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)

Criminal legal background of cyberspace management

Puchkov D.V.
Ural State Law University
Yekaterinburg, Russia
d.puchkov@loys.law

Goncharov D.Yu.
Ural State Economic University
Yekaterinburg, Russia
goncharov_d@mail.ru

***Abstract* — The article deals with the problem of criminal law prerequisites for managing cyberspace. The author notes that the increasing complexity and the increasing use of cybertechnologies and infrastructures are sources of potential risk to cyberstability and cybersecurity. More serious are the threats posed by external events, such as natural disasters or attacks by governments, criminal organizations or individuals. However, the expansion of cyberinfrastructure and cyberservices will provide greater opportunities and benefits, but will also lead to additional vulnerabilities and new challenges that could undermine personal and public security and safety of our societies. The author points out that at present the development of information and communication networks makes it necessary to consider the issues of information security not only at the international level, but also the question of solving the problem of unified management of such networks in the context of international security. At the same time, the achievement of the set goals in this sphere presupposes a political compromise between all the UN member states and the involvement of all interested parties in this process.**

Keywords — criminal law, cybercrime, cybercrime management, cybersecurity, cybertechnology, information security

Cyberspace, if to consider it as the fifth dimension alongside with land, air, sea and space, makes it urgent to coordinate the efforts of all countries like with all the other four dimensions. In this connection, we find it necessary to underline:

- an insufficient current level of security measures undertaken;
- an instable infrastructure and a rather weak ability to face challenges;
- low public awareness among different layers of society, including educational institutions – from elementary to higher education, including lifelong education – as well as a very low level of research offering "national" decisions;
- lack of cybercompetence and workforce in each and every domain and in every sphere of human activity;
- lack of technical equipment at the disposal of courts and police to combat cybercrime.

At present, there is a growing concern over the increased use of digital devices; additional vulnerabilities due to the increased "application" of digital technologies; problems of security caused by the switch over to mobile and cloud applications; an increased use of new components of malware; an uprising of incidents connected with cybercrime, which are accompanied by huge costs for national economies, corporations and individual digital users; emergence of even more powerful criminal syndicates working on the international scale which are ready and well-equipped to commit cybercrimes and participate in cyberconflicts on hire. The combination of all these circumstances is a new factor – a new qualitative level of cyberthreats which can completely undermine trust to the cyberspace.

Nowadays, sources of potential risk for cyberstability and cybersecurity include the use of more advanced infrastructures and cybertechnologies. Even more serious are threats posed by external events, such as natural disasters or attacks by governments, criminal organizations or individuals. Research has shown that even designers, operators and users of different systems may either intentionally or unintentionally become one of the major sources of vulnerability of cybertechnologies. Therefore, we have to solve main technical and scientific problems how to face "challenges, emergencies and develop the capability to restore" in cyberspace.

Cyberspace is both virtual and real, made up and dependent upon the Internet technologies, services and data. Cyberspace has become, at least, for younger generations part of a "natural landscape" like land, sea, air and space, and as customary as electricity. Some view cyberspace either as a dynamic territory which is constantly developing or as a territory which has to be conquered, subjected and controlled.

Others consider cyberspace as a sphere where you can express and demonstrate your power; as a source of legal or illegal personal or economic enrichment; or a citadel of freedom or a battlefield. In fact, it is a combination of all these aspects in different degrees and to a different extent. On the whole, it reflects our political, economic and social realia, so it is neither worse not better than them. It is evidence of globalization, with economic and technical unification being its integral part. Nowadays, there is a need to adapt international law rules to the realia of the digital age and determine the limits of malicious use of digital technologies. However, there is a growing concern that instead of developing the cyberworld, our efforts to elaborate normative instruments will, in fact, legitimize a possibility for countries to expand their military potential by cyberweapons, thus making their deployment a part of strategic planning.

