Advances in Economics, Business and Management Research, volume 81
1st International Scientific Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2019)

Crime counteraction in the digital environment as a factor of the development of high technology

Chirkov M.A.
Moscow State University named after M.V. Lomonosov
Moscow, Russia
Email: mospil@mail.ru

Abdryashitova A.I.
Russian Presidential Academy of National Economy and Public Administration (RANEPA)
Vladimir, Russia
Email: ani-abdryashitova@yandex.ru

Chistyakov M.S.
Institute of Economics and Management, Vladimir State University named after Aleksandr Grigorevich and Nikolai Grigorevich Stoletovs
Vladimir, Russia
Email: shreyamax@mail.ru

***Abstract* — In this work, on the basis of a brief analysis of the fundamental factors of the evolution of criminal manifestations in the digital space, measures to leveling the consequences of cybercrime are considered. The research focuses on a certain disproportionate disconnecting of counteraction to digital crime at the international and national levels. The authors attempted to integrate the definition of "digital neglect" into the information and communication use in order to explain the processes occurring in the digital environment, including indirectly generated by the actions of "digital criminals". The problem of a psychological nature is analyzed - "immersion into a digital environment", which is a catalyst of the denial of traditional culture and values, destructive disharmony of personality and society.**

Keywords — the sixth technological order, changes in the technological sphere, activity in the information environment, digital technologies, multilateral partnership, the development of narrow-purpose specializations.

I. Introduction

Modern civilization is a witness of truly momentous changes in the technological sphere, which modify the course of the geopolitical and geoeconomic processes of the modern world order. This trend completely correlates with the theory of academician S.Yu. Glazyev, according to which, the growth of the sixth technological order, which core is formed by nanotechnologies that fundamentally modify and increase the efficiency of the evolution of the digital economy, is actively occurring.

At the same time, in parallel with these revolutionary technological transformations, that entailed the development of the digital industry and information and communication technologies, there occurred processes that contributed to the evolutionary transformations of the criminal orientation of not only individual states but also the entire civilized world. The boundless expanses of the information latent space were adopted by criminal elements as an environment (space) and a means of committing various illegal acts. These include manipulations from traditional fraud and encroachments on property to high-tech and multi-episode techniques (covert extortion, sale and distribution of confidential information, fraudulent schemes in the gamer industry, turnover of goods and services that are non-legal in legal law turnover. The growing trend of growth of increase of cyber extremism, and especially - its extreme form - cyberterrorism causes particular anxiety [2,42].

II. Research Methodology

Theoretical research methods based on the logical knowledge of the essence of certain phenomena of the surrounding reality prevail in the work. The basis of the empirical part of the research consists of the facts presented in the scientific literature, as well as empirical generalizations. The prevailing method of analysis is induction since the task of the authors is to obtain general conclusions based on the facts available in scientific sources on the subject of the research.

According to experts assessments, over 3 million offenses are committed annually on the Internet (850 thousand of which are sexual crimes, 144.5 thousand are connected with hacking computers, 207 thousand are connected with financial manipulations) [4,6], which is estimated by various specialists to cause significant harm not only economic but also the public interests [5, 3-4]. It is noted that the level of crime in the information space is largely determined by the specifics of the criminal law of a particular state, depends on activities in this direction and the ability of law enforcement agencies to implement measures to counter the criminal world.

In this perspective, the Russian Federation is among the states that are not sufficiently protected from threats of information-aggressive nature. The Russian legal system and legislation, in particular, are poorly adapted to confrontation with cybercrime and the challenges of the "digital age", due to insufficient attention to the regulation and coordination of the protection of public relations in the information and communication plane. These circumstances led to the low resistance of national legislation, to new manifestations of illegal actions using information and communication technologies. Responsibility for them is provided for by

Chapter 28 of the Criminal Code of the Russian Federation "Crimes in the sphere of computer information" (Article 272 of the Criminal Code of the Russian Federation (Illegal access to computer information), Article 273 of the Criminal Code of the Russian Federation (Creation, use and distribution of harmful computer programs) and Article 274 of the Criminal Code of the Russian Federation (Violation of the rules for the operation of means of storage, processing or transmission of computer information and information and telecommunication networks)), Art. 159.6 of the Criminal Code of the Russian Federation (fraud in the field of computer information) and art. 187 of the Criminal Code of the Russian Federation (Illegal turnover of funds of payments) [3, 202]. Analysis of the legal basis for the qualification of acts in the field of cybercrime suggests that they include a small range of mercenary manipulations in the field of information and communication relations. Cybercrime statistics is presented in Table 1.

