the urgency of this problem. Cybersecurity plays an important role in the continued development of information technology as well as Internet services. Enhancing cybersecurity and protecting critical information infrastructures is essential to the security and economic well-being of each country, and therefore ensuring the security of the Internet (and protecting Internet users) has become an integral part of the development of new services as well as government policy.

In this sense, the use of a technological and legal approach in the field of cyber technologies will help not only to widen the digital divide, especially if we add a second “security division”, but also to quickly create a reliable infrastructure that meets the needs of international development. However, it should be recognized that cybersecurity tools and legal frameworks pose additional challenges for the country's development. It is the responsibility of developed countries to find their own best practice through the transfer of practical knowledge and skills. In doing so, everyone has a responsibility to ensure a safe and secure cyber environment in the context of the emerging information society. The minimum level of security for information and communications technology must be provided at an affordable cost. In this case, security should not become an exclusion factor for those who would like to conduct private or business activities over the Internet.

There is now widespread concern about the explosion in the number of digital devices; additional vulnerabilities arise due to increased "use" of digital users; security issues are caused by the move to mobile and cloud applications; there is also the alarming growth of new malware components, a rising curve of incidents related to cybercrimes, which imposes enormous costs on national economies, corporations and individual digital users; and also there is an emergence of even more powerful international crime syndicates willing and able to engage in cybercrimes and cyber conflicts for hire. As noted above, the combination of these circumstances represents a new factor, if not a qualitative leap in cyber threats, that could further undermine cyber confidence.

Upon that, the sources of the potential risk to cyber stability and cybersecurity include the increasing complexity and increasing use of ICT infrastructures and services. Even more serious are threats from external events, such as natural disasters or attacks by governments, criminal organizations or individuals. Research has shown that even designers, operators and users of systems

can, intentionally or unintentionally, become a major source of ICT vulnerability. In this regard, the main scientific and technical problems associated with the issues of "complexity, emergency situations, resilience" in cyberspace must be resolved.

Human actions that pose a real threat can be carried out either intentionally (for example, insiders, hackers) or unintentionally, as a result of the work or behaviour of a user. The risk analysis should identify the most likely human actions causing harm and analyse the resulting vulnerabilities. In addition to vulnerabilities and threats, the analysis of cyber risks should take into account their impact on the capabilities and resources of the system, as well as the value of the corresponding resources. A threat, in this case, is understood as "a potential hazard in which a vulnerability can be used to compromise security and cause harm. Therefore, there must be taken into account and evaluated additional threats, which are caused by the actions of a human user with the system resources, incidents, natural disasters or other unexpected external events."

In a world where people are so dependent on cyber resources, the analysis of risk and resilience in cyberspace must take into account a range of dimensions, spanning both animate subjects and the diversity, and complexity of the digital age. The spectrum of cyberspace resources ranges from global digital infrastructures and services that can be used around the world and up to individual computing or cyber-physical devices. Also, it is necessary to distinguish between the roles of the people and their ability to use digital systems as either knowledgeable persons (insiders) or outsiders in relation to their activities in cyberspace, such as designers, developers or users.

The Internet being specifically used to destroy reputations, to influence people, groups and leaders, to spread misinformation and to manipulate opinions, is becoming a battleground for valuable information. At the same time, information technologies open up opportunities for malicious organizations and criminal organizations to increase their effectiveness, giving vent to their unlimited and immoral fantasies and waging new types of wars in cyberspace, including information wars. Failure to recognize this reality means unjustifiably exposing oneself to the potential loss of economic competitiveness, stability, national sovereignty and international confidence. The media, as well as industry professionals, report an endless series of large-scale data thefts at enterprises, successful cyberattacks or the capture of information resources for ransom.

Also, activities related to countering planned or ongoing cybercrimes were carried out not only at the level of an individual state but also by their blocks, for example, NATO. In particular, the significance of this problem is indicated in almost all documents of the block, which have a systemic nature and have been adopted in recent years. Thus, for the first time, the strategic concept of NATO contained a provision regarding cyberspace as a new area of military activity of this alliance (Efthymiopoulos, 2019; Eldem, 2020; Shypovskyi et al., 2020; Sz\Hoke, 2019).

The development of adequate legislation and (within the framework of this approach) the development of legislative ways to combat cybercrime is an integral part of the overall strategy for ensuring cybersecurity, including access for humans. This implies, first of all, the need to develop basic provisions of criminal law to criminalize acts related to cyber technologies, such as computer fraud, copyright infringement, illegal access, data interference, cyber terrorism, crimes in virtual reality (R. Dremliuga, Iakovenko, et al., 2019; R. Dremliuga, Kuznetcov, et al., 2019; Hänel, 2020; Sparrow, 2019; Strikwerda, 2015), AI-assisted crimes (Roman & Natalia, 2019), and child pornography. The fact that provisions giving a criminal-legal assessment of such acts exist in the criminal code and are applicable to such acts committed outside the network does not mean that they can also be applied to acts committed via the Internet. Therefore, a thorough analysis of the current regulatory provisions is vital to identify any possible gaps in this area.