The situation is further exacerbated by the fact that standard information technologies have opened up a new market for criminal activity – "dark net" where criminals combine their efforts to penetrate into IT systems and take advantage of them, undermining the trust of their users. At present, every Internet network, every site, operational system

and popular software application are constantly being checked by those criminals who are searching for vulnerabilities and weak spots to receive personal profit from the use of such vulnerabilities or sell them on the black market. And since the main tasks to prevent such attacks and to reinforce the ability to get the system restored after such attacks are much more difficult to complete, it is obvious that perpetrators have more advantages in this respect.

It should be taken into account that the process of convergence of electronic and real worlds is not a fiction, but a reality, in particular, if to speak about a human body and different sensors, prosthetic devices and other elements of biomedical electronics which can be implanted in the human body to eliminate certain dysfunctions (for example, insulin pumps, cardio stimulators). The already existing neural interfaces enable people to cooperate with computers by the power of thought.

Even though the convergence of these two types of worlds and different dimensions of their use can contribute to better welfare, access to their original meaning can lead to hacking, including the power of thought. These new risks make us analyze the issues of security more thoroughly to improve the management of such objects and to preserve our values which recently have been challenged by an increased impact of information technologies on the society.

Technically speaking, cyberrisks can be caused by engineering mistakes, failures and defaults of digital components in the working process, malfunctioning or unpredictable conduct of the system in "hypernetwork" systemic configurations. Besides, risks can occur due to the false or illegal use of digital systems as well as because of internal attacks, users' actions and even as a result of unexpected incidents or some space events.

Therefore, what we see at present is a very important and new type of event which is an unlimited, non-restricted, technically uncontrollable, unauthorized access to digital systems through the search of big data. It has led to an unprecedented level of digital industrial espionage and unlimited, and most often groundless, large-scale surveillance of intelligence services of some countries which goes far beyond their national powers infringing on the sovereignty and violating the law and order of other states. Thus, a combination of safe and reliable cybertechnologies is a necessary prerequisite for trust in the expanded use of technologies. However, at present we see several trends undermining such trust:

- large-scale espionage with the aim to guarantee national security further contributed by a sharp decrease in the cost of data collection and storage of personal information;
- the use of computer codes for military activities beyond the national borders;
- availability of an externally uncontrollable and eclectic group of imposters from hired spammers to hired botnet developers;
- almost impossibility of making cybercriminals liable if they are beyond the jurisdiction under the attack.

Cyberthreats occurring today – from espionage to attacks similar to the military ones – and multi-party interest and involvement as well as the transnational and transboundary character of the Internet create a rather unusual space for the activities of different states in cyberspace: national governments deal with a domain which they, in fact, have no direct control over; but in connection with which they often have to defend their citizens, especially, when it comes to the protection of their human rights. At present, there are some comprehensive regional measures and a limited number of global measures undertaken to establish general basic rules which enable to enjoy such protection.

In this case, a wider development of formal methods of depiction and designing a system can provide for a possibility to detect and avoid certain (unsafe and critical) conditions of the system if proper measures of detection and prevention are deployed. However, events and risks which could not be anticipated while designing a system can lead to unpredictable and unexpected conduct of the system which can be difficult or even impossible to control or correct. In the worst scenario, the system can get disabled and not restored. Therefore, we have to develop and implement proper methods of reinforcement of its restorative capability.

Another feature of cyberspace is that it is becoming more militarized, because more and more states have been developing their offensive weapons aimed at not only military objects, but, in fact, at the most important civilian infrastructure objects and the way of life of the civilian population of their enemy. All this leads to uncontrollable side effects and there are no factors which would curb the digital race of states. Nowadays, more than 100 states are increasing their technological potential to commit digital attacks in an uncontrollable and rather spontaneous race to provide strategic dependence. In the relevant instruments it is clearly stated that information technologies can be maliciously used as a means of achieving their military and political ends. These fears, however, do not except grounded self-defense.