TABLE 1. DYNAMICS OF CYBERCRIME IN RUSSIA IN THE PERIOD 2010-2016

Crimes, under	2010	2011	2012	2013	2014	2015	2016
Ch. 28 of the Criminal Code of the RF	7,398	2,698	2,820	2,563	1,736	2,377	2,570
including:							1,443
Art. 272	6,309	2,005	1,930	1,799	1,150	1,395	1,124
Art. 273	1,089	693	889	764	583	970	3
Art. 274	0	0	1	0	1	13	
Art. 159.6 of the Criminal Code of the RF	-	-	-	693	993	5,442	5,380
Art.187 of the Criminal Code of the RF	-	-	-	-	-	-	234
Total criminal offenses in the Russian Federation	2,628,799	2,404,807	2,302,168	2,206,249	2,190,158	2,388,476	2,160,063

Source: [3,202]; http://crimestat.ru/offenses_map

The researchers note that there is a steady tendency to increase the number of criminal proceedings under Art. 159.6 of the Criminal Code of the Russian Federation, which indicates the presence and manifestation of serious contradictions in the investigation of criminal acts, committed with the use of information and communication format technologies.

Transparency of the information environment allows criminals to carry out their actions within the legal environment of the state, which is most comply with criminal intentions and optimizes their manipulations to implement the planned illegal actions, that meet their goals with the least possible negative consequences for them. So-called “information harbors (shelters)” are a control element in the counteraction to crime in the digital space, which is a consequence of the inhibition of the all-round development and transfer of high technologies in the legal field.

As a victim provocative format of cybercrime, it is necessary to note the so-called. “Digital homelessness (neglect)”. “Digital homelessness” is a new metaphor that allows you to voice the fullness of the threat for information and national security through the disclosure of the mechanism of the processes occurring in the world wide web. “Digital homelessness” carries the danger of desocialization and destruction of the personality, involution (reduction), accelerated maturation and psychological aging as a result of chronological disproportionate entry into information resources intended for a different age audience. As a result of low “digital culture”, society faced manifestations of “digital dependence”, “cyber dependence”, “digital dementia”, etc. Scrappy consciousness formed by the digital world (digital reality) becomes the foundation of mosaic identity, leading to gaps in awareness of the individual in the world civilization structure of society, potentially capable to become the primary source of conflict situations and problems in the relationship between the individual and society in the era of digital transformational changes.

One of the characteristic features of the modern stage of development of digital technologies is exactly the informational impact on the public and individual consciousness, incl. in the most aggressive forms - up to open and hidden information wars.

Social engineering, as one of the tools to influence the psyche in the digital age, is an aggregated synthesis of various methods of influencing a person for the purpose of unauthorized penetration into protected information environment. Indeed, in the era of increasing digital development, information is an expensive and strategic resource, that attracts the attention of the corrupt part of the community.

Group crime in synergy with information technology gets unique, peculiar to the digital environment, properties and forms. Among foreign scientists, the prevailing view is that these groups regress the sign of cohesion. Instead, in the digital space, an ephemeral configuration of interaction — criminal mega-networks — is being formed. Visitors of forums, social networks, chat rooms, covert online communities are involved in them as active residents [8]. However, in order to enter this community, it is necessary to gain the trust of the members of this group. In addition, it is advisable to have a status position and reputation, recommendations. In this regard, it is not entirely clear whether the functioning of this kind of virtual criminal configuration is less stable than contacts in the criminal community of the classical type [6].