Conclusions

Thus, even if there is general agreement among most countries of the world regarding the importance and relevance of the fight against cybercrime, which presupposes a constant and coordinated response, this problem itself cannot be described within quantitative boundaries, as various ways of practical implementation of cybercrime in the world cannot also be described. Nevertheless, it has become an overriding form of the struggle presenting today unique challenges and a special need for international cooperation, as, for example, in the fight against drug trafficking. Despite the fact that a number of agreements on mutual legal assistance already exist and are in force, there is a pressing need to improve procedures for an adequate response to acts of cybercrime, especially at the international level and, accordingly, in the form of international cooperation in the fight against these phenomena.

References

Aazam, M., Khan, I., Alsaffar, A. A., & Huh, E.-N. (2014). Cloud of Things: Integrating Internet of Things and cloud computing

and the issues involved. *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014*, 414–419.

Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, *38*, 100467.

Chaudhry, P. E. (2017). The looming shadow of illicit trade on the internet. *Business Horizons*, *60*(1), 77–89.

Clough, J. (2015). Towards a common identity? The harmonisation of identity theft laws. *Journal of Financial Crime*.

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer Applications*, *67*, 99–117.

Donegan, M. (2019). Crime script for mandate fraud. *Journal of Money Laundering Control*.

Dremliuga, R. (2014). Subculture of hackers in Russia. *Asian Social Science*, *10*(18), 158.

Dremliuga, R. I., Korobeev, A. I., & Fedorov, A. V. (2017). Cyberterrorism in China: Criminal law and criminological aspects. *Russian Journal of Criminology*, *11*(3), 607–614.

Dremliuga, R., Iakovenko, A., & Prisekina, N. (2019). Crime in virtual reality: Discussion. *2019 International Conference on Cybersecurity (ICoCSec)*, 81–85.

Dremliuga, R., Kuznetcov, P., & Mamychev, A. (2019). Criteria for Recognition of AI as a Legal Person. *J. Pol. & L.*, *12*, 105.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1), 1–26.

Eldem, T. (2020). The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security. *International Journal of Public Administration*, *43*(5), 452–465.

Guiney, T. (2020). Excavating the archive: Reflections on a historical criminology of government, penal policy and criminal justice change. *Criminology & Criminal Justice*, *20*(1), 76–92.

Hänel, H. C. (2020). *Problems of conceptual amelioration: The question of rape myths*.

Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: A qualitative study. *Security Journal*, *32*(2), 102–118.

Norgaard, J. R., Walbert, H. J., & Hardy, R. A. (2018). Shadow markets and hierarchies: Comparing and modeling networks in the Dark Net. *Journal of Institutional Economics*, *14*(5), 877–899.

Osipenko, A. L. (2004). The fight against crime on a global computer network: International experience: monograph. M. *Norma*, 432.

Roman, D., & Natalia, P. (2019). Artificial Intelligence Legal Policy: Limits of Use of Some Kinds of AI. *Proceedings of the 2019 8th International Conference on Software and Computer Applications*, 343–346.

Shypovskyi, V., Cherneha, V., & Marchenkov, S. (2020). Analysis of the ways of improvement of Ukraine–NATO cooperation on cybersecurity issues. *Journal of Scientific Papers «Social Development and Security»*, *10*(2), 11–15.

Sparrow, L. A. (2019). The moral (im) permissibility of groping in virtual reality games. *DiGRA Australia. The University of Sydney, Australia. Retrieved from Http://Digraa. Org/Wp-Content/Uploads/2019/01/DIGRAA_2019_paper 9. Pdf*.

Strikwerda, L. (2015). Present and future instances of virtual rape in light of three categories of legal philosophical theories on rape. *Philosophy & Technology*, *28*(4), 491–510.

Sz\Hoke, D. (2019). NATO's Evolving Approach to Cybersecurity. *Foreign Policy Review*, 128.

Tao, F., Cheng, Y., Da Xu, L., Zhang, L., & Li, B. H. (2014). CCIoT-CMfg: Cloud computing and internet of things-based cloud manufacturing service system. *IEEE Transactions on Industrial Informatics*, *10*(2), 1435–1442.

Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R., & Burns, L. (2016). Who sells what? Country specific differences in substance availability on the Agora cryptomarket. *International Journal of Drug Policy*, *35*, 16–23.

Wood, J. A. (2009). The Darknet: A digital copyright revolution. *Rich. JL & Tech.*, *16*, 1.

Zhou, J., Leppanen, T., Harjula, E., Ylianttila, M., Ojala, T., Yu, C., Jin, H., & Yang, L. T. (2013). Cloudthings: A common architecture for integrating the internet of things with cloud computing. *Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 651–657.