Considering the above said, we should emphasize some measures to prevent failures, malfunctioning, or defaults of the system, to restore the system and reinforce the capability to restore the system in cyberspace from the viewpoint of designing computer equipment. We have listed measures to be undertaken in the order of preference:

- at the physical level: restrictions on the use of materials and devices only in accordance with the pre-determined conditions of the environment (for example, by the temperature, radiation). Besides, we can make backups using other possible materials, additional processes of operation, etc., and also using different combinations of components;
- at the technical level: use of computer devices following N from M scheme, principles of transfer and coding of excessive data or use of different but standardized protocols of safe transfer makes it possible not only to avoid the spread of failures but to guarantee self-regulation. Besides, measures at the technical level, which enable to avoid the spread of failures, increase the reliability of the system and better the capability to restore, include diversification, for example, the use of different variants of computational algorithms, different computational nodes, or the use of different principles of storage;
- at the information level: the aim is to preserve confidentiality, integrity and accessibility of

information. Besides, there might be other features involved, for example, authenticity, a possibility of record and prevention of the refusal from the authorship – ISO/IEC 27000;

- at the corporate/ institutional/ personal level: the system of laws and rules of exploitation; institutional, regional and cultural codes of behavior; proper education; spread of information and training to increase the level of awareness in the issues of cybersecurity;
- at the global level: adherence to the worldly recognized political agreements and as far as it is possible to the global codes of behavior;
- creation of a system of international laws and rules of exploitation, imposition and adherence to regional and cultural codes of behavior; introduction of proper education; the spread of information materials and a possibility of professional training to increase the level of awareness in the issues of cybersecurity.

As we can see, the closer we are on our inevitable way to the Internet of things, the wider use of sensor technologies, cyberphysical systems, cloud services, big data and adaptive intellectual systems we will see, and that will increase possibilities of using cybertechnologies and their impact on our everyday life. This trend is accounted for not only by the development of technologies, but by a regular new market demand and demand in such production. The expansion of the cyberinfrastructure and cyberservices will not only provide privileges and benefits, but will bring additional vulnerabilities and new threats which can undermine personal and public security and the protection of the society on the whole.

This problem is rather topical because our trust to the digital age and our common welfare to a large extent depend on our ability to determine a wide range of cyberthreats and cope with them. On the basis of a thorough analysis and assessment of risks and vulnerabilities, we have to elaborate relevant measures to guarantee cybersecurity and, at least, good capabilities to restore, in particular, most important infrastructures, for example, of such systems as energy and water supply, medicine, transport and finance.

It should be pointed out that Russia has developed a systematic approach to research the questions of "information security" and "network security at the global level". It is reflected in domestic legislative acts as well as in international legal initiatives of the Russian Federation. Thus, in 2013, Russia adopted "Basics of the State Policy of the Russian Federation in the Sphere of International Information Security till 2020".

As early as in 2011, at a UN meeting, Russia initiated drafting of the necessary international instruments concerning the regulation of information security at the international level. In particular, permanent representatives of Russia, China, Uzbekistan and Tajikistan sent a common letter to the UN Secretary General in September 2011 at the 66th UN General Assembly meeting. These UN member states offered to discuss "Rules of conduct in the sphere of providing international information security". Underlying the necessity to adopt such rules, representatives of these states emphasized the importance of the issues of Internet security to be considered under the principles of international cooperation and mutual respect.

Moreover, the same year Russia offered to discuss conceptual basics of the "Convention on International Information Security". This document contained a possible definition of rights and obligations of states in the global information space with the proclaimed principle of state sovereignty over "national segments" on the Internet. A very important message of this document is the impossibility to apply information and telecommunication technologies for committing different aggressive or malicious acts, and a call to develop cooperation in the field of counteraction to terrorist and criminal activity, with the respect to human rights and freedoms in the information space.

At present, the development of information and communication technologies makes it necessary to consider the questions of information security at the international level, but require solving a question of a unified management of such communications in the context of international security. At the same time, achieving of the said goals requires a political compromise to be established between all UN member states and involvement of all the parties concerned.

A favourable situation for enhancing cooperation between the countries will enable us to solve a set of tasks in the sphere of joint management of information and communications networks (ICN) taking into account their transboundary character. First of all, we have to elaborate a system of security guarantees under the rules of international law for the use of ICN. That was the aim of the RF initiatives in the sphere of information security.