The problem of “Internet addiction”, which is a provoking victimological factor, along with other dependencies (“telemania”; “game addiction”, including gemblig, etc.) should be under the supervisory and analytical control of the relevant public services and public organizations, since it carries a threat for the health of the nation, and therefore is dangerous to the national self-preservation of the state. Supervisory control measures will help to counteract the

significant and rapid critical spread of harmful digital distribution.

The formation and development of digital dependence are associated not only with the demand for a different identical reality but also with the totality of individual personality characteristics. Among the digital addictions are: obsessive Internet surfing (continuous search for information on the Internet), virtual communication and cybersex (dependence on porn sites), passion for online stock trading and online gambling, computer network games [1,105]. Digital space, which "brings" a lot of advantages to everyday life, is a "harbor" of latent threats, a source of decreasing resistance to habituation (addiction) and addictions of various formats (character), which, in turn, are an element of the trigger mechanism of consequences of the victim order.

Since the overwhelming majority of economic crimes are committed in the so-called inter-country space - on the world wide web, crime in the digital economy is a cross-border process. In this regard, it is advisable to develop supranational cooperation in the field of confronting the expansion of the influence of digital crime. In countering cybercrime, an international approach provide for the consolidation of the efforts of law enforcement agencies of various states, the formation of special units whose activities are aimed at struggling crimes in the digital space. The specific nature of cyber frauds imply not isolated state confrontation in solving the increasing problem of digital crime, but effective counteraction against it when activating international cooperation and combined efforts of various organizations. The fight against cybercrime in modern reality is carried out by the following structures:

1. International Multilateral Partnership Against Cyber Threats (IMPACT) is the executive authority in the field of cybersecurity of a specialized UN agency, bringing together the efforts of many states, non-governmental organizations, as well as experts in the field of information security;

2. International Cyber Security Alliance (ICSPA), which unites law enforcement agencies, including Europol, international business and governments of many countries of the world (Australia, Great Britain, Canada, New Zealand, USA, etc.);

3. The International Criminal Police Organization (Interpol), which ensures a fast and effective mechanism for communication coordination between states, Interpol itself in the process of international efforts to find, identify and register criminal elements, etc.

The activity of these organizations are aimed at developing standards for cyber acts of a united international format that must be criminalized and have significant specific differences in different states; the formation of a united terminological apparatus and conceptual toolset; assistance in providing advisory help at the national level [7, 147].

It should be noted that there is some disunity in the activities of subjects of the digital crime prevention sphere, which is explained by the specifics of ensuring national security and the sovereignty of states; differences in legislation, incl. legal support of the structures activities in the direction of cybersecurity, the organization of countering to digital arbitrariness; various financial, economic and technological potential of states, etc. Political controversies and geopolitical opposition of the Russian Federation and the states of the "Anglo-Saxon world" make a contribution. Disunity in this aspect is a significant factor in countering the spreading of cyber threats to the national security of states.

III. Results of the Research

An international approach means the use of a legal approach, which means the improvement and verification of legal mechanisms at the national and international levels to counteract acts in the field of digital communications. In this regard, a complex of intergovernmental measures is needed to organize and implement measures aimed at leveling cyber attacks and their consequences:

1. Unified coordination of national legislation on crimes in the digital sphere;

2. Formation at the international level with the subsequent implementation of procedural toolset, that would allow to carry out investigations consolidatedly and effective on the fact of the committed criminal acts in the digital space, on the intrastate format;

3. The development of rapid response practices at the international level in response to criminal actions in information networks;

4. The adjusted mechanism for reviewing and solving issues related to different jurisdictions, necessary to implement actions regarding committed cybercrime.

IV. Discussion of Results

Thus, measures in this segment of jurisprudence in the international format are the determining factor in minimizing of legal gaps that were formed as a result of asynchrony in the development of digital technologies and the legislative acts that are resistant to them.