Another important aspect is the necessity to adjust legal remedies and methods of regulating ICN at the national level. It can be achieved by harmonizing the national legislation, in particular, procedurally regulating the work of law enforcement bodies and prosecution.

A third aspect is the necessity to elaborate norms of international law regulation aimed at developing rules and principles of providing security of the critically important infrastructure of ICN taking into account their transboundary functioning.

Solving a problem of adequate identification of ICN users as well as owners of Internet resources and operators rendering electronic services is another vital aspect to be considered at the level of international law.

And, finally, we should improve the existing legal regulation of the order of rendering electronic services by means of ICN by their providers which are legal entities established in full compliance with the national legislation. To a large extent, it is connected with the necessity to preserve stability and unity of the transboundary functioning of ICN for which we have to adjust the regulation of the issues of jurisdiction of states at the domestic and international level.

We should agree that we need a real and immediate international agreement to work out a consistent and global approach to solve the problem of vulnerability of cyberspace. Different organizations, enterprises and states face significant risks of improper disclosure of information, misappropriation and destruction of data and information. Such incidents analyzed at the macroscopic level can be considered as a potential threat not only to competitiveness and reputation of a commercial enterprise, but also to public security, protection and the very democracy at the national level.

At the same time, the idea of drafting a global agreement of a binding character, which would establish a majority of rules to be complied with in cyberspace and which would stipulate

consequences for their non-compliance, may seem interesting. Thus, a global agreement or a set of agreements on cybersecurity and cybercrime at the UN level must become a platform for maintaining peace, justice and security in cyberspace. Such an agreement would contribute to the development of a global strategy to curb threats appearing on any part. It will contribute to better understanding of different aspects of cybersecurity in all countries regardless of their level of economic development. Such an agreement must become a universal approach to reducing risks and challenges in cyberspace. It should provide for the necessary architecture of taking efficient national and international measures to combat cyberattacks and must include a precise definition of acceptable and unacceptable conduct as well as the necessary models of management.

Therefore, topical issues in the management of the use of cybertechnologies are: to elaborate a system of security guarantees at the international law level while using ICN; to harmonize the national legislation, in particular, to procedurally regulate the cooperation of law enforcement bodies and prosecution bodies; to develop norms of international law regulation defining certain rules and principles of guaranteeing security of the critically important infrastructure of ICN taking into account its transboundary functioning; to solve the problem of adequate identification of ICN users as well as owners of Internet resources and operators rendering electronic services via ICN; to improve the existing legal regulation of the order of rendering electronic services by means of ICN by their providers.

References

[1] Kapustin A. Ya., K voprosu o mezhdunarodno-pravovoj kontseptsii ugroz mezhdunarodnoj informatsionnoj bezopasnosti // Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniia [On the Issue of the International Law Concept of Threats to International Information Security // Journal of Foreign Legislation and Comparative Law Study]. 2017. No. 6, pp. 44 - 51.

[2] Basics of the State Policy of the Russian Federation in the Sphere of International Information Security till 2020 http://www.scrf.gov.ru/security/information/document114/

[3] Pashkov R., Yudenkov Yu., Sistema upravleniia riskami pri osuschestvlenii operatsij s ispol'zovaniem platezhnykh bankovskikh kart // Bukhgalteriia i banki [The System of Risk Management with Banking Card Operations // Accounting and Banks]. 2017. No. 7, pp.48 – 56.

[4] Information Security Management Systems. GOST ISO/IEC 27000

[5] http://gostexpert.ru/data/files/27000-2012/69110.pdf

[6] Dr Hamadoun Touré, V poiskakh kiberdoveriia. Mezhdunarodnyj soiuz elektrosviazi i Vsemirnaiia federatsiia uchenykh. 2015, p. 57

[7] https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.02-1-2014-PDF-R.pdf

[8] Challenges, Vulnerabilities and Exploits – Can You Imagine!

[9] https://www.icann.org/news/blog/ru-a90a62fd-2dc0-4480-bd62-0dc1acdd4d8c

[10] SOC members initiated to the UN rules on providing international information security https://tass.ru/politika/1732434