The national level also involves the improvement of the legal norms against digital format crime. Presidential Decree No. 1274 of 12.12.2014 "On the Concept of the State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks on Information Resources of the Russian Federation" defines the purpose of the state system of detection, prevention and elimination of the consequences of computer attacks (SOPKA). This system is a united centralized, territorially-distributed complex, which includes the forces and means of detecting, preventing and eliminating the consequences of computer attacks, the federal executive body authorized to ensure the security of the critical information infrastructure of the Russian Federation (a unit of the FSB of Russia). In addition, the Concept involves the creation of a system of special centers to ensure cybersecurity, including the main and regional centers, as well as the centers of state bodies of Russia and the subjects of the Russian Federation. Thus, a system of protection against cyberthreats of state authorities and financial institutions is being created at the state level.

The technical approach involves the prevention of cybercrime through the implementation of technical measures to ensure security in the information sphere, as well as the formation of the material and technical base of units to struggle with cybercrime, based on the principle of "the most modern" [9,188].

V. CONCLUSIONS

Digital crime prevention should include a range of victimological measures in various age groups and stratums of the population. It is necessary to carry out the development of narrow-purpose specializations in legal and economic universities, especially educational institutions of power ministries and departments. It is advisable to focus on the detection of victimological patterns in the commitment of cybercrime in order to detect objective trends and characteristics of the implementation of illegal acts, directed, in particular, to the unprotected stratums of the population; determinants provoking illegal acts using digital technologies; differentiation of certain personality types of criminal elements, as well as the development and improvement of additional digital security mechanisms.

Generality of problems of confronting digital crime in Russia and abroad allow to suggest the need for measures to analyze, synthesize and accumulate the positive experience of high-tech development states (Great Britain, Germany, Denmark, Norway, Switzerland, etc.) that succeeded not only in the development of an innovative economy but also have significant achievements in preventing the use of high technology for illegal mercenary use.

References

[1] Arpentieva M. R. Security Issues in the Internet: digital homelessness as a cause of digital addiction and digital crime // Bulletin of the Prikamskiy social Institute. 2017. No. 3 (78). P. 99-110.

[2] Brazhnikov D., Shiyan V. I. Main criminal threats to state and public security // Investigation of crimes: problems and solutions. 2016 No. 4. P. 41–46.

[3] Goncharova M. V. Prevention of cybercrime // materials of all-Russian scientific-practical conference "Criminal liability and punishment" dedicated to the memory of professors of the Department of criminal law of the Ryazan higher school of the Ministry of internal Affairs of the USSR V. A. Olive and N. Ogurtsov / Under the editorship of V. F. Lapshin. - Ryazan, February 17, 2017, P. 200-206.

[4] Komarov: Criminological aspects of fraud in the global Internet. Diss. PhD. Faculty of law. Pyatigorsk, 2011. 262 p.

[5] Lapshin, V. F., Crimes in the sphere of distribution of financial resources: issues of differentiation of liability and legislative techniques. Diss. PhD. Faculty of law. Kazan, 2004. 24 p.

[6] Leukfeidt E.R. Organised cybercrime and social opportunity structures: a proposal for future research directions / E.R. Leukfeidt // The European Review of Organised Crime. - 2015. - No. 2. - P. 91-103.

[7] Moroz N. O. Activities of Interpol to coordinate cooperation in the fight against crime in the field of high technology // Bulletin of Polotsk state University. Series D. Economic and legal Sciences. 2011. No. 14. P. 143-148.

[8] Organizations and cyber crime: an analysis of the nature of engaged in cyber crime / R. Broadhurst, P. Grabosky, M. Alazab, S. Chan // International Journal of Cyber Criminjlogy. - 2004. - Vol. 8, iss. 1. - P. 1-20.

[9] Romanenko A. S. Some aspects of the fight against cybercrime // Actual problems of law, Economics and management. 2015. Vol. XI. P. 187–188.Chirkov Maxim Andreevich

PhD in Economic sciences, Associate Professor, Associate Professor of the political economy department, Lomonosov Moscow State University, Moscow, E-mail: mospil@mail.ru